MOROĞLU ARSEVEN

Turkish Data Protection Law 2024

Developments in Practice in its Ninth Year

Preface

Moroğlu Arseven is pleased to present our latest study on Turkish data protection law following the enactment of the Personal Data Protection Law No. 6698. Now in its fifth edition, this year's study delves into the pivotal developments during the Law's ninth year of implementation, spanning the period from 1 January 2024 to 31 December 2024. It provides a comprehensive analysis of key considerations for compliance with the law on the protection of personal data, alongside insights into legislative updates, practical applications, and the perspectives of the Personal Data Protection Board.

This study draws on historical data, including *the Information Note on the 2024 Activities of the Personal Data Protection Authority* and the 2023 Activity Report. It also incorporates public announcements, reports, and decisions made available on the official website of the Personal Data Protection Board as of the publication date.

Should any specific topic catch your attention or be of particular importance to you, please do not hesitate to contact us for a more detailed discussion.

Contents

MOROĞLU ARSEVEN

Contents

MOROĞLU ARSEVEN

A. DEVELOPMENTS IN LEGISLATION AND PRACTICE

MOROĞLU ARSEVEN

I. Overview of the Legislation on the Protection of Personal Data

Although personal data is protected by several legislative sources, including primarily the Constitution of the Republic of Turkiye, the main inclusive regulation in compliance with the international modern approach to personal data protection was adopted in Turkiye through the Personal Data Protection Law No. 6698 ("**DP Law**"). With the DP Law's coming into force, several pieces of legislation regarding personal data protection and its interpretation and practice have been clarified, primarily including the provisions of the Turkish Criminal Code No. 5237 ("**TCC**").

Under the DP Law, the Personal Data Protection Authority ("**Authority**") was established as a financially and administratively autonomous public legal entity with regulatory and supervisory authority. The Authority conducts its operations through a structure comprising the decision-making body, the Personal Data Protection Board ("**Board**"), and the Presidency.

Secondary legislative processes have been executed subsequent to the DP Law coming into force, including the Regulation on the Data Controllers Registry; Regulation on the Deletion, Destruction or Anonymization of Personal Data; Communiqué on Application Procedures and Principles for Data Controllers; Communiqué on the Procedures and Principles to be Complied with in Fulfilling the Obligation to Inform; and Communiqué on Procedures and Principles Regarding Personnel Certification Mechanisms. Since then, the Authority has been leading practice in the field of personal data protection through its public announcements and decisions of the Board on its supervisory activities.

MOROĞLU ARSEVEN

II. Legislation and Regulations on Data Protection and Privacy

In 2024, significant amendments were made to the DP Law to align it with the European Union General Data Protection Regulation ("**GDPR**"), which changes had been anticipated for a long time.

1. Amendments to the DP Law and the Regulation on the Principles and Procedures for the Transfer of Personal Data Abroad

With the Law on Amendments to the Code of Criminal Procedure and Certain Laws No. 7499, published in the Official Gazette No. 32487 dated 12 March 2024 ("**Law Amendment**"), changes were made to Articles 6, 9, and 18 of the DP Law.

The amendments include provisions regarding the processing of special categories of personal data, the transfer of personal data abroad, administrative fines, and appeal processes. These changes came into effect on 1 June 2024. An additional transition period was introduced through Provisional Article 3 concerning cross-border data transfers, stipulating that the previous version of Article 9/1 of the DP Law (*data transfers based on explicit consent*) would continue to apply alongside the amended version until 1 September 2024.

Detailed explanations regarding the Law Amendment are provided below.

1.1. Amendments to the DP Law and the Regulation on the Principles and Procedures for the Transfer of Personal Data Abroad

The Law Amendment removes the prior distinction concerning data related to health and sexual life, as stipulated under Article 6/3 of the DP Law. While the prohibition on processing special categories of personal data remains intact, the conditions for processing have been expanded. The requirement to adopt adequate safeguards determined by the Board for processing special categories of personal data also remains in place.

Following the Law Amendment, the conditions for processing special categories of personal data are as follows:

- The explicit consent of the data subject.
- An explicit stipulation in law.
- Situations where it is necessary to protect the life or physical integrity of the person or another individual who is incapable of giving consent due to actual impossibility or whose consent is not legally valid.
- The personal data being made public by the data subject and processed in accordance with the intention of such disclosure.
- Necessity for the establishment, exercise, or protection of a legal right.
- Necessity for purposes of public health protection, preventive medicine, medical diagnosis, treatment, and care services, as well as the planning, management, and financing of health services, carried out by persons under an obligation of confidentiality or authorized institutions and organizations.
- Necessity to fulfill legal obligations in the areas of employment, occupational health and safety, social security, social services, and social assistance.
- Data being processed by foundations, associations, or other non-profit organizations or entities established for political, philosophical, religious, or trade union purposes, provided that the processing is in compliance with the applicable legislation and the organization's purpose is limited to its field of activity and is not disclosed to third parties. This applies to data concerning current or former members and affiliates or individuals who are in regular contact with such organizations or entities.

1.2. Amendments Regarding the Transfer of Personal Data Abroad

Long-awaited regulations concerning the transfer of personal data abroad were implemented with the Law Amendment, and the mandatory requirement for explicit consent in practice was abolished. Throughout 2024, the procedures and principles for applying the new transfer conditions were shaped through secondary legislation, guidelines issued by the Board, and public announcements. In this regard, the amendments made to Article 9 of the DP Law were assessed alongside the following developments:

- The regulations introduced by the Regulation on the Principles and Procedures for the Transfer of Personal Data Abroad ("**Regulation**"), published in the Official Gazette No. 32598 dated 10 July 2024, which came into force on the date of its publication.
- The Standard Contractual Clauses[1] ("**SCCs**") and Binding Corporate Rules[2] ("**BCRs**") Application Form published on the official website of the Authority on 10 July 2024.
- The *Public Announcement Regarding the Standard Contractual Clauses Notification Module*, published on 25 October 2024 on the Authority's official website, regarding the decision of the Board dated 17 October 2024 No. 2024/1793, enabling data controllers and processors to fulfill their notification obligations more efficiently and promptly via the "Standard Contractual Clauses Notification Module"[3].

[1] The English versions of the SCCs were published on the Authority's official website on 29 August 2024. You can refer to the Authority's announcements on this matter in Section VII.1.3.
[2] The English versions of the BCRs have not yet been published by the Authority.
[3] Only the Turkish version is available.

- The "*Announcement on the English Translations of the Regulation on the Principles and Procedures for the Transfer of Personal Data Abroad and the Standard Contractual Clauses*", published on the Authority's official website on 29 August 2024.

- The "*Guidelines on the Transfer of Personal Data Abroad*"[4] ("**Cross-Border Data Transfer Guidelines**"), published on the Authority's official website on 2 January 2025.

In parallel with the new regulations introduced by the Law Amendment, the procedures and principles to be applied in cross-border data transfers have been defined by the Regulation, while detailed explanations of the processes are provided in the Cross-Border Data Transfer Guidelines. Similarly, the final versions of the SCCs and BCRs, which were expected to be shared with the public by the Board, came into effect as of 10 July 2024.

With the Regulation, a "cross-border data transfer" was defined for the first time, as "*the transfer of personal data by a data controller or data processor subject to the DP Law to a data controller or data processor abroad or otherwise making such data accessible abroad.*" The Cross-Border Data Transfer Guidelines specify that the activity of transferring personal data abroad occurs when the following three conditions are all met:

- The data exporter, whether a data controller or data processor, is subject to the DP Law for the personal data processing activity. The Cross-Border Data Transfer Guidelines provide detailed explanations under this heading, particularly regarding the territorial scope of the DP Law. It emphasizes that the scope of the DP Law is interpreted based on the "effect principle" rather than the "territoriality principle."

- The personal data processed by the data exporter is transferred or otherwise made accessible. In this regard, the Cross-Border Data Transfer Guidelines include numerous practical examples of data transfer activities.

- The data recipient, whether a data controller or data processor, is geographically located in a third country, regardless of whether they are subject to the DP Law.

Before the Law Amendment, the transfer of personal data abroad was possible under the following conditions: **(i)** obtaining the explicit consent of the data subject; **(ii)** the presence of an adequacy decision issued by the Board regarding the foreign country to which data would be transferred; **(iii)** in the absence of adequate protection, the execution of a commitment between the parties and its approval by the Board; or **(iv)** the presence of BCRs approved by the Board. With the Law Amendment, alternative methods for cross-border data transfers have been introduced, establishing a three-step process for such transfers:

i. The presence of an adequacy decision regarding the country, specific sectors within that country, or international organizations to which the transfer will be made.

i. In the absence of an adequacy decision, ensuring that the data subject has the ability to exercise their rights and access effective legal remedies in the country to which the transfer will be made, provided that one of the appropriate safeguards specified under Article 9 of the DP Law is fulfilled by the parties.

i. If no adequacy decision is in place and none of the appropriate safeguards can be ensured, the transfer may still proceed on an exceptional basis, provided that it is incidental in nature and one of the conditions outlined under Article 9 of the DP Law is met.

The details of the cross-border data transfers to be carried out under these conditions are explained below.

a. Cross-Border Data Transfer Under an Adequacy Decision: Pursuant to Article 9/1 of the DP Law, personal data may be transferred abroad by data controllers and data processors if one of the conditions specified in Articles 5 and 6 of the DP Law[5] is met, and there is an adequacy decision in place regarding the country, specific sectors within the country,

[4] Only the Turkish version is available.

or international organizations to which the transfer will be made. The amendment allows adequacy decisions to be issued not only for countries as a whole but also for specific sectors or international organizations.

Adequacy decisions are issued by the Board and published in the Official Gazette. The Board may consult relevant institutions and organizations if needed. Adequacy decisions are reviewed by the Board every four years or as required. Based on its assessment or other necessary circumstances, the Board may amend, suspend, or revoke adequacy decisions with prospective effect.

When issuing adequacy decisions, the following factors are primarily considered:

- The reciprocity status regarding personal data transfers between Türkiye and the country, sectors within the country, or international organizations to which personal data will be transferred.
- The legislation and practices of the country to which personal data will be transferred, as well as the rules applicable to the international organization receiving the data.
- The presence of an independent and effective data protection authority in the country or within the international organization receiving the data, along with the availability of administrative and judicial remedies.
- Whether the country or international organization receiving the data is a party to international agreements or a member of international organizations related to the protection of personal data.
- The membership status of the country or international organization receiving the data in global or regional organizations to which Türkiye is a member.

As of yet, the Board has not issued any adequacy decision.

[5] "Conditions for processing personal data" in Article 5 of the DP Law, (1) Personal data shall not be processed without explicit consent of the data subject.
(2) Personal data may be processed without seeking the explicit consent of the data subject only in cases where one of the following conditions is met:
a) It is expressly provided for by the laws.
b) It is necessary for the protection of life or physical integrity of the person himself/herself or of any other person, who is unable to explain his/her consent due to the physical disability or whose consent is not deemed legally valid.
c) Processing of personal data of the parties of a contract is necessary, provided that it is directly related to the establishment or performance of the contract.
ç) It is necessary for compliance with a legal obligation to which the data controller is subject.
d) Personal data have been made public by the data subject himself/herself.
e) Data processing is necessary for the establishment, exercise or protection of any right.
f) Processing of data is necessary for the legitimate interests pursued by the data controller, provided that this processing shall not violate the fundamental rights and freedoms of the data subject.

"Conditions for processing of Special categories of personal data" in Article 6 of the DP Law,
(1) Personal data relating to the race, ethnic origin, political opinion, philosophical belief, religion, religious sect or other belief, appearance, membership to associations, foundations or trade-unions, data concerning health, sexual life, criminal convictions and security measures, and the biometric and genetic data are deemed to be special categories of personal data.
(2) Repealed.
(3) The processing of special categories of personal data is prohibited. However, such data may be processed under the following conditions:
a) The explicit consent of the individual is obtained,
b) Explicit provision in the law,
c) In cases where the individual is unable to express consent due to actual impossibility or where consent is legally invalid, it is mandatory for the protection of the individual's or another person's life or physical integrity,
ç) If the personal data in question has been made public by the individual and the processing aligns with their intention to make it public,
d) If it is mandatory for the establishment, exercise, or protection of a legal right,
e) If it is necessary for the protection of public health, preventive medicine, medical diagnosis, treatment and care services, as well as the planning, management, and financing of health services, carried out by persons or authorized institutions bound by confidentiality obligations,
f) If it is mandatory for fulfilling legal obligations related to employment, occupational health and safety, social security, social services, and social assistance,
g) If it is for political, philosophical, religious, or trade union purposes within the framework of associations, foundations, and other non-profit organizations or formations, provided it complies with the legislation they are subject to, is limited to their activities, and not disclosed to third parties. It may also apply to their current or former members or individuals in regular contact with such entities.
(4) Adequate measures determined by the Board shall be also taken while processing the special categories of personal data.

b. Cross-Border Data Transfer Based on Appropriate Safeguards: In the absence of an adequacy decision, *data controllers and data processors* may transfer personal data abroad if the following conditions are all met: **(i)** the existence of the conditions specified in Articles 5 and 6 of the DP Law; **(ii)** the data subject has the ability to exercise their rights and access effective legal remedies in the country to which the transfer will be made; and **(iii)** one of the appropriate safeguards listed below is provided by the parties.

Before relying on the appropriate safeguards, the existence of the other two conditions must always be assessed. This approach aligns with the transfer impact assessment ("**TIA**") concept applied within the European Union ("**EU**").

i. Providing Appropriate Safeguards Through Non-Treaty Agreements: Appropriate safeguards can be ensured for personal data transfers between public institutions and organizations in Türkiye, public professional organizations with public institution status, and public institutions or organizations or international organizations in foreign countries through provisions on personal data protection included in non-treaty agreements. Such agreements must contain the minimum provisions[6] on personal data protection specified under the Regulation and must be submitted to the Board for its opinion during the negotiation stage. As stated in the Cross-Border Data Transfer Guidelines, this safeguard applies to international data transfers conducted between public institutions for the purposes of cooperation. It does not cover the transfer of personal data from a public institution to a private entity or vice versa.

Within the scope of the Guidelines, non-treaty agreements can take the form of cooperation protocols, memorandums of understanding, or administrative agreements. The Guidelines highlight the administrative agreement concluded between the Turkish Medicines and Medical Devices Agency and the European Commission as a concrete example of such an arrangement.

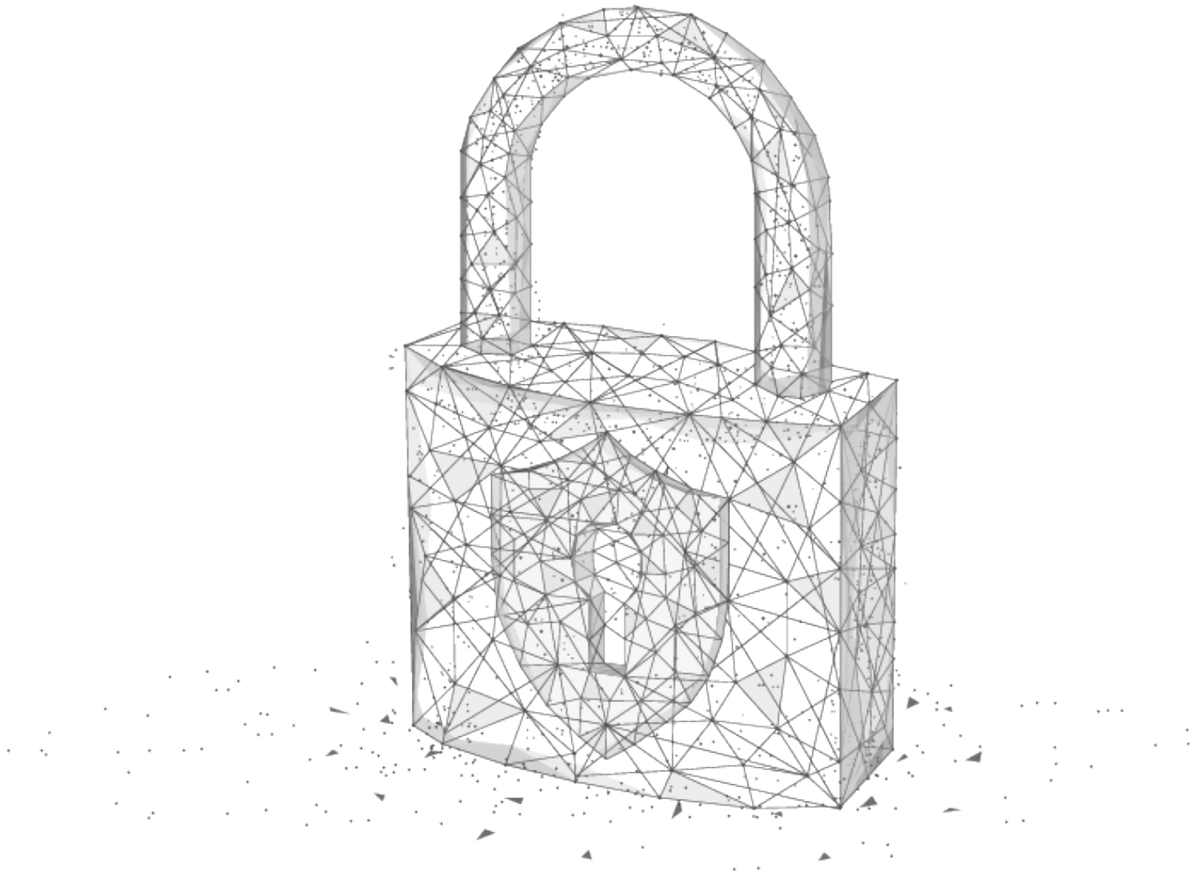
ii. Providing Appropriate Safeguards Through BCRs: The Law Amendment establishes BCRs as a legal safeguard within the legislative framework. Accordingly, appropriate safeguards can be ensured through BCRs that set out obligations regarding the protection of personal data for companies within a group engaged in joint economic activities. To transfer personal data abroad based on BCRs, an application for approval must be submitted to the Board. The approval process must be completed before the

[6] The provisions on personal data protection to be included in the agreement shall specifically cover the following:
a) The purpose, scope, nature, and legal basis of the personal data transfer.
b) Definitions of key concepts in compliance with the DP Law and related legislation.
c) A commitment to adhere to the general principles outlined in Article 4 of the DP Law.
ç) The procedures and principles for informing data subjects about the agreement and the personal data transfers conducted under the agreement.
d) A commitment to enable the data subjects to exercise their rights specified under Article 11 of the DP Law, along with procedures and principles for applications related to exercising these rights.
e) A commitment to take all necessary technical and administrative measures to ensure an adequate level of data security.
f) A commitment to adopt the adequate measures determined by the Board for the transfer of special categories of personal data.
g) Restrictions on further transfers of personal data.
ğ) Remedies available to the data subjects in the event of a breach of the provisions on personal data protection included in the agreement.
h) A monitoring mechanism to oversee the implementation of the provisions on personal data protection included in the agreement.
ı) A clause granting the data exporter the right to suspend data transfers and terminate the agreement if the data importer fails to comply with the provisions on personal data protection included in the agreement.
i) A commitment by the data importer, in the event of termination or expiration of the agreement, to either return the transferred personal data along with its backups to the data exporter or permanently destroy the personal data, depending on the preference of the data exporter.

commencement of the data transfer, and transfers can only be carried out based on the approval granted by the Authority.

Article 13 of the Regulation specifies the minimum requirements that must be included in BCRs, while the Cross-Border Data Transfer Guidelines provide detailed explanations regarding these minimum elements. In this regard, a BCR document must, at a minimum, include the following:

- The organizational structure and contact details of each member of the group engaged in joint economic activities.
- Details regarding the transfers to be conducted under the BCRs, including personal data categories, processing activities and purposes, data subject group(s), and the country or countries to which the data will be transferred.
- A commitment that the BCRs are legally binding both within the internal relationships of the group engaged in joint economic activities and in their other legal relationships.
- Data protection measures, including compliance with general principles, conditions for processing personal data, conditions for processing special categories of personal data, technical and administrative measures to ensure data security, adequate safeguards for processing special categories of personal data, and restrictions on further transfers of personal data.
- A commitment to enable data subjects to exercise their rights under Article 11 of the DP Law, as well as the right to lodge a complaint with the Board in accordance with the procedures and principles set out in Article 14 of the DP Law, along with the procedures and principles for exercising these rights.
- A commitment that, in the event of a breach of the BCRs by any group member not located in Türkiye, a data controller and/or data processor established in Türkiye will assume responsibility for the breach.
- Explanations on how data subjects will be informed about matters related to the BCRs, in addition to the information provided under Article 10 of the DP Law as part of the obligation to inform.
- Explanations regarding training to be provided to employees on the protection of personal data.
- The responsibilities of individuals or units tasked with monitoring the group's compliance with the BCRs, including activities related to responding to data subject requests.
- Mechanisms to monitor and verify compliance with the BCRs within the group, including data protection audits and methods to ensure corrective actions to protect the rights of the data subjects. The results of such audits must be reported to the individuals or units responsible for monitoring compliance with the BCRs, the management board of the controlling company within the group, and, on request, the Board.
- Mechanisms for reporting and recording changes to the BCRs and notifying the Board of such changes.
- An obligation for the group members to cooperate with the Authority to ensure compliance with the BCRs.
- A commitment that there are no national regulations in the countries where the transfer will occur that contradict the safeguards provided by the BCRs, and a mechanism to notify the Board of any legislative changes likely to negatively impact these safeguards.
- A commitment to provide appropriate data protection training to personnel who have regular or continuous access to personal data.



The factors considered by the Board when evaluating applications for BCRs are as follows:

- The BCRs must be binding and enforceable for all members of the group.
- There must be commitments to protect the rights of data subjects.
- The BCRs must include the minimum elements specified in Article 13 of the Regulation.

As of 10 July 2024, two separate application forms have been published on the official website of the Authority: the *BCR Application Form for Processors*[7] and the *BCR Application Form for Controllers*[8]. In addition to the BCR application forms, the following supporting guides were also made available: *Key Considerations for Binding Corporate Rules for Controllers – Supporting Guide*[9] and *Key Considerations for Binding Corporate Rules for Processors – Supporting Guide*[10].

For BCR applications, in addition to completing the BCR Application Form, it is also necessary to complete the Supporting Guides. The Cross-Border Data Transfer Guidelines aim to establish a standard form for applications submitted to the Board concerning BCRs, clarify the content of the minimum elements that must be included in BCR applications, ensure compliance with regulatory requirements through the Supporting Guides, and specify the documents that must be submitted to the Board.

Prior to the Law Amendment, the BCRs method was only available to data controllers. However, it can now also be used by data processors. The details regarding the points to be considered in BCRs applications are regulated by the Regulation and the Cross-Border Data Transfer Guidelines. BCRs applications have been accepted since 2020. However, the Cross-Border Data Transfer Guidelines indicate that three applications were submitted to the Authority up until 1 June 2024 but were rejected due to procedural and substantive deficiencies.

[7] Only the Turkish version is available.
[8] Only the Turkish version is available.
[9] Only the Turkish version is available.
[10] Only the Turkish version is available.

The guidelines also specify the factors to be considered when making BCRs applications, as follows:

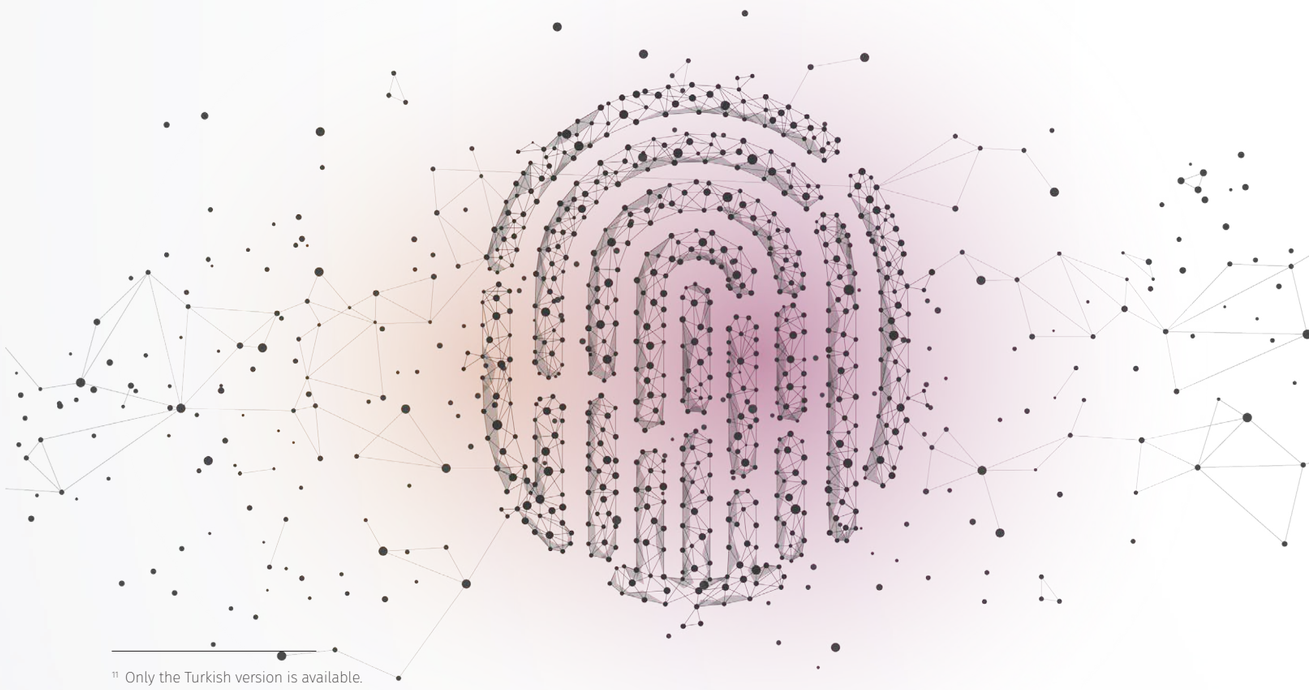
- A request for approval must be submitted to the Board for the transfer of personal data abroad, and the application must be submitted by hand, by post, or through methods specified by the Board.
- The application must be submitted with a copy of the BCRs text, the Application Form, and the relevant information and documents.
- If the responses in the Application Form and the Guidelines are insufficient, additional pages or annexes must be used.
- Certified Turkish translations of documents in foreign languages must be included with the application. If the document is prepared in a foreign language, the Turkish version will be considered the primary document.
- Documents proving the authority of the person signing the application, documents related to representation rights for legal entities, and the original or certified copy of the power of attorney for representative applications must be provided.
- If the group center is located in Türkiye, the application must be made by the institution in Türkiye. If a different institution is authorized, reasons must be provided.
- If the group center is located outside Türkiye, a group company in Türkiye must be authorized to submit the application on behalf of the company.
- Separate forms must be filled out for both Data Controller-BCRs and Data Processor-BCRs.
- Supporting documents must only be submitted for explanatory purposes and must be appropriately named (e.g., "(ANNEX-3-1)").
- The contact person or unit for inquiries

iii. Ensuring Adequate Safeguards with SCCs: SCCs are framework agreements published by the Authority that regulate the transfer of personal data abroad and establish data protection obligations between the parties. The transfer of data abroad is possible through the execution of appropriate SCCs between the transfer parties and notification to the Authority. As of 10 July 2024, the Board has published four SCCs:

i. Data Controller to Data Controller
ii. Data Controller to Data Processor
iii. Data Processor to Data Processor
iv. Data Processor to Data Controller

The procedures and principles regarding the implementation of SCCs have been regulated as follows:

- The SCCs must be signed without any amendments. After the parties determine the appropriate type of SCC in the context of personal data transfer, changes can only be made to optional or alternative clauses of the SCC.
- If the SCC is executed in both a foreign language and Turkish, the Turkish text will prevail.
- The SCC must be signed by the parties or by individuals authorized to represent and sign on behalf of the parties.
- The SCC must be notified to the Authority within five business days from the completion of the signatures, either physically, via registered electronic mail ("KEP"), or through other methods determined by the Board. To facilitate the notification process more quickly and effectively, the Standard Contract Notification Module[11] has been made available for use online.
- The parties to the transfer can determine who will fulfill the notification obligation in the SCC. If no such determination has been made, the SCC must be notified to the Authority by the data exporter. If the data processor is responsible for notifying the SCC, the data processor must fulfill the notification obligation without requiring instructions from the data controller.
- The notification must include evidentiary documents confirming the authority of the signatories of the SCC, as well as a notarized translation of any foreign-language document.
- In case there is any change in the information or explanations provided by the parties in the SCC or in the content of the SCC itself, or if the standard contract expires, the parties must notify the Authority physically, via KEP address, or through the notification module.



[11] Only the Turkish version is available.

The preparation and content of the SCCs are detailed in the Cross-Border Data Transfer Guidelines. Detailed explanations have been provided regarding the most common questions about how to fill out the SCC appendices:

» **Activities of the Data Exporter and Data Importer Regarding Personal Data Transferred Under the SCCs:** General explanations regarding personal data transfers must be provided, and the activities conducted by the transfer parties on the personal data subject to transfer must be specified in the explanations.

» **Data Subject Group(s):** The data subject group(s) to which the transferred personal data pertains must be specified on a personal data basis.

» **Transferred Personal Data Categories and (if Any) Transferred Special Categories (Sensitive) Personal Data Categories:** The transferred personal data must be indicated by category (e.g., communication) and type (e.g., email address).

» **Legal Basis for the Transfer:** The processing condition used as the basis for the transfer under Articles 5 and 6 of the DP Law must be specified.

» **Nature of Processing Activities:** The type of personal data processing activity to be carried out on the transferred personal data (e.g., storage, recording, publishing, merging, categorizing, etc.) must be explained.

» **Purposes of the Data Transfer and Subsequent Processing Activities:** The purposes of the transfer to be carried out based on the SCC and the purposes of the subsequent personal data processing activities to be carried out by the data importer (e.g., processing bank payments, providing customer support services, conducting market research, etc.) must be explained.

» **Retention Period for Personal Data:** The duration for which the transferred personal data will be retained must be specified. If it is not possible to indicate an exact period, the criteria used to determine the retention period (e.g., the duration of the personal data processing agreement) must be explained. If different categories of personal data are subject to different retention periods, these periods must be specified separately.

» **Recipients or Recipient Groups:** The recipients to whom personal data obtained from the data exporter will be transferred under the SCC must be specified in the event of subsequent transfers by the data importer. This section must be kept up to date throughout the term of the SCC.

» **Data Exporter's Information in the Data Controllers' Registry System ("VERBIS"):** If the data exporter is required to register and notify in VERBIS, the VERBIS information must be included under the relevant section for the SCCs between the data controller and the data controller, and between the data controller and the data processor. In this regard, the information provided by the data exporter in the SCC appendices must be consistent with the VERBIS records.

» **Subject, Nature, and Duration of Processing Activities in Transfers to (Sub) Data Processors:** In cases where the data importer transfers personal data to sub-processors, the subject, nature, and duration of the processing activities carried out by the sub-processor must be explained under the relevant sections for the SCCs between the data controller and the data processor, and between the data processor and the data processor.

◊ **Providing Adequate Safeguards through a Commitment:** Adequate safeguards can be provided through provisions related to the protection of personal data in a written commitment to be concluded between the transfer parties. In order to transfer personal data abroad based on the commitment, the data exporter must apply for permission to the Board.

If the commitment is concluded in a foreign language, the Turkish text will prevail. Personal data transfer can begin only after the Board grants permission. In applications for permission to the Board, in addition to the information of the person authorized to apply, documents verifying the person's authority to sign must also be included.

The provisions to be included in the commitment related to the protection of personal data must specifically cover the following points:

- The purpose, scope, nature, and legal basis of the personal data transfer.
- Definitions of basic concepts in accordance with the DP Law and relevant legislation.
- A commitment to comply with the general principles.

- Procedures and principles for informing the data subject about the data transfer under the data transfer agreement.
- A commitment to allow the exercise of the rights of the data subjects as specified in Article 11 of the DP Law, and the procedures and principles for applications to exercise these rights.
- A commitment to take all necessary technical and administrative measures to ensure an appropriate level of data security.
- A commitment to implement the sufficient measures determined by the Authority in case of transferring special categories of personal data.
- Restrictions on the subsequent transfer of personal data.
- The methods of legal redress available to the data subjects in case of a breach of the agreement.
- A commitment to comply with the decisions and opinions of the Authority regarding the processing of the personal data subject to transfer.
- A commitment to inform the data exporter as soon as possible about the absence of national regulations that would prevent compliance with the agreement, and of any potential legislative changes that may occur, and to provide the data exporter the right to suspend data transfer and terminate the agreement in such a case.
- A provision that the data exporter has the right to suspend the data transfer and terminate the agreement in case the data importer fails to comply with the agreement.
- A commitment that, in the case of termination of the agreement or expiration of its duration, the data exporter may choose to either return the transferred personal data along with its backups to the data exporter or completely delete the personal data.
- A provision that the agreement is subject to Turkish law and, in the event of a dispute, Turkish courts have exclusive jurisdiction, with the data importer agreeing to submit to the jurisdiction of Turkish courts.

Two types of commitment application forms, namely the Transfer from Data Controller to Data Controller and the Transfer from Data Controller to Data Processor, were published on the official website of the Authority on 9 March 2020. As of the latest developments, no changes have been made to the relevant forms[12]; it is still possible to submit the commitment application using the same forms, or, alternatively, an application can be made through a commitment text prepared to include the aforementioned regulations.

[12] An update is expected under the Law Amendment.

c. Exceptional Transfers: According to the Regulation, "exceptional transfers" are defined as *"non-regular, one-off or infrequent, non-continuous, and transfers not part of the usual course of activities."* Personal data may be transferred abroad as exceptional transfers where a decision of adequacy or adequate safeguards for international data transfer cannot be established, provided that one of the exceptional transfer conditions listed below is met:

» The data subject gives explicit consent to the transfer and is informed about potential risks.

» The transfer is necessary for the performance of a contract between the data subject and the data controller or for taking pre-contractual measures.

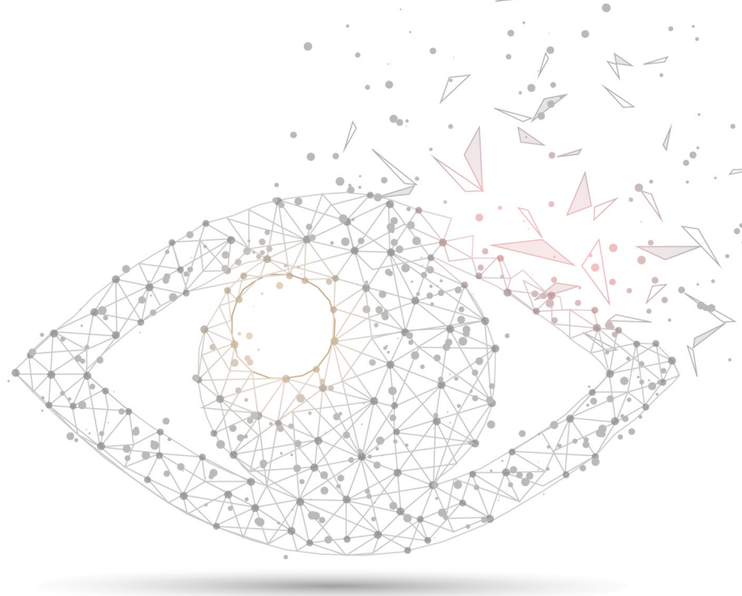
» The transfer is necessary for the establishment or performance of a contract between the data controller and third parties for the benefit of the data subject.

» The transfer is necessary for the purposes of a significant public interest.

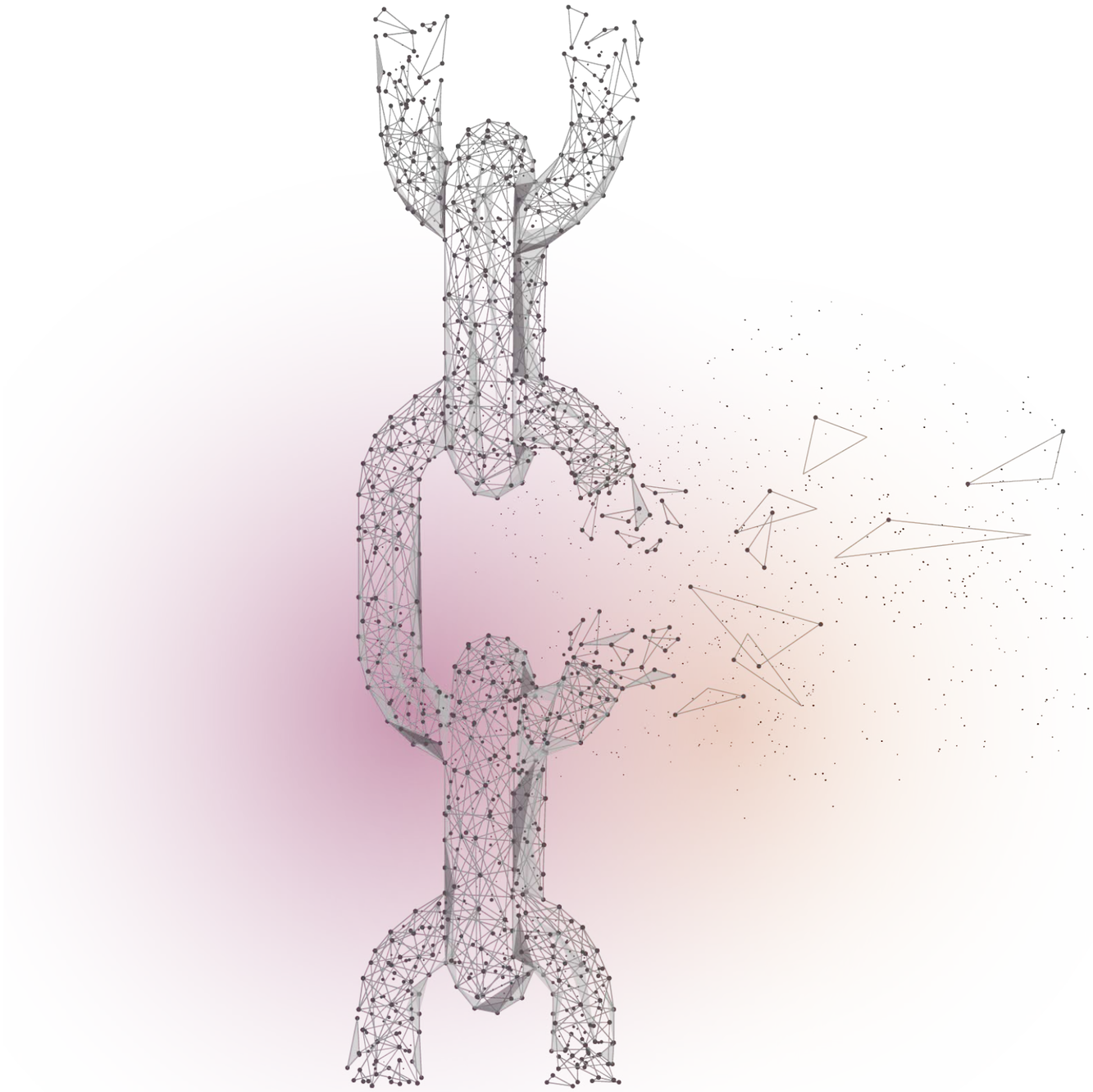
» The transfer is necessary for the establishment, exercise, or defense of legal claims.

» The transfer is necessary to protect the life or physical integrity of the data subject or another person, where the data subject cannot express consent due to physical impossibility or where the consent is not legally recognized,

» The transfer is made from a public record accessible to the public or to persons with legitimate interests, provided that the conditions required by the relevant legislation for accessing the record are met and requested by a person with legitimate interests. Personal data may be transferred abroad from open registers on the request of a person with legitimate interests.



MOROĞLU ARSEVEN



According to the Cross-Border Data Transfer Guidelines, “exceptional transfers” should be interpreted narrowly, since they are exceptional cases. An exceptional transfer covers processes that are outside the regular course of business. Exceptional transfers are outside the regular flow of activities and occur one or more times, under unforeseen conditions, and within uncertain time intervals, provided they are not regular. Personal data transfers that occur regularly as a result of an ongoing relationship between the data exporter and the data importer are generally considered systematic and repetitive data transfers. For example, as stated under the “Exceptional Transfer” section in the Cross-Border Data Transfer Guidelines, “granting direct access to a database to the data recipient” is considered a transfer of a continuous nature.

In the case of exceptional transfers, it is not necessary to meet the personal data processing conditions under Articles 5 and 6 of the DP Law. When an exceptional transfer occurs, personal data can be transferred abroad without the need for these conditions to be fulfilled. There is also no requirement for the Board's permission or approval, nor any notification obligation for exceptional transfers.

The Cross-Border Data Transfer Guidelines also provide examples of exceptional transfers, such as the following:

» Transfers made by a tourism company regarding its customers' reservation information will not be considered exceptional, as they are part of the company's regular business operations.

» Transfers of personal data by travel agencies to hotels or other commercial partners in order to organize the accommodation of individual customers abroad may be considered mandatory and in line with the purposes of the contracts between the travel agency and the customers.

» The transfer of a sales manager's personal data by their employer in order to meet with clients abroad as part of fulfilling an employment contract may be considered an exceptional transfer.

» A Turkish company's transfer of personal data to another company abroad to fulfill a customer's payment request, provided that the transfers between the two companies are not regular, occur once or a few times, are not continuous, and do not fall within the regular course of business, may be considered an exceptional transfer.

» A multinational company's systematic transfer of personal data, such as the names, surnames, and job titles of employees participating in training courses at an educational center abroad, would not be considered an exceptional transfer.

» The submission of personal data-containing documents to judicial authorities abroad to ensure the exercise of the right of defense in the context of an investigation may be considered an exceptional transfer based on the necessity for the establishment, use, or protection of a right.

1.3. Amendments Regarding Appeals Against Board Decisions and Administrative Fines

The amendment to Article 18 of the DP Law titled "*Administrative Offenses*" imposes a penalty ranging from TRY 50,000 to TRY 1,000,000 TRY (TRY 71,965 to TRY 1,439,300 in 2025) for violations of the notification obligation under Article 9/5 of the DP Law. Additionally, the scope of administrative fines has been expanded with the Law Amendment. Under the previous regulation, administrative fines were only imposed on data controllers. However, with the new regulation, the scope has been broadened to include data processors in the context of cross-border data transfers.

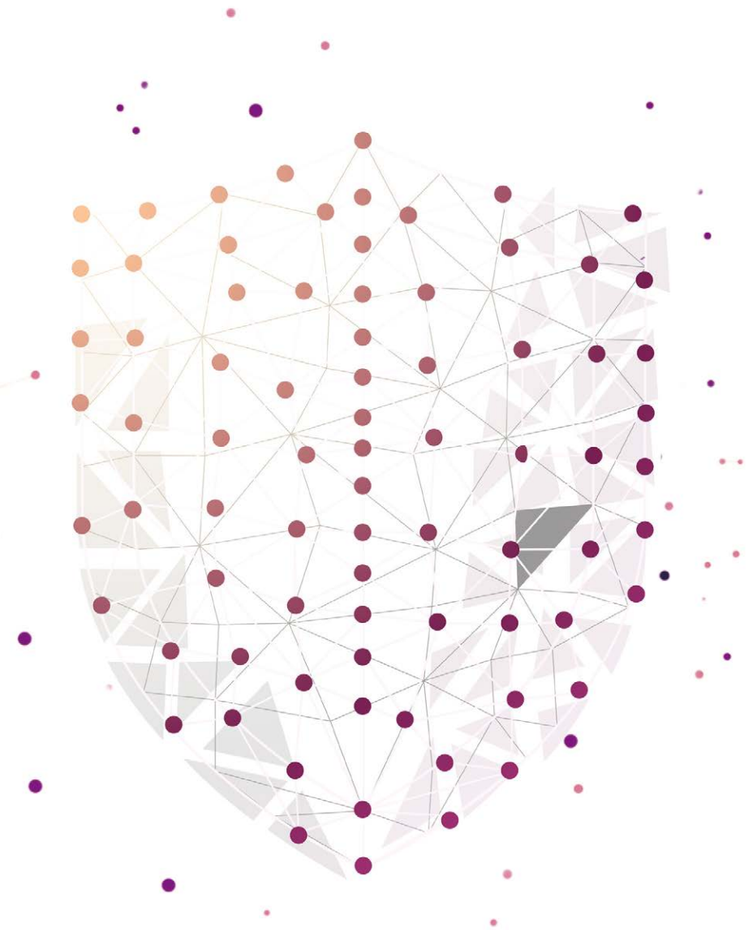
Additionally, prior to the Law Amendment, appeals against administrative fine decisions issued by the Board had to be made to the criminal courts. However, following the amendment, lawsuits can be filed in the administrative courts against administrative fines imposed by the Board.

2. Developments in Artificial Intelligence

On 24 June 2024, the Artificial Intelligence Bill was first put on the agenda of the Grand National Assembly of Türkiye ("**TBMM**"). The main objectives of the bill include promoting the use of artificial intelligence ("**AI**") systems in a manner that secures individuals' fundamental rights and freedoms, ensuring the adoption of fair, transparent, and ethical principles in the development and application of artificial intelligence technologies, and establishing a framework compatible with international standards. The bill also aims to enhance global competitiveness and create an ecosystem supporting sustainable economic growth based on innovative technologies. As outlined in Section A.IX.1, it is envisaged that AI ventures will be promoted in line with Türkiye's strategic plans and goals.
The Artificial Intelligence Bill includes the following provisions:

- Definitions of artificial intelligence and related terms.
- Key principles to be followed in the development, use, and distribution of AI systems: security, transparency, fairness, accountability, and privacy.
- Risk management provisions, requiring risk assessments during the development and use of AI systems, and special measures for high-risk systems. High-risk AI systems should be registered with the relevant regulatory authorities and subjected to compliance assessments.
- Regulations on compliance and oversight, making distributors, users, importers, and distributors responsible, and granting extensive powers to regulatory authorities to audit and detect violations of AI system compliance. Administrative fines are provided for in case of violations.

On 5 October 2024, the Official Gazette No. 32683 published the "Decision to Establish a Parliamentary Research Commission on Identifying Steps to Be Taken for AI Achievements, Creating a Legal Framework in This Field, and Preventing Risks Associated with AI Use" adopted by the TBMM. Within the framework of this decision, a Parliamentary Research Commission on Artificial Intelligence ("AI Commission") was established, consisting of 22 members. On 16 January 2025, the Official Gazette No. 32784 published the TBMM's decision on the selection of members for the AI Commission. With the selection of its members, the AI Commission is now ready to begin its work.



3. Legislative Developments in Cybersecurity

With Presidential Decree No. 177 ("**Decree**") published in the Official Gazette on 8 January 2025, the establishment of the Cybersecurity Directorate under the Presidency was approved. The Decree authorizes the Cybersecurity Directorate with key responsibilities, including the formulation of cybersecurity policies, execution of legislative efforts, and implementation of awareness-raising activities.

Following the establishment of the Cybersecurity Directorate, on 10 January 2025, the Cybersecurity Bill was submitted to the National Defense Commission of the TBMM. The bill encompasses all public institutions and organizations, professional bodies, and entities with or without legal personalities, as well as individuals operating in cyberspace. Through this regulation, the implementation of cybersecurity strategies, mitigation of the effects of cyberattacks, and the obligation to take necessary precautions are equally distributed between the public and private sectors.

The Cybersecurity Bill establishes the fundamental principles of cybersecurity and defines key concepts. In addition to the provisions of the Decree, it comprehensively regulates the duties, powers, and responsibilities of the Cybersecurity Directorate. The bill also envisions the establishment of the Cybersecurity Board to develop and implement cybersecurity policies. Furthermore, it sets out the principles for the standardization and certification of cybersecurity products and services.

The regulation revises forensic rules specifically tailored to cybersecurity breaches and transfers the authority of the National Cyber Incident Response Center (USOM) to the Cybersecurity Directorate. The Cybersecurity Bill adopts a more holistic approach by introducing amendments that align with both Law No. 5651 on the Regulation of Publications on the Internet and Combating Crimes Committed through Such Publications and Law No. 5809 on Electronic Communications.

The obligations related to the lawful processing, storage, and, where necessary, deletion of personal data belonging to parties operating in cyberspace are comprehensively outlined. Within this scope, various measures have been implemented to ensure that personal data is processed in compliance with data protection and privacy principles, to prevent data breaches and to secure confidential information.

Finally, the Cybersecurity Bill provides for both administrative and criminal sanctions in response to cybersecurity breaches. For instance, imprisonment is prescribed for offenses such as cyberattacks, data breaches, and the dissemination of leaked data. Additionally, administrative fines determined based on revenue are imposed for violations of the legislation, failure to take necessary measures, or obstruction of inspection activities. The Cybersecurity Bill explicitly addresses how administrative penalties are to be applied in cases involving benefits obtained or damages incurred.

Various regulations and sanctions have been introduced within Turkish legislation to ensure cybersecurity. Notably, the Turkish Panel Code No.5237 ("**TPC**") includes a dedicated section titled "Crimes in the Field of Information Systems," while the Law No. 5846 on Intellectual and Artistic Works, addresses actions that may constitute cybercrimes. Additionally, the increasing prevalence of cybercrimes in the online environment, the establishment of specialized internet-related institutions, and the need for a regulatory framework have been addressed by Law No. 5651 on the Regulation of Publications on the Internet and Combating Crimes Committed through Such Publications, dated 4 May 2007. However, as stated in the rationale of the Cybersecurity Bill, the growing threats to critical infrastructures and the increasing complexity of cyber incidents, driven by technological advancements, necessitate a reevaluation of this area and its approach from a new perspective. Accordingly, as highlighted in its rationale, the Cybersecurity Bill is considered to address more specific regulations for ensuring cybersecurity, distinct from the broader provisions included in existing general legislation.

4. Regulations on Health Data

With the Law on Amendments to the Social Insurance and General Health Insurance Law and Certain Other Laws, published in the Official Gazette on 15 January 2025, an additional Article 19, titled "*Authority to Collect, Process, and Share Information*," was added to the Basic Health Services Law No. 3359 ("**Law No. 3359**").

This additional article establishes the principles for processing, securing, and sharing personal data within the scope of healthcare services. According to the article, the personal health data of individuals seeking healthcare services may be processed for purposes such as protecting public health, planning healthcare services, calculating costs, and managing healthcare delivery. It is also stipulated that health data cannot be transferred except under the conditions specified in the DP Law.

Additionally, the Ministry of Health is required to securely store this data, establish a system to enable individuals to access their data, and implement oversight mechanisms for the system.

Furthermore, public institutions and organizations, as well as private legal entities and individuals employing healthcare personnel, must notify the Ministry of Health about their personnel and personnel movements.

MOROĞLU ARSEVEN

MOROĞLU ARSEVEN

III. Documents Published by the Board in 2024

1. Published Documents

1.1. Strategic Plan 2024–2028

The Strategic Plan for 2024–2028 ("**Strategic Plan**"), published on the official website of the Authority, evaluates the strategic plan concerning the activities carried out by the Authority during the 2019–2023 period. The Strategic Plan also establishes long-term goals and strategies to ensure that the Authority can effectively fulfill its duties over the next five years, while aiming for the efficient management of resources and activities.

The key highlights of the Strategic Plan are as follows:

- The objectives and goals of the Strategic Plan include ensuring the lawful processing of personal data, increasing societal awareness about the protection of personal data, positioning the Authority as a leading and influential institution internationally, improving its institutional structure, and enhancing the capacity of the Authority's operations.

- During the 2019–2023 period, a total of eight principal decisions and 5,030 Board decisions were issued as a result of complaints submitted to the Board or ex officio investigations. The number of decisions exceeded expectations, with an achievement rate of 81% for the current year's target.

- In 2019, the Data Breach Notification Module was introduced, enabling data controllers to report personal data breaches electronically. To date, 517 data breach notifications have been received through this module. Additionally, the e-Complaint Module and the Investigation Module were implemented in 2020.

- The number of notices and complaints submitted to the Authority by data subjects has increased every year. By 2023, 2,733 notices and complaints had been resolved.

- Since 2018, the Alo 198 DP Law Information and Consultation Call-Center has handled a total of 575,285 calls. These calls comprised 5% on data transfers, 6% on the scope of the DP Law, 7% on explicit consent, 10% on Board decisions and public announcements, and 54% on VERBIS registrations. Additionally, other topics included the obligation to inform, applications to data controllers, and data subject rights.

- Under Article 16 of the DP Law, natural and legal persons processing personal data must register with VERBIS. This includes natural and legal persons based in Türkiye and abroad, as well as public institutions, except for data controllers exempted by the Board. The Authority has taken significant steps through VERBIS to ensure the protection of personal data and compliance with data controllers' obligations.

- Since VERBIS became operational in 2018, a total of 210,051 data controllers have registered. According to the relevant Board decision, data controllers subject to the registration obligation had to complete their registration by 31 December 2021. Data controllers who become subject to the registration obligation after that date must register within 30 days. Consequently, registrations of data controllers have continued. Moreover, a total of 1,676,258 inquiries about data controllers were conducted through VERBIS during this period.

- To contribute to the development of the Authority and guide its activities, a survey was conducted among internal stakeholders to identify employee expectations, strengths, weaknesses, and areas for improvement. The results of this survey served as a foundation for PEST and SWOT analyses during the strategic planning process.

- In preparing the PEST analysis, political, economic, sociocultural, technological, and legal factors were examined in detail:

  - Political factors include the EU membership process, the designation of safe countries, data protection legislation, geopolitical position, public policies, data analytics, new regulations, and international agreements.

  - Economic factors include international trade, the cost of data breaches, the competitiveness of compliant companies, new business opportunities, and certification processes.

  - Technological factors include R&D efforts, artificial intelligence, technological product diversity, reliance on imports, and the need for legislation to address evolving technology.

  - Social factors include societal awareness, technology usage, educational curricula, demographic structure, education levels, rising crime rates, and increasing internet dependency.

- The SWOT analysis identifies the strengths and areas for improvement of the Authority, as well as opportunities and threats that may arise externally:

» Strengths include the Authority's exclusive regulatory and supervisory powers, its significant position for international collaborations, and its ability to make decisions swiftly.

» Areas for improvement include limited physical working conditions, the need for enhancement of institutional capacity and organizational structure, and the continuous development of technological infrastructure.

» Opportunities include the prominence of personal data protection at both national and international levels, the availability of funding for national and international projects, and the increasing public awareness of data protection.

» Threats include resistance from data controllers to comply with the legislation, challenges in enforcing sanctions against data controllers based abroad, and the difficulty of legal regulations keeping pace with technological advancements.

• Additionally, the Strategic Plan outlines the Authority's objectives under the strategy development heading for the next five years, along with the strategies, responsible parties, risks, and costs associated with achieving these objectives. These objectives include:

» OKeeping legislation on the processing of personal data up to date to reflect societal and technological changes and enacting necessary legal regulations within this scope.

» Resolving notices and complaints swiftly and effectively.

» Ensuring that data controllers take necessary administrative and technical measures to secure data.

» Ensuring compliance with VERBIS registration and notification obligations and keeping VERBIS updated.

» Conducting awareness-raising and training activities related to the protection of personal data.

» Meeting the information needs of all segments of society regarding personal data protection legislation and its application.

» Educating children and young people on the importance of personal data and raising awareness among school-aged children and youth.

» Strengthening relations with public and private institutions/ organizations.

» Enhancing international cooperation within the scope of global practices related to personal data protection.

» Strengthening the Authority's image on an international level.

» Increasing the effectiveness of personal data transfer processes abroad.

» Improving the Authority's physical infrastructure and working environment.

» Enhancing the capacity and security of the Authority's information systems.

» Increasing the quality and quantity of human resources.

1.2. Deepfake Information Note

The Authority published the "*Deepfake Information Note*" on 19 January 2024. Through this note, the Authority explained deepfake technology and shared with the public the key considerations for protecting personal data. The key points included in the Deepfake Information Note are summarized below:

- Deepfake technology, a term derived from the combination of the English words "deep learning" and "fake," is defined as the use of artificial intelligence techniques to imitate or alter a person's face, movements, and voice by utilizing their photos, videos, or audio recordings.

- It is stated that deepfake technology poses risks such as manipulation of individuals using personal data, financial harm, cyberbullying, and fraud. Specifically, combining audio and visual data with other personal data can create hybrid content that is detached from reality but incorporates real personal data. Therefore, offenses and violations involving personal data may arise in deepfake content.

- The Deepfake Information Note includes an example question list prepared by the Massachusetts Institute of Technology (MIT). It is noted that the answers to these questions may provide clues about whether a piece of content was created using deepfake technology. For example: "*Does the person in the video have unnatural eye movements or blink?*"; "*Does the face in the content appear too smooth or too wrinkled?*"; "*Does the facial expression of the person in the video match the emotion conveyed by their speech?*"

- The Deepfake Information Note also shares some solution proposals to mitigate the risks posed by the use of deepfake technology. These include paying attention to personal data shared individually on platforms such as social media, raising awareness and consciousness about this issue, and utilizing tools developed for detecting deepfake content. On the institutional side, it is emphasized that organizations should effectively manage their network and cybersecurity operations, establish a centralized reporting and monitoring unit, improve internal communication channels, and collaborate with public relations departments. Additionally, it is suggested that anti-deepfake software be developed to prevent the use of deepfake technology for impersonation or identity theft on social media and content provider platforms. For cybersecurity companies, recommended measures include developing tools to detect deepfake content, analyzing deepfake videos, creating databases by referencing original content, raising user awareness about deepfake technology, and developing defense methods against potential cyberattacks utilizing deepfake technology.

1.3. Document on Common Mistakes in Complaints and Notices Submitted to the Board

The Authority published an informational guide titled "*Common Mistakes in Complaints and Notices Submitted to the Board*", addressing frequently encountered errors during the evaluation of complaints and notices concerning the protection of personal data, on 16 July 2024. This document serves as a crucial resource aimed at ensuring that applications related to personal data protection are assessed more effectively and accurately. The document provides a detailed analysis of the most common mistakes made during submissions, such as incomplete information, unclear documents, or misinterpretation of legal regulations. It systematically outlines the methods to be followed to submit error-free applications. Within this scope, the processes for preparing accurate and complete applications are examined as follows:

- Pursuant to Article 13/1 of the DP Law and Article 14 titled "Complaint to the Board," a complaint to the Board can only be filed after first applying to the data controller and exhausting this avenue. Complaints submitted directly to the Board without first applying to the data controller will be rejected on the grounds of not meeting procedural requirements.

- Applications to the data controller must comply with the methods specified under Article 5 of the Communiqué on the Procedures and Principles for Applications to the Data Controller. Applications submitted in violation of the Communiqué will be dismissed by the Board at subsequent stages without being examined.

- One of the methods for submitting applications to data controllers is through the use of a KEP address. This method is notable for the accuracy and reliability it provides in official communication processes. The KEP system not only verifies the applicant's identity but also secures the content and timestamp of the application, thereby giving it legal evidentiary value. For applications submitted via an email address other than KEP to be valid, the email address must have been previously communicated to the data controller and recorded in their system.

- If the data controller has a website, guidance on the application processes is typically provided in the privacy notice or other sections related to personal data on the site. The data controller may clearly explain the steps required for applications, the communication channels that can be used, and the information that must be provided in the application. In such cases, it is essential for applicants to carefully review such information and follow the specified procedures to prevent potential procedural errors.

- In complaints, the failure to provide sufficient information regarding the nature and scope of the violation prevents data subjects from effectively exercising their rights. Under Article 11 of the DP Law, data subjects are granted extensive rights concerning their processed personal data, and data controllers are obligated to provide the necessary information to facilitate the exercise of these rights.

- In complaint and notice processes, legal entities cannot be considered "data subjects" under Article 3 of the DP Law. Therefore, requests regarding the protection of data belonging to legal entities fall outside the scope of the DP Law and cannot be processed. Similarly, requests concerning data belonging to deceased individuals are not covered by the DP Law. However, if the data of a deceased person identifies or makes identifiable a living individual, such data may be considered personal data with respect to the living individual. This approach is based on the fundamental principle of the DP Law, which exclusively focuses on protecting the personal data of natural persons.

- If applications are not submitted within the timeframes specified under the legislation, there is a risk that the relevant requests may not be considered. Pursuant to Articles 13 and 14 of the DP Law, the Board establishes specific and definite timeframes for applications, particularly those related to data breaches. Exceeding this timeframe negatively impacts the validity of the application. Additionally, to accurately calculate timeframes, it is crucial to submit the application documents sent to the data controller, the response letters from the data controller, and the submission documents as a complete package, including the dates indicated on these documents.

- Under Article 13 of the DP Law, applications must be made in a clear and comprehensible manner. Therefore, complaints containing vague or ambiguous

expressions make it difficult for the Board to conduct its review, potentially leading to the rejection of applications or prolonging the review process.

- Failure to fully provide the required documents during the application process not only hinders the evaluation but may also result in the rejection of the application. The DP Law and related regulations explicitly outline the documents required during the application process. Within this framework, if powers of attorney and their copies submitted to the Board do not bear the required stamp or seal, contrary to the requirements specified in Article 18/3 of the Regulation on Attorneyship Law by the Union of Turkish Bar Associations, titled *"Sample Power of Attorney and Authorization Certificate,"* the process will result in the rejection of the documents. Similarly, if a complaint or notice is submitted to the Board through a legal representative, the power of attorney must be complete and legible, and a current copy must be submitted. Additionally, according to Article 4 of Law No. 3071 on the Use of the Right to Petition, titled "Mandatory Conditions for a Petition," written applications submitted to the Board must include the complainant's name, surname, signature, and residential address.

- Failure to clearly state the applicant's relationship to the incident and their authority can cause problems regarding the application's acceptability. The DP Law requires the data subject or their representative to explicitly state their authority for the application to be valid, as a person who does not have the authority to act on behalf of the data subject cannot file a complaint with the Board on behalf of the data subject.

1.4. Information Note on the Legal Basis of "Processing Personal Data as Prescribed by Law

On 5 August 2024, the Authority published the "*Information Note on the Legal Basis of Processing Personal Data as Prescribed by Law*", clarifying the scope of the legal basis under Article 5 of the DP Law within the framework of the Constitution, the DP Law, and the GDPR. Key highlights include:

- Article 20 of the Constitution stipulates that personal data can only be processed in cases prescribed by law or with the explicit consent of the data subject, as further regulated under Article 5 of the DP Law, titled "Conditions for Processing Personal Data." None of the provisions of the Constitution can be interpreted in a way that allows the state or individuals to engage in activities aimed at eliminating fundamental rights and freedoms recognized by the Constitution or restricting them beyond the limits specified in the Constitution. Therefore, as evident from the wording of the provision, fundamental rights and freedoms cannot be regulated or restricted through instruments such as bylaws, regulations, or decrees with the force of law. The legal basis of "processing personal data as prescribed by law" under the DP Law is considered a restrictive regulation within the scope permitted by the Constitution. Accordingly, it has been clarified that restrictions can only be imposed "exclusively" by law. It is not possible for administrative regulatory actions to directly impose a restriction on fundamental rights or to create a new limitation beyond the restrictions introduced by a specific law that complies with the wording and spirit of the Constitution. However, the administration may issue regulations that concretize legal limitations. Consequently, a provision in the law permitting the processing of personal data can constitute a condition for data processing. If there is an explicit provision in a law regarding personal data processing or if a clear provision directs to secondary legislation, the processing of personal data will be permissible in such cases.

- While it has been stated in legal doctrine that the term "explicit" implies that personal data can only be processed when there is an explicit regulation in the law and that a general authority granted by law cannot be considered sufficient as a condition for processing personal data, the Information Note on Processing Personal Data as Prescribed by Law emphasizes the need to consider the intent of the legislator. It further notes that relying solely on a literal interpretation would contradict the spirit of the DP Law and that such an approach would result in the processing condition being applicable in only very limited circumstances.

- The issue has also been evaluated within the scope of the GDPR, where the fulfillment of a legal obligation and explicit prescription by law are addressed under the same article. It has been clarified that secondary regulations can also be considered within this context. According to the reasoning of the GDPR, as outlined in Recital 41, if the application of the law is foreseeable for those subject to it, the legal obligation may be applied without the need for it to be explicitly stated.

- In conclusion, the "prescribed by law" condition under the DP Law is a restrictive regulation within the scope permitted by the Constitution. It has been stated that norms outlined by law can be further detailed and implemented through regulations, communiqués, and circulars. In this context, regulatory actions duly enacted and put into effect by the administration remain binding within the administrative organization and must be implemented unless annulled.

1.5. Information Note on Chatbots (Example of ChatGPT)

The Authority published the "*Information Note on Chatbots (Example of ChatGPT)*" ("**Chatbots Information Note**") on its official website on 8 November 2024. This note provides fundamental information about chatbots, along with evaluations in the context of personal data protection and considerations for application development. It also emphasizes that chatbots must comply with the obligations under the DP Law and adhere to international standards for ensuring the security of personal data.

The Chatbots Information Note explains that chatbots are used in various sectors for purposes such as customer support, content creation, and information access. Through these applications, a wide range of personal data, including user identity information, message content, device information, and IP addresses, are processed.

The note highlights that chatbot users must be thoroughly informed about how their data is processed, including details on data retention, sharing practices, and security measures. It further states that, due to a lack of user awareness, data subjects may share excessive or privacy-compromising information, which could increase the risk of data breaches. Additionally, technical vulnerabilities in chatbot applications could expose users to cyberattacks, further elevating the risk of data violations.

Additionally, it was emphasized that the obligation to inform in accordance with the DP Law must be fulfilled, and necessary technical and administrative measures for ensuring personal data security must be implemented. It was underlined that chatbots should comply with international standards, hold relevant certifications, and that privacy-by-design and privacy-by-default approaches should be considered at every stage of the development process. Furthermore, it was stated that secure methods should be preferred for transmitting inputs such as text, voice, and visual data to the environments where they will be stored.

1.6. Information Note on the Temporal Application of Misdemeanors

On 19 December 2024, the Authority published the "*Information Note on the Temporal Application of Misdemeanors*", addressing the time-based application of the framework of the Law Amendment dated 12 March 2024 to misdemeanors.

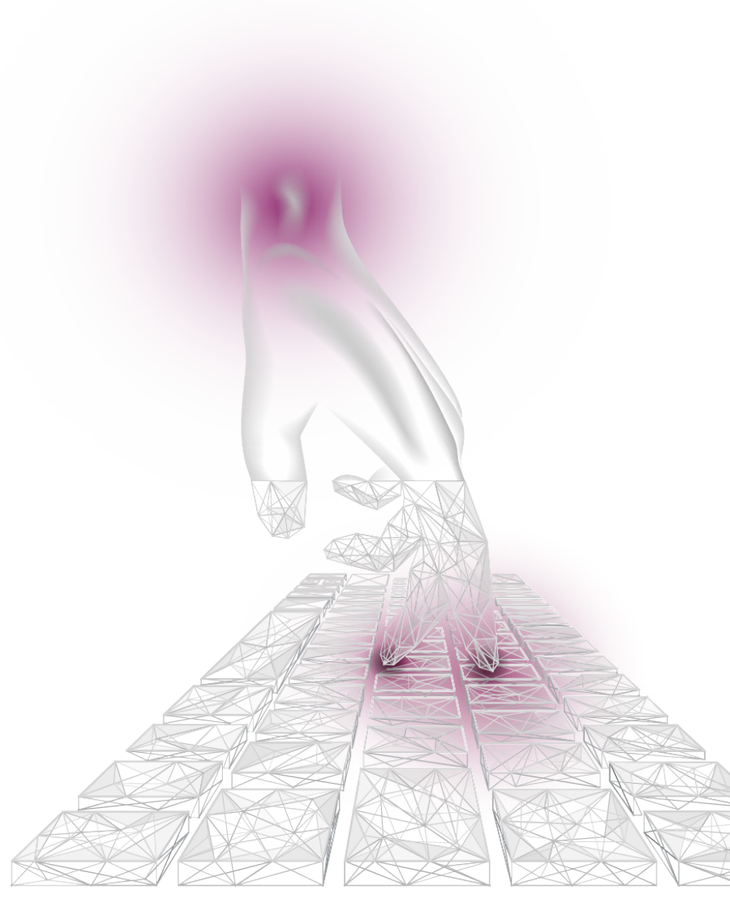
The Information Note emphasizes the importance of correctly determining the time of the act in the context of the DP Law's temporal application. According to Article 5/2 of Law No. 5326 on Misdemeanors ("**Misdemeanors Law**"), a misdemeanor is considered committed at the moment the offender performs the relevant act. Additionally, the same article of the Misdemeanors Law stipulates that the temporal application of a law must be evaluated within the principles outlined in the TPC. According to Article 7 of the TPC, which governs the principle of temporal application, the principle is to apply the law in effect at the time the offense is committed. However, if a newly enacted law includes provisions that are more favorable to the offender, the more ***favorable law*** is applied. The same approach is also adopted under Article 5 of the Misdemeanors Law. Additionally, it is stipulated that temporary laws apply only to acts committed during their effective period and are not applicable to acts committed before or after that period.

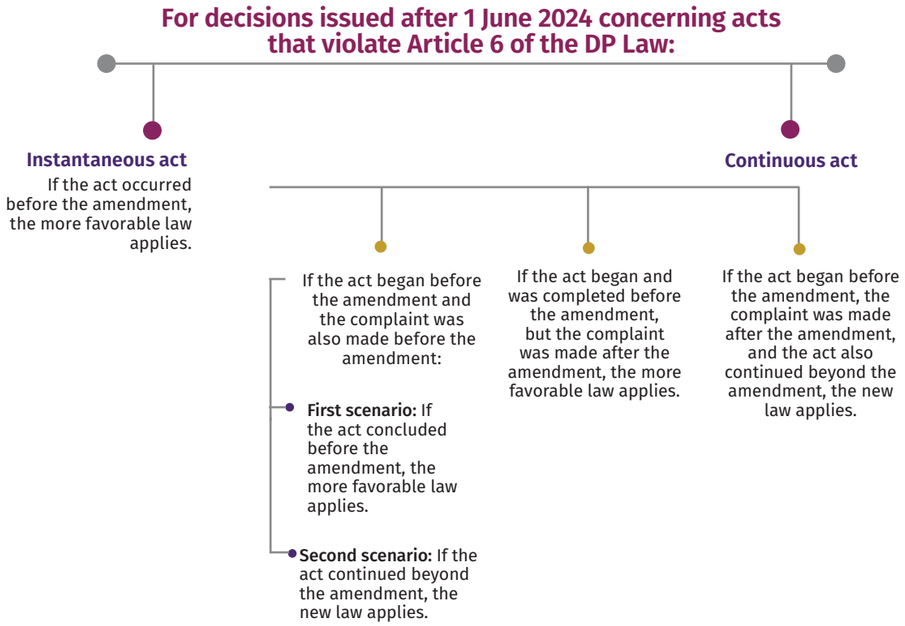
The Information Note also highlights a critical distinction for characterizing the exact time when an act is committed. This distinction arises from whether the acts are instantaneous or continuous in nature. Instantaneous acts refer to violations that occur at a single point in time, while continuous acts encompass violations that persist over a certain period. Within this context, the following points are emphasized:

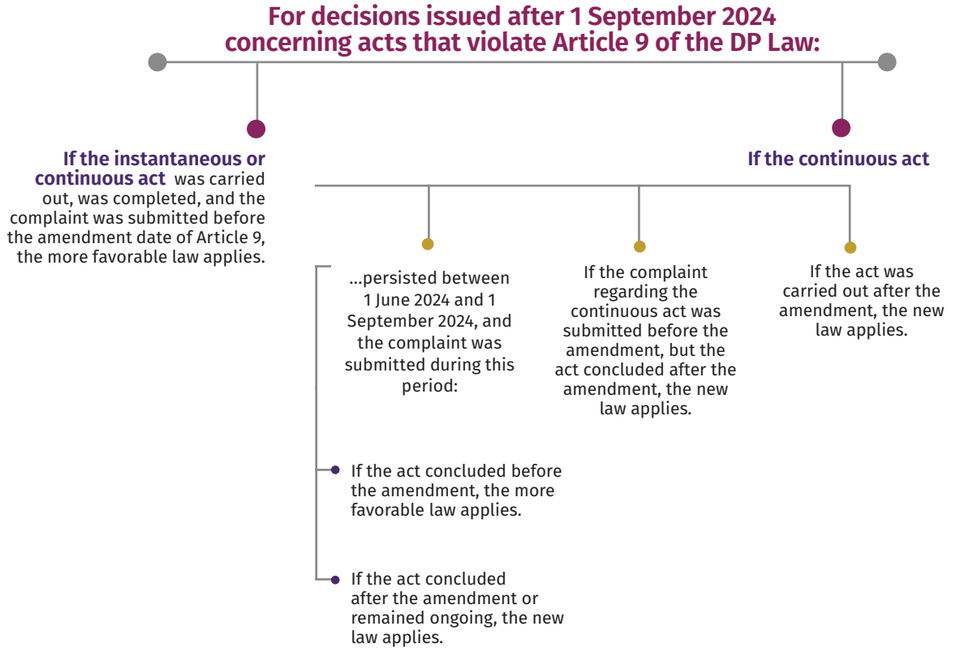
- For instantaneous acts, the law in effect on the date the act is committed is applied. If there is a provision more favorable to the offender, that provision may be applied.

- For continuous acts, all legal provisions in effect between the starting and ending dates of the act are considered. If the act concluded during the period of the former law, the former law applies; if it continued into the period of the new law, the new law applies. Indeed, Article 15 of the Misdemeanors Law stipulates that misdemeanors committed through continuous acts are considered as a single offense and are deemed ongoing until a definitive sanction is imposed.

Considering the distinctions outlined above, the Information Note provides the following conclusions regarding the temporal application of sanctions under the DP Law:







2. Bulletins

As of 2024, the Authority has published four KVKK Bulletins. The first of these, the October–December 2023 issue, No. 3 – "*Online Privacy and Cookies*," was shared with the public in 2024, and it covers the definition and historical development of cookies and digital fingerprint technology. The second bulletin, the January–March 2024 issue, No. 4 – "*Amendments to the Personal Data Protection Law*," provides a detailed explanation of the amendments made to KVKK Articles 6, 9, and 18 under the Law Amendment of 12 March 2024, as well as the legal basis of the obligation to inform. The third bulletin, the April–July 2024 issue, No. 5 – "*Privacy in the Digital Age: Protection of Children's Personal Data*," focuses on the protection of children's personal data, particularly the phenomenon of "Sharenting" and the measures that need to be taken to ensure children's privacy in the digital world. The latest published bulletin, the August–November 2024 issue, No. 6 – "*Personal Data Protection and Cybersecurity*," highlights cybersecurity issues, with an interview with the Cybercrime Department (SİBERAY) and a detailed examination of activities under the National Cybersecurity Strategy and Action Plan.

IV. Guidelines

1. Cross-Border Data Transfer Guidelines

The detailed regulations included in the guidelines have been discussed under Section A.II.1.2. Amendments Regarding Cross-Border Data Transfers and are not repeated here to avoid redundancy.

2. Guidelines on the Processing of Turkish Republic Identification Numbers

The "*Guidelines on the Processing of Turkish Republic Identification Numbers*" aim to define the legal obligations and principles that data controllers must follow when processing Turkish Republic Identification Numbers ("**ID numbers**"). When reviewing complaints and notifications submitted to the Authority, it was observed that there were claims of unlawful data processing directly related to the processing of ID numbers, which could negatively impact the right to protection of personal data. The Guidelines on the Processing of Turkish Republic Identification Numbers emphasize that, while ID numbers are not considered special category data, they hold significant importance among general personal data due to their ability to link to other personal data. As such, it is stressed that ID numbers should be processed in accordance with the principle of proportionality.

In accordance with the relevant regulations on the processing of ID numbers under the DP Law, the following explanations are provided:

a. Situations Where the Processing of ID Numbers is Required:

- **Invoice Issuance for Goods and Services Purchases:** According to Article 29/(a) of the Tax Procedural Law No. 213, an invoice is a commercial document issued in exchange for goods or services. Under Article 230/3, the invoice must include the customer's name, trade name, address, and other information. Since 2006, the tax identification numbers of individual taxpayers have been converted to ID numbers. According to Article 232/1, the issuance of invoices for goods and services sales is required, without any threshold for transactions. Additionally, the invoice must be issued if the commodity value exceeds TRY 4,400 or if the buyer requests an invoice. Furthermore, taxpayers must report certain purchases of goods and services exceeding a specified amount through the "Goods and Services Purchases Notification Form." In sales to the final consumer, the invoice does not need to include the ID number information.

MOROĞLU ARSEVEN

- **Order/Delivery of Cargo:** In remote shopping, during the cargo delivery, the law requires the recipient's name, surname, and ID number (or passport number or equivalent document number for foreign nationals) to be recorded by the cargo company representative.

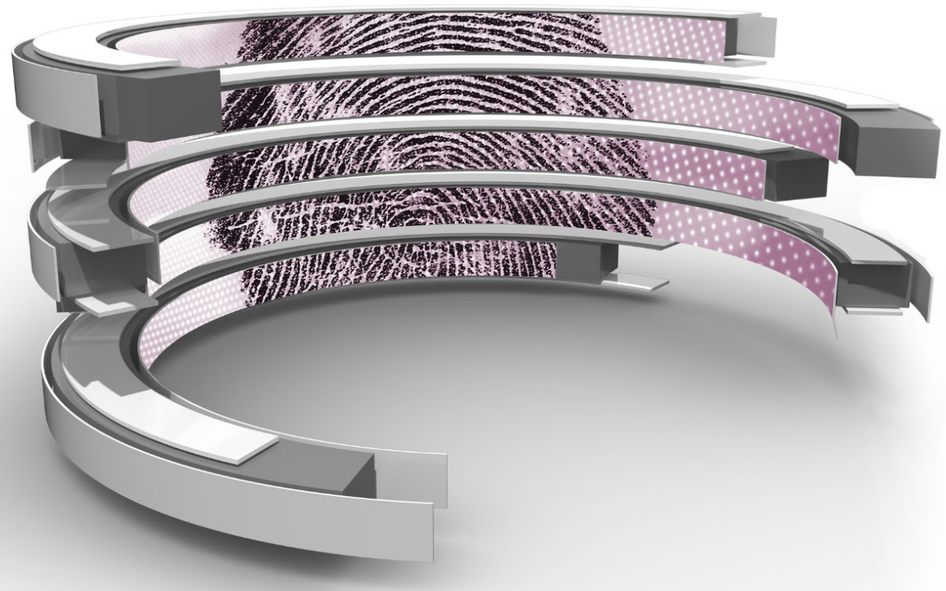
- **Delivery of Postal Shipments:** In the case of the sender and recipient being natural persons, the sender's ID number and the recipient's ID number must be processed. If the shipment is delivered by someone else, the ID number of the person delivering the package must also be recorded.

- **Complaint Applications to Electronic Commerce Intermediary Service Providers:** According to the Regulation on Electronic Commerce Service Providers and Intermediary Service Providers, the ID number of a complainant who is a natural person must be included in the complaint applications.

- **Sending Commercial Electronic Messages by Tradesmen:** According to the Regulation on Commercial Communication and Commercial Electronic Messages, the name, surname, and ID number of tradesmen must be included in the commercial electronic messages they send. For merchants, information such as the MERSIS number and trade name is also mandatory.

- **Complaints Regarding Commercial Electronic Messages by Natural Persons to the Ministry of Trade:** According to Article 14(2) of the Regulation on Commercial Communication and Commercial Electronic Messages, complaints regarding commercial electronic messages can be submitted through the following methods: (i) short message, (ii) email, (iii) voice call. These complaints must include the complainant's ID number. Article 12(1) of the same regulation emphasizes that service providers are responsible for protecting the data they collect, while Article 12(2) highlights that prior consent must be obtained for sharing personal data with third parties.

- **Registration in the Trade Registry and Certificate of Registry:** According to Article 16(1) of the Trade Registry Regulation, the ID number of natural persons must be included in the registration of a commercial enterprise. However, in accordance with Article 41 of the Trade Registry Regulation, these ID numbers will not be published. According to Article 49 of the Trade Registry Regulation, the ID number of the trader is required



for the registration of the commercial enterprise. In addition, according to Article 50, the name, surname, and ID number of the business owner and, if applicable, their representative, must be registered.

» In the registration of the commercial representative, their name, surname, ID number, and residence address must be provided.

» In the registration of association enterprises, the ID number of the authorized persons is required.

» Similarly, in the registration of foundation enterprises, the ID number of the authorized persons is required.

» For public legal entities and public benefit associations, the ID number of the authorized persons is required in their business registration.

» In the registration of a shipping company, the ID number of stakeholders and the ship manager is required.

» In the registration of collective and limited partnerships, the ID number and residence address of the partners are required.

» In the registration of joint-stock companies, the ID number of board members and authorized persons must be recorded.

» In limited companies, the ID number of the managers and authorized persons must be registered.

» The ID numbers of auditors of joint-stock and limited companies and corporate groups must be registered.

» In cooperatives, the ID numbers of the auditors and board members are required.

» For branches, the ID number of the persons authorized to represent the branch must be registered.

» In the registration of concordat terms and decisions, the ID number of the commissioner must be registered.

- **Posting of Voter Lists and Sharing with Political Parties Eligible to Participate in Elections:** According to Article 14 of Law No. 298 on the Basic Provisions of Elections and Voter Registers, the Supreme Election Council determines and announces the political parties eligible to participate in elections. Voter registers must be kept by the Supreme Electoral Board and made available on request by political party centers or authorized presidencies, provided that the cost required for access to these registers is deposited in the finance cashier.

- **Filing for Enforcement Proceedings:** According to Article 58 of the Enforcement and Bankruptcy Law No. 2004, the creditor's identification details, as well as the Turkish Republic ID number information of both the creditor and debtor, must be requested. Articles 94 and 95 of the Enforcement and Bankruptcy Law Regulation specify that creditors may obtain a certificate of inability to pay, which includes the debtor's ID number information.

- **Legal Transactions Conducted at Notaries:** According to Article 84 of Notary Law No. 1512, the identification details of the parties involved in legal transactions, especially their ID number, must be included. Notaries are required to record this information in legal documents.

- **Registration in the Land Registry:** Article 1002 of the Turkish Civil Code No. 4721 stipulates that registration processes in the land registry must be conducted with identification information. Therefore, the ID number of the parties involved must be recorded.

- **Filing Lawsuits, Appeals, and Other Petition Requests:** The Civil Procedure Law No. 6100 clearly states that the TCKN information of the parties involved must be included in legal documents such as lawsuits, appeals, and petitions for cassation.

- **Registration of Family Registers:** Article 7 of the Population Services Law No. 5490 requires the maintenance of separate family registers for each neighborhood or village, and it mandates that the ID number be included in these registers.

- **Divorce or Marriage Annulment:** Article 27 of the Population Services Law No. 5490 requires the inclusion of the parties' ID number in decisions regarding divorce or annulment of marriage.

- **Identification Documents Issued to Individuals:** Article 47 of the Population Services Law No. 5490 stipulates that the ID number must be included in identification documents (such as identity cards, driver's licenses, etc.) issued to individuals.

- **Sharing of Identity Information by the Ministry of Interior under Law No. 5490:** Article 45 of the Population Services Law No. 5490 states that the Ministry of Interior may share identity data with various public service providers and certain official institutions.

- **Identity Sharing System (*Kimlik Paylaşımı Sistemi "KPS"*):** Article 6 of the Identity Sharing System Regulation mandates compliance with legal provisions related to privacy in the operation of the system. According to Article 8 of the Identity Sharing System Regulation, the ID number is included in the KPS database, and this information can be transmitted to recipient institutions according to the existing legislation and agreements. The Ministry of Interior states that identity data can be queried using the ID number, and it specifies which institutions are authorized to perform such queries, with system log records being retained for at least eight years. Authorized institutions commit to using the system in compliance with Article 20 of the Constitution and the DP Law.

- **Use of the "White Code" by Doctors and Healthcare Workers:** The White Code Usage Process Guide ensures that incidents of violence against healthcare workers are recorded. The identity information (or description) of the perpetrator must be included in the incident report and entered into the system. The ID number of those making the complaint must be processed during the White Code call. Additionally, if the perpetrator's identity information is available, it should be included in the report.

- **Transactions of Insured Persons under Social Security and General Health Insurance:** Article 92 of the Social Security and General Health Insurance Law No. 5510 mandates the use of ID numbers as the social security registration numbers for Turkish citizens. According to Temporary Article 11, a unified information database will be established for currently insured persons, and TCKN information will be used in this process.

- **Establishment of Unions:** Article 8 of the Trade Unions and Collective Bargaining Law No. 6356 requires the inclusion of the ID number of the founders in the union's founding statute.

- **Issuance of Airline Tickets:** According to the Turkish Civil Aviation Law No. 2920, information about individuals traveling by air can be processed for security and risk assessment purposes. Airlines issuing e-tickets are required to include the passenger's ID number on the ticket. Furthermore, the tax or ID number of the taxpayers should also be displayed on the ticket.

- **Scheduled/Non-Scheduled Passenger Transport and Ticketing on Highways:** The Road Transport Regulation requires that a ticket be issued for each passenger in a scheduled

passenger transport, and the ID number of the passenger must be included on the ticket. For non-scheduled transport, it is also stated that the ID number of passengers must be written in transport contracts.

- **Cargo Transport on Highways and Obtaining and Renewing Authorization Certificates:** According to the Road Transport Regulation, the transportation document issued for cargo transportation must include the ID number of the natural person responsible for the transport. Additionally, a declaration of the ID number is required in the documents for obtaining and renewing authorization certificates.

- **Ticketing for Travel, Events, and Sports Competitions:** E-ticket issuers are required to include the TCKN information of both the passenger and, if applicable, the taxpayer on the tickets. For passenger transport tickets, if the person holding the authorization certificate is a natural person, the ID number of the certificate holder must be included, and, if the passenger is a Turkish citizen, the passenger's ID number must also be included. Additionally, for sports competitions, individuals wishing to purchase tickets must have their identity information, along with their photos, on an electronic card.

- **Bulk Customer Acceptance for Salary Payments:** According to the General Communiqué of the Financial Crimes Investigation Board, public administrations under general management, professional organizations with the status of public institutions, or institutions, organizations, or businesses employing more than 100 personnel must collect ID numbers from individuals for salary payments. This information is verified through KPS or other methods. The same regulations apply to bulk salary payments made to international organizations.

- **Prevention of Money Laundering from Criminal Proceeds:** Before carrying out transactions, obligated parties under Law No. 5549 on the Prevention of Money Laundering must identify the individuals performing the transactions and the individuals whose accounts are involved in the transactions. The documents required for identity verification and the circumstances under which identification should be made are determined by the Ministry of Treasury and Finance. Additionally, under the relevant law, institutions recording economic events and illegal activities, as well as public institutions, may grant access to their information systems to the Financial Crimes Investigation Board ("**MASAK**"). According to the Regulation on Measures for the Prevention of Money Laundering and Terrorism Financing, the obligated parties must identify the customer or those acting on their behalf and confirm the accuracy of their identity information in the following circumstances:.
  - When establishing a continuous business relationship, if there are doubts about the adequacy and accuracy of previously obtained identity information, and when a suspicious transaction report is required, without regard to the amount.
  - When the transaction amount or the total amount of several connected transactions is TRY 185,000 or more, or, in the case of electronic transfers, when the transaction amount or the total amount of several connected transactions is TRY 15,000 or more.

- **Data Sharing Among Members of the Turkish Banks Association Risk Center:** According to the Turkish Banks Association Risk Center Regulation, credit institutions are required to report the identity information of individual customers with debts to be liquidated to the Risk Center. Additionally, credit limit and credit risk information for each customer may also be shared.

- **Number Portability Transaction:** The Number Portability Regulation states that the subscriber's number and identity information must be provided to the receiving operator. The receiving operator verifies the accuracy of this information by comparing it with the current operator. For individual subscribers, it is also mandatory to collect the ID number.

- **Working or Becoming a Member at Gyms/Facilities:** According to the Private Physical Education and Sports Facilities Regulation, a sporting facility owner must maintain a registry containing identity and contact information. It is required to collect ID number information from those who will become members of the facility.

b. Cases Involving the Presentation, Display, or Reporting of Documents Containing ID Numbers or Identity Information:

- **Participation in the General Assembly of the Company with Shares:** Under Article 415 of the TCC, individual shareholders attending the general assembly must present their identity. In general assemblies held electronically, the participants' identity information is kept for ten years, maintaining confidentiality and integrity.

- **Distance Contracts:** Under Article 5 of the Distance Contracts Regulation, the identity of the seller or provider must be disclosed to the consumer before the contract. Additionally, their identity must be announced at the beginning of each telephone conversation, and each transaction must be documented.

- **Voting in General and Local Elections:** Under Article 87 of the Basic Provisions on Elections and Voter Registers Law No. 298, the identities of voters must be verified with official documents. Valid documents are announced by the Supreme Election Board.

- **Voting in the Selection of Chambers of Commerce and Exchanges:** Under Article 81 of the Chambers of Commerce and Commodity Exchanges Law No. 5174, to vote, the voter's identity must be verified with a document, and the voting ballot must be signed.

- **Voting in Union Elections:** Under Article 14 of the Trade Unions and Collective Bargaining Law No. 6356, those voting at the General Assembly must show an official identity document and sign the list.

- **Notification of Union Representative's Identity to Employer:** Under Article 27 of the Trade Unions and Collective Bargaining Law No. 6356, the workplace representatives of the authorized union must notify their identity to the employer.

- **Identity Verification Procedures Performed by Notaries:** Under Article 61 of Notary Law No. 1512, notaries must verify identities and statements.

- **Identity Verification Procedures at Healthcare Service Providers:** Under Article 67 of the Social Insurance and General Health Insurance Law No. 5510, the identities of individuals under the age of 18 must be verified when receiving healthcare services.

- **Identity Verification and Reporting in Accommodations, Workplaces, Dormitories, and Residences:** Under the Law on Identity Reporting No. 1774, the identities of employees and residents in accommodations and workplaces must be regularly reported.

- **Electronic Payment Service:** Under Article 12 of Law No. 6493, information systems necessary for customer identity verification must be used during electronic payments. During identity verification, the use of a Turkish ID card, card PIN, or biometric data together; a secure electronic signature; or passwords accessible through the Mobile Application PIN are considered "strong authentication." In such cases, the requirements of the provision will be deemed fulfilled.

- **Identity Verification in the Electronic Communication Sector:** Identity verification is required in certain transactions within the electronic communication sector. One of the methods of identity verification is specified as creating a PAdES (electronic signature) along with the Turkish ID card.

- **Betting on Sports Matches and Winning Prizes:** The identities of individuals placing bets must be determined, and the prize must be paid accordingly. Identification is a requirement for prize payments.

- **Winning Prizes in National Lottery Draws:** According to the National Lottery Administration, the winner's identity must be determined through official documents, and an identity slip must be issued for the prize payments.

- **Police Authority to Request Identity:** The police and watchmen have the authority to request identification when there is a reasonable cause.

- **Biometric Identity Verification in Private Hospitals:** To prevent potential abuses and fraudulent activities in which individuals who have not received treatment are falsely represented as having received treatment to obtain payments from the Social Security Institution ("SSI"), biometric methods for identity verification have been made mandatory for individuals applying to private hospitals under a contract with an SSI. This practice was suspended in 2020 due to the COVID-19 pandemic, and SGK has set the deadline for its resumption as 1 January 2024.

  - Article 26 of the General Health Insurance Implementation Regulation requires contracted healthcare providers to conduct identity verification using biometric methods, except in emergency situations, and to present one of the identity documents.

  - According to Article 1/6 of the Social Security Institution Health Application Communiqué, identity verification must be carried out using biometric methods and one of the identity documents, with the exception of emergencies, in which case the verification should be completed once the emergency situation has ended.

3. Personal Data Protection Guide on Election Activities

On 24 January 2024, the Authority published the "*Personal Data Protection Guide on Election Activities*" ("**Guide on Election Activities**") on its official website. The Guide on Election Activities provides a detailed explanation of the legal framework regarding the processing of personal data in election processes. The key points are as follows:

- It is stated that election activities such as voter registry management, candidate nomination, publication of candidate lists, election campaigning, public opinion surveys, and voting, along with the personal data processing activities of public institutions, political parties, and independent candidates, must comply with the DP Law and other relevant legal regulations.

- The Guide on Election Activities clarifies that the Supreme Election Council ("**YSK**"), political parties, and independent candidates are considered "data controllers."

- As the YSK is legally responsible for managing and overseeing elections, it is stated that, in accordance with Article 28/2 of the DP Law, the personal data processed by the YSK in the course of election activities falls under an exemption, meaning that certain provisions of the DP Law, including the obligations under Article 10 (*regarding the obligation to inform*), Article 11 (*except for the right to request damage compensation*) and Article 16 (*regarding the obligation to register in the VERBIS*), do not apply to the YSK's activities related to managing and overseeing elections. However, it is emphasized that this exemption is partial, and the YSK must comply with the other provisions of the DP Law. Similarly, political parties and independent candidates must fulfill their legal obligations as data controllers in the processing of personal data.

- It has been emphasized that the conditions specified in DP Law Articles 5 and 6 must be followed for the processing and transfer of personal data, and the processing conditions for various election activities have been discussed in detail with examples for each data controller (*YSK, Political Parties, and Independent Candidates*)

- The Guide on Election Activities provides explanations on the general principles to be followed for personal data processing (*legality and fairness, accuracy and up-to-date information, processing for specific, clear, and legitimate purposes, processing being relevant, limited, and proportionate to the purposes, and retention for as long as required by the applicable law or for the purpose they were processed*). The Guide emphasizes that data controllers must act in accordance with these principles during the election processes.

- The responsibilities of data controllers are discussed in detail in the Guide on Election Activities:

  - **Obligation to Inform:** The YSK, which is responsible for the administration and supervision of elections, is exempt from the obligation to inform under Article 28/2 of the DP Law for personal data processing activities related to election activities. However, political parties and independent candidates must fulfill the obligation to inform in accordance with DP Law.

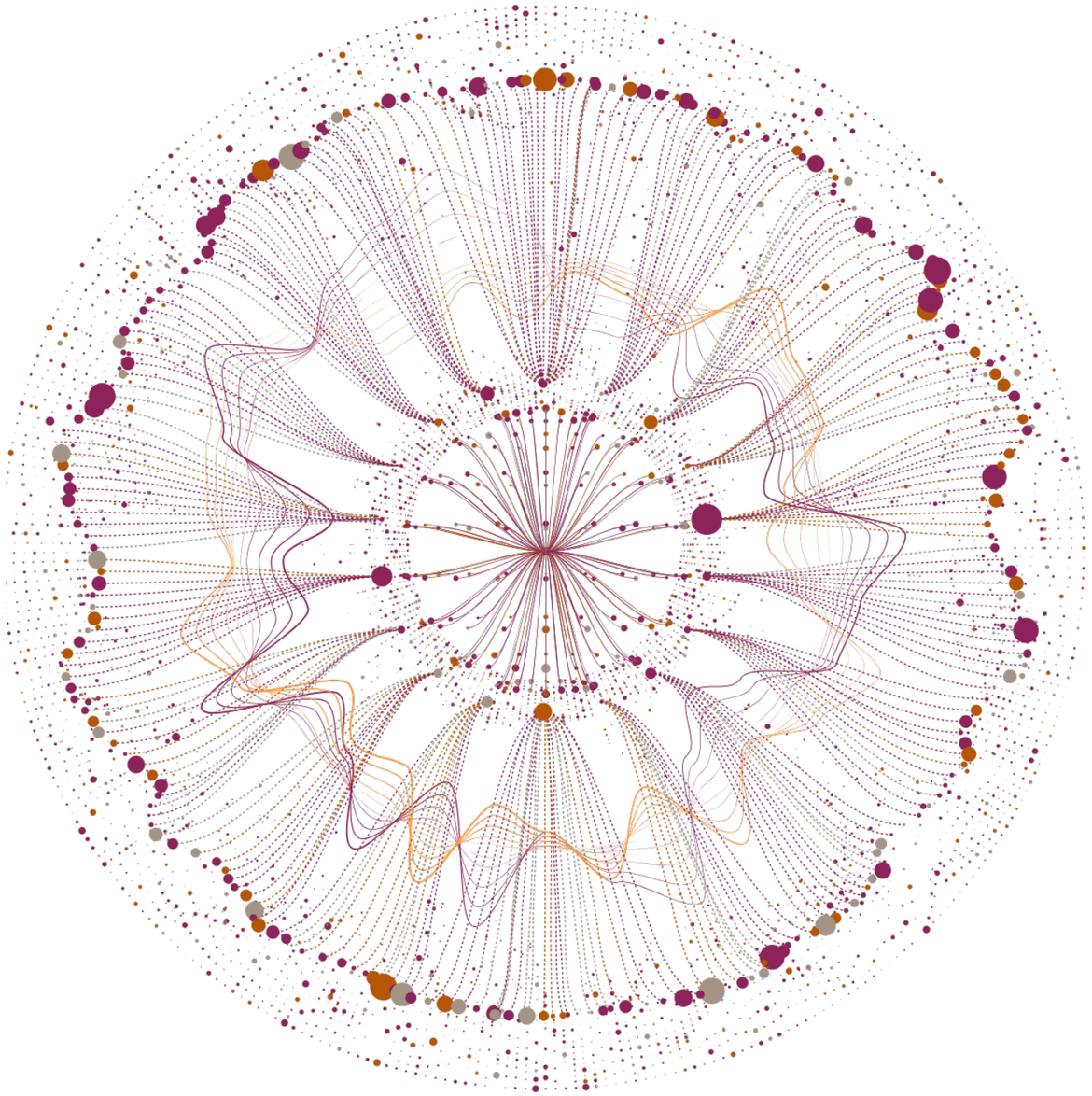
  - **VERBIS Registration Obligation:** The YSK is exempt from the VERBIS registration obligation under Article 28/2 of the DP Law for personal data processing activities related to election activities. Similarly, political parties are also exempt from the VERBIS obligation under the Board's decision dated 2 April 2018, number 2018/32.

  - **Data Security:** All data controllers must comply with the data security obligations under Article 12 of the DP Law.

  - **Obligation to Delete, Destroy, or Anonymize:** All data controllers must delete, destroy, or anonymize data, either ex officio or on request of the data subject, using appropriate methods.

- Regarding the rights of data subjects, it has been emphasized that data subjects can exercise their rights under DP Law Article 11 and communicate them to the data controller in accordance with DP Law. It is also stated that the YSK, under DP Law Article 28/2, is exempt from the provisions of DP Law Article 11, except for the right to request the rectification of damage. However, the obligations under the legislation applicable to the YSK remain intact.

MOROĞLU ARSEVEN



4. Corporate Social Media Use Guidelines for Public Institutions

On 10 October 2024, the "*Corporate Social Media Use Guidelines for Public Institutions*" were published by the Communications Directorate. The guidelines provide essential principles and recommendations for public institutions and their staff to use social media platforms consciously, effectively, and responsibly. The guidelines aim to raise awareness not only about the use of social media accounts specific to the public institution but also regarding the use of personal accounts by public employees.

In this regard, the guidelines highlight the obligations of public employees under various legal frameworks on both personal and institutional social media accounts. Particular emphasis is placed on data protection laws in relation to social media use; it is advised that personal data should not be shared, and principles such as transparency, proportionality, and accountability should be followed. Furthermore, issues regarding the security of social media accounts are discussed, with visual examples provided, highlighting necessary measures such as password security, two-factor authentication, and regular checks of privacy settings to ensure data security.

The guidelines also emphasize social media crisis management, combating misinformation, and the importance of ethical principles in content sharing. It is suggested that visuals created with artificial intelligence should include the label "created with artificial intelligence," and guidance is provided on using reverse search engines to verify the accuracy of news and images before sharing them on social media accounts. Additionally, the risks associated with VPNs and other communication applications, commonly used today for accessing content contrary to decisions made by public authorities, are highlighted, underscoring the importance of developing local and secure communication platforms.

5. Draft Guidelines

The Authority has not shared any draft guidelines with the public as of the end of 2024. The draft Guidelines on Loyalty Programs within the scope of Personal Data Protection Legislation, dated 16 June 2022 from the previous year, are still in the draft stage and have not been finalized by the Authority and shared with the public.

[4] Detaylar için bkz. https://www.morogluarseven.com/wp-content/uploads/2023/05/KVKK-Round-Up-2023-Vol2_TR-1.pdf

MOROĞLU ARSEVEN

V. Public Announcements Made by the Authority in 2024

1. Transfer of Financial Account Data of Turkish Citizens Abroad

On 17 Jan 2024, the "*Public Announcement on Requests by Turkish Citizens Residing Abroad Regarding the Non-Disclosure of Their Financial Account Data to Foreign Jurisdictions*" was published on the Authority's official website. Various petitions submitted to the Authority by Turkish citizens residing abroad stated that inquiries had been made under the DP Law to the Turkish Revenue Administration and the banks holding their financial account information to ascertain whether such data had been transferred to foreign authorities. However, the responses received were considered insufficient, leading to a request for the necessary actions to be taken under the DP Law. Following its examination, the Board reached the following conclusions:

- The transfer of financial account data to foreign jurisdictions is permissible under the framework of the Convention on Mutual Administrative Assistance in Tax Matters, signed by OECD member states, including Türkiye, on 3 November 2011 and subsequently ratified through Law No. 7018 on 3 May 2017. Furthermore, such transfers are also governed by the Multilateral Competent Authority Agreement on the Automatic Exchange of Financial Account Information, signed in 2017 and published in the Official Gazette No. 30995 dated 31 December 2019.

- In Türkiye, the Revenue Administration, operating under the Ministry of Treasury and Finance, has been designated as the competent authority authorized to collect and share information for the purposes of automatic information exchange under the Multilateral Competent Authority Agreement on the Automatic Exchange of Financial Account Information. Furthermore, pursuant to Article 152/A of the Tax Procedure Law, the Revenue Administration is expressly authorized to collect data subject to information exchange under the aforementioned agreement.

- Under Article 9/5 of the DP Law, personal data may only be transferred abroad with the permission of the Board and after obtaining the opinion of the relevant public institution or organization, provided that international agreements remain unaffected, in cases where such transfer would significantly harm Türkiye's or the data subject's interests. Furthermore, under Article 9/6 of the DP Law, it is stipulated that, where international agreements are applicable, personal data may be transferred abroad without seeking the explicit consent of the data subject or requiring the Board's approval, as long as the transfer occurs within the framework of those agreements.

- Additionally, under Article 90 of the Constitution, international agreements duly ratified and brought into force carry the force of law. Accordingly, it has been assessed that data transfers abroad under the Multilateral Competent Authority Agreement on the Automatic Exchange of Financial Account Information would not constitute a violation of Article 9 of the DP Law. Furthermore, in cases where the processing of personal data is necessary for the protection of the state's economic and financial interests in relation to budgetary, tax, or financial matters, Article 28/2(ç) of the DP Law stipulates that the provisions of Article 11 of the DP Law, which regulate the rights of the data subject, shall not apply.

- In conclusion, issues concerning automatic data sharing are regulated under the Multilateral Competent Authority Agreement on the Automatic Exchange of Financial Account Information, and personal data transfers to foreign jurisdictions carried out in accordance with the provisions of international agreements are compliant with the law.

2. Amendments to the DP Law

On 12 March 2023, the Authority issued a public announcement on its official website regarding the Law Amendment, specifying that the amendments would take effect on 1 June 2024. Additionally, it was noted that Article 9/1 of the DP Law, which governs the procedures and principles for the transfer of personal data abroad, would continue to apply in its revised form until 1 September 2024.

3. Draft Regulation Regarding the Procedures and Principles for the Transfer of Personal Data Abroad

On 9 May 2024, the "*Public Announcement on the Draft Regulation Regarding the Procedures and Principles for the Transfer of Personal Data Abroad*" was issued. Through this announcement, the Draft Regulation on the Procedures and Principles for the Transfer of Personal Data Abroad, along with its General Justification and Feedback Form, was shared and opened for public consultation until 20 May 2024.

4. Documents Related to Data Controllers and Data Processors

On 10 July 2024, the "*Public Announcement on Documents Related to Standard Contracts and Binding Corporate Rules*" was published on the Authority's official website. Accordingly, the SCCs and BCRs documents to be used for the transfer of personal data abroad, reflecting the amendments to Article 9 of the DP Law, were approved by the Board through its Decision No. 2024/959, dated 4 June 2024, and shared with the public.

The following is the list of documents that have been approved and published:

- *Standard Contract for the Transfer of Personal Data Abroad -1 (Controller to Controller)*
- *Standard Contract for the Transfer of Personal Data Abroad - 2 (Controller to Processor*
- *Standard Contract for the Transfer of Personal Data Abroad - 3 (Processor to Processor)*
  Standard Contract for the Transfer of Personal Data Abroad - 4 (Processor to Controller)
- *Application Form for Binding Corporate Rules for Data Controllers*[13]
- *Key Considerations for Binding Corporate Rules for Controllers – Supporting Guide*[14]
- *Application Form for Binding Corporate Rules for Data Processors*[15]
- *Key Considerations for Binding Corporate Rules for Processors – Supporting Guide*[16]

On 29 August 2024, the Authority announced on its official website that the English translations of the Regulation and the SCCs were shared with the public through the "*Announcement on the English Translation of the Regulation on the Procedures and Principles for the Transfer of Personal Data Abroad and Standard Contractual Texts*."

5. VERBIS

On 1 August 2024, the "*Public Announcement (on the Data Controllers' Registry)*" was published on the Authority's official website. The announcement stated that, out of approximately 130,600 data controllers identified as having an obligation to register and notify VERBIS, around 16,350 data controllers were found to have failed to fulfill this obligation. It was further noted that the Board has been conducting VERBIS reviews pursuant to Article 18 of the DP Law regarding these data controllers. As a result of these reviews, administrative fines continue to be imposed based on an algorithm table prepared according to the annual financial balance sheet totals of the data controllers.

As a result of these reviews, it was stated that, as of 1 August 2024, the Board had imposed administrative fines amounting to TRY 503,935,000 on domestic and foreign natural and legal person data controllers who failed to comply with their obligation to register and notify VERBIS, despite being subject to this requirement. Furthermore, disciplinary provisions were applied to public institutions, organizations, and professional associations with the status of public institutions.

[13] Only available in Turkish.
[14] Only available in Turkish.
[15] Only available in Turkish.
[16] Only available in Turkish.

MOROĞLU ARSEVEN

6. Personal Data Processing Activities of Research Companies in the Scope of Random Number Dialing

On 26 August 2024, the "*Public Announcement on Personal Data Processing Activities Carried Out by Research Companies Using the "Random Digit Dialing Telephone Interview Method" for Statistical Research Purposes*" was published on the Authority's official website.

In several complaints submitted to the Authority, it was alleged that data subjects were contacted by research companies for statistical research purposes, despite never having shared their phone numbers. It was further noted that no information was provided during these calls regarding how the phone numbers were obtained. On inquiries being directed to the data controllers, data subjects were informed that the phone numbers had been generated randomly and automatically through a system or software, and that the method employed for the calls was a globally recognized statistical methodology known as the "*random digit dialing telephone interview*" method. Additionally, it was asserted that explicit consent was not obtained for the processing of phone numbers, nor was the processing based on any of the other legal bases stipulated in Article 5 of the DP Law. The Board has conveyed its assessments as follows:

- Article 28/1(b) of the DP Law stipulates that the provisions of the DP Law do not apply in cases where "*personal data is processed for purposes such as research, planning, and statistics by rendering it anonymous or for official statistical purposes.*" However, it was noted that the studies conducted by research companies do not serve the purpose of official statistics and do not involve the processing of data in an anonymous manner.

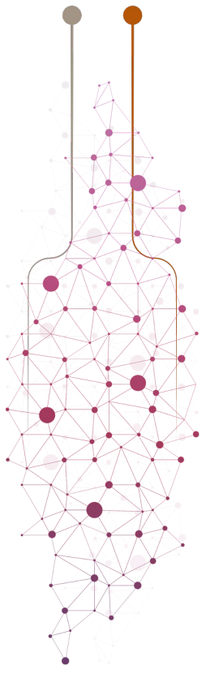
- In the incident subject to the complaint, it was reported that, during telephone surveys conducted by research companies, the explicit consent of data subjects was obtained prior to proceeding with the survey, and interviews were terminated if consent was not provided. However, even in cases where explicit consent was withheld, telephone conversations were recorded, traffic logs were maintained, and the data were stored for two years using pseudonymization methods. It was emphasized that the data were not anonymized and, as such, retained their status as personal data, necessitating strict compliance with the provisions of the DP Law.

The public announcement underscored the following obligations for research companies processing personal data:

- Data controllers are required to implement appropriate technical and administrative measures to ensure compliance with the DP Law and to safeguard personal data. It was emphasized that these measures should adhere to the principles of "data protection by design" and "data protection by default." Furthermore, it was stated that the default settings of the software used by the data controller must be configured to perform only the activities necessary for the intended purpose of data processing.

- Under Article 5/2(f) of the DP Law, for personal data to be processed based on the legitimate interests of the data controller (*without relying on explicit consent as a legal basis*), the data controller must:
  - » Ensure that the legitimate interest pursued through the processing of personal data is balanced against the fundamental rights and freedoms of the data subject.
  - » Verify that the processing of personal data is necessary to achieve the intended legitimate interest.
  - » Establish that the legitimate interest is existing, specific, and explicit.
  - » Demonstrate that achieving the legitimate interest, which competes with the fundamental rights and freedoms of the data subject, provides a tangible benefit, and that such a benefit cannot be achieved through other means or methods without processing personal data.
  - » Ensure that the legitimate interest meets transparent and accountable criteria, such as having a broad impact on the organization as a whole rather than a single unit or a limited number of data subjects, avoiding a sole focus on profit-making or economic gain, and facilitating business processes or operations (*e.g., affecting the organization broadly rather than at the level of a single department or a small group of employees*).
  - » Protect the data subject from any foreseeable, clear, and immediate risks that may harm their fundamental rights and freedoms, particularly their right to personal data protection.
  - » Guarantee that the processing of personal data complies with lawful processing principles, supported by all necessary technical and administrative measures to prevent harm and violations.
  - » Ensure that the processing adheres to the general principles governing personal data processing.
  - » Conduct a balance test to evaluate the fundamental rights and freedoms of the data subject against the legitimate interests of the data controller.

In conclusion, it was determined that the telephone numbers used in public opinion research were generated through the "random digit dialing telephone interview" method and not obtained from any other source, and that the generated numbers were not visible to the personnel conducting the interviews. Furthermore, it was noted that the processing



of personal data commenced upon the dialing of the data subject's telephone number. In this data processing activity, personal data processing operations, to the extent necessary and limited in scope, include recording the date and duration of calls made to the data subject, maintaining traffic logs in the form of calling and called numbers, processing the phone numbers of data subjects who requested not to be contacted again into a do-not-call list, and recording the audio of interviews. These activities may be deemed lawful under "the legitimate interest of the data controller" when carried out for purposes such as **(i)** *conducting quality control audits for the research,* **(ii)** *ensuring the researcher fulfills their obligations,* and **(iii)** *demonstrating compliance with obligations in the event of legal disputes*.

- It has been emphasized that, at the initial point of contact with data subjects, at a minimum, they must be informed about the identity of the entity conducting the call, the categories of personal data being processed (including, if applicable, a clear indication that the call is being recorded, along with details on all other processed data such as the phone number and call traffic logs), the fact that their phone number was generated through the random digit dialing method, and the purpose of the processing. Additionally, it was stated that a layered approach to transparency could be implemented by providing access to further details contained in the information notice via a specified channel.

- In conclusion, research companies must fulfill their obligation to inform the data subject before commencing the interview. It was further noted that (i) in cases where explicit consent is not provided, personal data processed up to that point (e.g., requests not to be contacted again, call date or duration, call traffic logs, or the recording of the conversation) may be processed under the legitimate interest of the data controller, and (ii) where explicit consent is given, the telephone interview may continue, and personal data may be processed within the scope of the research.

7. The Compromise of Personal Data of 108 Million Citizens

Following reports on various news outlets and social media platforms alleging the unauthorized access to personal data of 108 million citizens, the Board issued a public announcement on 13 September 2024.

The Board stated that, despite the reports of unauthorized access to the data of 108 million citizens, it had not received any data breach notifications. It also announced that, due to similar reports that had surfaced previously, a proactive investigation had already been initiated and was ongoing within this scope.

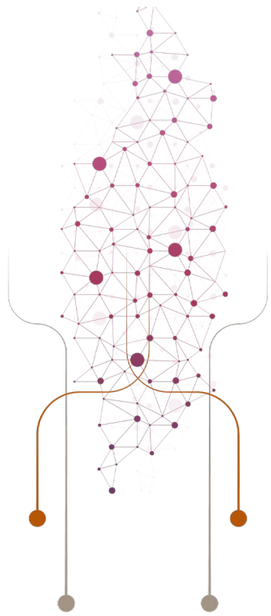
8. SS Notification Module

Article 9/5 of the DP Law stipulates that SCCs must be notified to the Authority within five business days of their execution. Notification methods include physical mail, KEP, and other methods determined by the Board. On 25 October 2024, through the "*Public Announcement on the Standard Contract Notification Module*" published on the Authority's official website, the Board announced that the "Standard Contract Notification Module" had been launched on 17 October 2024 to enable faster and more efficient submission of such notifications.

The Standard Contract Notification Module Guide was published simultaneously with the launch of the Standard Contract Notification Module and made available to the public on the module's homepage. This guide provides a comprehensive resource to ensure that SCCs, prepared by users for their data transfer activities abroad are submitted accurately and systematically through the module. Within this scope, data controllers or data processors intending to submit notifications must first register with the system, then log in to assign an "authorized person." The assigned authorized person will complete the notification process on behalf of the parties by submitting the necessary information through their account. Through the account of the assigned "authorized person," various actions can be performed, including adding, editing, or deleting SCCs parties, as well as adding, editing, or deleting SCCs documents. From the accounts belonging to data controllers and data processors, only specific actions are permitted, such as updating account information, assigning authorized persons, and viewing SCCs submitted by the assigned authorized persons.

9. Fulfillment of the Obligation to Inform in Mediation Activities

On 13 January 2024, the "*Public Announcement on Fulfilling the Obligation to Inform Within the Scope of Mediation Activities*" ("**Mediation Public Announcement**") was published on the Authority's official website. Through the Mediation Public Announcement, explanations were provided regarding the application of the DP Law to mediation activities carried out under Law No. 6325 on Mediation in Civil Disputes ("**Law No. 6325**").



Law No. 6325 regulates the definition of a mediator and the procedures and principles governing mediation activities. Article 11 of Law No. 6325, titled "*Informing of the Parties,*" stipulates that "At the beginning of the mediation process, the mediator is obliged to adequately inform the parties about the principles, process, and outcomes of mediation." However, the obligation to inform the parties under Law No. 6325 differs from the obligation to inform in relation to the processing of personal data under Article 10 of the DP Law. Therefore, it has been stated that the information provided under Law No. 6325 cannot be interpreted as fulfilling the obligation to inform under the DP Law. Consequently, mediators must separately fulfill their obligation to inform regarding personal data processed during mediation activities by providing information in accordance with the requirements set out in Article 10 of the DP Law.

MOROĞLU ARSEVEN

VI. Other Activities of the Authority

1. Important Announcements

This section includes announcements published on the Authority's official website that have a significant impact on the procedures and principles governing the protection of personal data.

1.1. Administrative Fines

On 3 January 2025, the Authority published on its official website the updated administrative fine amounts stipulated under Article 18 of the DP Law, which were increased for 2025 in accordance with Article 17/7 of the Misdemeanor Law and the provisions of Article 298 of the Tax Procedure Law (Law No. 213) on revaluation. The revaluation rate for 2025 was announced as 43.93%. Details are provided in the table below:

DP Law Article	DP Law Article Constituting the Violation	Explanation	Fine Amount for 2025
18/a	10	Failure to Fulfill the Obligation to Inform	TRY 68,083 – TRY 1,362,021
18/b	12	Failure to Fulfill Data Security Obligations	TRY 204,285 – TRY 13,620,402
18/c	15	Failure to Comply with Board Decisions	TRY 272,380 – TRY 13,620,402
18/ç	16	Non-Compliance with VERBIS Registration Obligation	TRY 340,476 – TRY 13,620,402
18/d	9	Failure to Notify the Board of SCCs	TRY 71,965 – TRY 1,439,300

1.2. Announcements on Commitment Applications

In 2024, the Board finalized three commitment applications, which were officially announced on the Authority's website:

- On 28 May 2024, it was announced[17] on the Authority's official website that the commitment application submitted by Huawei Telekomünikasyon Dış Ticaret Limited Şirketi regarding the transfer of personal data abroad had been finalized, and the Board granted permission for the data transfer on 28 May 2024.
- On 2 May 2024, it was announced[18] on the Authority's official website that the commitment application submitted by Bosch Termoteknik Isıtma ve Klima Sanayi ve Ticaret Anonim Şirketi regarding the transfer of personal data abroad had been finalized, and the Board granted permission for the data transfer on 2 May 2024.
- On 29 January 2024, it was announced[19] on the Authority's official website that the commitment application submitted by Celltrion Healthcare İlaç Sanayi ve Limited Şirketi regarding the transfer of personal data abroad had been finalized, and the Board granted

1.3. Announcement on the English Translation of the Regulation on the Procedures and Principles for the Transfer of Personal Data Abroad and SS Texts

On 29 August 2024, the Authority announced on its official website that the English translations of the Regulation on the Procedures and Principles for the Transfer of Personal Data Abroad and the SCCs were shared with the public through the "*Announcement on the English Translation of the Regulation on the Procedures and Principles for the Transfer of Personal Data Abroad and Standard Contractual Texts*."

[17] Only available in Turkish.

[18] Only available in Turkish.
[19] Only available in Turkish.

2. Collaborations

2.1. Collaboration Protocol with Selçuk University

On 6 May 2024, it was announced on the Authority's official website that a Collaboration Protocol[20] had been signed between the Authority and Selçuk University to facilitate cooperation on various topics related to the protection of personal data.

2.2. Collaboration Protocol with the Turkish Republic of Northern Cyprus

On 18 April 2024, it was announced on the Authority's official website that a Collaboration Protocol[21] had been signed between the TRNC Personal Data Protection Board and the Authority. The protocol aims to ensure compliance with and implementation of each country's respective laws and regulatory measures and to contribute to the more comprehensive protection of human rights and freedoms, particularly in the field of privacy and personal data protection, within their respective countries and regions through cooperation and

2.3. Collaboration Protocol with the Ministry of Trade

On 28 August 2024, it was announced on the Authority's official website that a Collaboration Protocol[22] had been signed between the Ministry of Trade and the Authority. The protocol aims to develop a joint approach to the impact of digital transformation in marketing and advertising on consumer rights and personal data privacy. It seeks to take significant steps to protect consumer rights and raise awareness regarding personal data-driven practices, such as targeted advertising and deceptive design techniques. Within the scope of this collaboration, monitoring international regulations on the use of personal data in digital advertising and applications, empowering consumers to exercise greater control over their personal data, and developing policies to address potential violations are envisioned.

2.4. Collaboration Protocol with the Capital Markets Board

On 6 January 2025, it was announced on the Authority's official website that a Collaboration Protocol[23] had been signed between the Capital Markets Board and the Authority. This protocol aims to strengthen cooperation and coordination regarding the processing and protection of personal data in capital markets. Under the protocol, the two institutions are expected to exchange information and opinions on shared matters within their respective jurisdictions, develop joint projects on personal data security, privacy, and protection, provide training for professional staff, organize awareness-raising activities, and prepare publications.

2.5. Collaboration Protocol with the Human Rights and Equality Institution of Türkiye

On 8 January 2025, it was announced on the Authority's official website that a Collaboration Protocol[24] had been signed between the Human Rights and Equality Institution of Türkiye and the Authority. This protocol aims to conduct joint efforts to protect human rights and freedoms, combat discrimination, and promote social awareness. The protocol includes plans to organize workshops, panels, and symposiums to enhance awareness of human rights and personal data protection, implement awareness-raising projects, and prepare joint publications.

[20] Only available in Turkish.
[21] Only available in Turkish.
[22] Only available in Turkish.
[23] Only available in Turkish.
[24] Only available in Turkish.

3. Other Activities

Since 2018, the Authority has continued its Wednesday Seminars, and, since 2021, it has also sustained its “Bir Küçük Farkındalık Yeter” podcast series, both of which remained active throughout 2024. Additionally, in 2024, the Authority organized numerous seminars, workshops, training sessions, visits, and events.

Some of these key events included the:

- 28 January Data Protection Day Event.
- Conference on Personal Data Security in the Digital Age.
- 7 April Personal Data Protection Day Event.
- Panel on Amendments to the DP Law No. 6698.
- Event on the Role of Internal Audit in Personal Data Protection.
- Information and Technology Law Summit.
- e-Sade Personal Data Protection Summit.
- Conference on Amendments to the DP Law and Their Implications.
- Event on Cyber World and Personal Data Protection.
- 4th Personal Data Protection Summit.
- Panel on Artificial Intelligence Under the Lens of Privacy and Ethical Principles.
- Workshop on Preparing a Good Practice Guide for Personal Data Protection in the Payment and Electronic Money Sector.

The Wednesday Seminars included topics such as:

- Artificial Intelligence Systems and Their Legal Implications.
- Privacy-Enhancing Technologies.
- Protecting Personal Data After Death Within the Framework of Personality Rights.
- Amendments to the DP Law No. 6698.
- Data Portability from the Perspective of Competition Law.
- Personal Data in Advertising, Targeted Advertising, and Advertising Board Decisions.
- The projects and programs included the:
- KVKK in Schools Project.
- World Children’s Rights Day and KVKK Program.

The “Bir Küçük Farkındalık Yeter” podcast series, highlighting the power of awareness through unique content, has been connecting with listeners since 2023. This podcast, prepared under the Authority’s leadership and branded as “KVKK Agenda,” aims to raise awareness about personal data protection. In 2024, the podcast series released eight episodes.

MOROĞLU ARSEVEN

VII. Constitutional Court Decisions

1. Decision of the Constitutional Court on Application Number 2020/36976, Dated 13 February 2024

In its decision on Application Number 2020/36976, dated 13 February 2024, and published in the Official Gazette No. 32497 dated 22 March 2024, the Constitutional Court ("**CC**") held that the right to request the protection of personal data had been violated. The Court determined that the Public Prosecutor's decision not to pursue prosecution, rendered without collecting the requested evidence or taking the defendant's statement, constituted a breach of this right.

The Applicant, who filed an individual application with the CC, submitted a criminal complaint to the Samsun Chief Public Prosecutor's Office on 9 October 2020, alleging that their employer ("**S.Y.**") had reviewed their account transactions without their knowledge or consent in an attempt to avoid paying employment entitlements after terminating their employment contract. In the complaint, the Applicant claimed that S.Y. had accused them of unlawfully gaining financial benefits by abusing company authority and, as a result, had examined their bank and credit card transaction records.

In this context, the Applicant provided the names and addresses of individuals they wished to have heard as witnesses. The Applicant further asserted that S.Y. had also filed a criminal complaint against them and, in that complaint, had requested the examination of one of the Applicant's account transactions, specifying the bank name, amount, and date. The Applicant argued that it would have been impossible for S.Y. to know such details without having accessed their personal information and requested the examination of the relevant investigation file.

The Chief Public Prosecutor's Office rendered a decision of non-prosecution on 14 October 2020. In its reasoning, the Prosecutor's Office stated that the mere acquisition and disclosure of personal data through sensory perception would not constitute the offense of unlawfully obtaining personal data, but, if certain conditions were met, the offense of violating the confidentiality of private life could be considered. The Applicant objected to this decision before the Samsun 1st Criminal Judgeship of the Peace on 21 October 2020, arguing that they had presented concrete evidence, yet the decision of non-prosecution was issued without collecting the evidence. The Judgeship of the Peace, finding no error in the decision, dismissed the objection with finality on 23 October 2020. The Applicant received notification of the final decision on 31 October 2020 and subsequently filed an individual application with the CC on 24 November 2020.

In the individual application to the CC, the Applicant claimed the following:

- The Applicant asserted that they had requested the issuance of official correspondence to banks and the hearing of their witness, as well as the examination of the investigation file related to the criminal complaint filed against them. Despite these requests, a decision of non-prosecution was rendered on the grounds that there was no evidence other than abstract statements.

- The Applicant stated that the Chief Public Prosecutor's Office had rendered a decision based solely on the case file without taking S.Y.'s statement or collecting the evidence cited in S.Y.'s complaint petition.

- The Applicant alleged that S.Y. had accessed their bank account transactions, identified the individuals to whom they had transferred money, and contacted these individuals by phone. In this context, the Applicant requested that M.Ç., one of the individuals contacted by S.Y., be heard as a witness.

- The Applicant claimed that an ongoing investigation was being conducted by the Ankara Chief Public Prosecutor's Office based on S.Y.'s complaint against them. The Applicant further alleged that, in the complaint petition submitted by S.Y. within the scope of the investigation, S.Y. referenced a money transfer belonging to the Applicant, specifying the bank name, amount, and transaction date, and also attached a summary of the Applicant's account transactions to the petition.

- The Applicant contended that S.Y. could not have lawfully accessed information regarding them and requested that the relevant investigation file be examined as evidence to substantiate their claims.

- The Applicant alleged that their personal data had been unlawfully obtained.

The notable aspects of the CC's decision with Application Number 2020/7518 and Decision Date 12 October 2023 can be outlined as follows:

- The essence of the Applicant's complaint pertained to the unlawful acquisition of their personal data; therefore, it was deemed necessary to evaluate the application within the scope of the right to request the protection of personal data.

- During the admissibility review, it was determined that the claim regarding the right to request the protection of personal data was not manifestly ill-founded and that there was no other reason requiring the application to be deemed inadmissible.

- Pursuant to Article 20 of the Constitution, it was stated that everyone has the right to request the protection of their personal data, which includes the rights to be informed, to access, to request correction or deletion, and to learn whether the data is being used in accordance with its intended purpose.

- The CC emphasized that the state is obligated not only to prevent arbitrary interference with personal data but also to protect this right from violations by third parties. This responsibility includes establishing an effective judicial system to prevent infringements of individuals' personal data. However, this obligation does not necessarily require initiating criminal proceedings in every instance; administrative or disciplinary investigations may suffice in certain cases.

- The CC determined that the evidence presented by the Applicant had not been adequately addressed and that an effective criminal investigation had not been conducted. This led to the conclusion that the positive procedural obligation had not been fulfilled.

- The CC ruled that the Applicant's right to request the protection of their personal data had been violated.

- It was decided that a new investigation should be conducted to remedy the consequences of the violation. The relevant investigative authorities were instructed to address the deficiencies that caused the violation and to render a new decision in accordance with the principles outlined in the violation ruling.

2. Constitutional Court's Decision on Application Number 2021/45975, Dated 17 July 2024

The CC's decision dated 17 July 2024 on Application Number 2021/45975 was published in the Official Gazette No. 32755 dated 17 December 2024. The Applicant filed a complaint with the CC, alleging that the rejection of their request to access personal data in their personnel file violated their right to respect for private life and the right to request the protection of personal data, which are both guaranteed under Article 20 of the Constitution. The CC accepted the allegations and evaluated the case. The decision includes significant findings on the classification of professional records of public officials as personal data and provides guidance on how requests for access to such data should be handled.

The Applicant, a public official serving at the Ministry of Foreign Affairs, claimed that the adverse circumstances encountered during their professional career stemmed from records, evaluations, and informational notes contained in their personnel file. Seeking access to these records, the Applicant submitted a request to the Ministry of Foreign Affairs under Law No. 4982 on the Right to Information. However, the Ministry rejected the request, citing the nature of the information in the personnel file and referring to provisions that mandate the confidentiality of such information and restrict its disclosure to third parties.

The Applicant filed an annulment case with the Ankara 4th Administrative Court regarding the denial of their request for information by the Ministry of Foreign Affairs. On 19 June 2019, the court dismissed the case, referencing the principle of "confidentiality of the personnel file" stipulated in Section (D) titled "*Procedures and Principles for Maintaining Personnel Files*" of the *Public Personnel Circular* published in the Official Gazette No. 27906 dated 15 April 2011. The court justified the rejection of the Applicant's request based on this principle, emphasizing that the contents of a personnel file cannot be disclosed without the individual's consent. Additionally, it ruled that the provision on the confidentiality of personnel files limits access to personal data under the right to information. However, the court did not evaluate whether the Applicant should have been granted access to their own data contained within the personnel file.

The applicant appealed the decision of Ankara 4th Administrative Court to the Regional Administrative Court. However, the Regional Administrative Court found the decision of the Administrative Court lawful and dismissed the appeal by a decision rendered on 23 October 2019. Following the notification of the final judgment on 13 November 2019, and, in light of the Ministry of Foreign Affairs' rejection decision and the judiciary's stance deeming this decision lawful, the applicant lodged an individual application with the CC on 9 December 2019, seeking redress for the violation of their rights.

In the assessment conducted by the CC, the following noteworthy points were highlighted:

- Record reports include evaluations concerning public servants' discipline, professional competence, and commitment to duty, and these reports are prepared for assessing such attributes. In this context, it was stated that individuals' private lives must be protected during the storage of record reports. The CC evaluated the applicant's request for access to this information as related to the right to privacy. It was noted that personal data, such as record reports, must be protected against unauthorized access during storage, emphasizing the absolute necessity of adhering to confidentiality principles.

- The CC observed that there was no explicit legal provision justifying the rejection of the applicant's request for access to their personal data. It determined that this constituted a violation of the right to privacy. Furthermore, the CC highlighted the absence of any compelling rationale to support the infringement of the applicant's right to seek protection of their personal data.

- The CC emphasized that any interference with the right to request the protection of personal data must adhere to the principle of "limitation by law" as enshrined in Article 13 of the Constitution. It further underlined that such interferences must be proportionate and based on legitimate grounds, concluding that the contested interference failed to satisfy these requirements.

- The principle of legality, the CC stressed, necessitates compliance with the standards of legal certainty and foreseeability. The CC noted that the lower courts, in addressing the applicant's requests, should avoid interpretations that create legal ambiguity. It found that the applicant's requests had not been thoroughly examined and that such omissions could not be justified as lawful interventions.

- Regarding the preparation, storage, and evaluation of record reports concerning public personnel, the CC acknowledged the public interest in ensuring the effective functioning of public services. However, it stressed that the right to privacy of individuals must be respected during these processes, and confidentiality of the information must be maintained to prevent unauthorized disclosures. Public Personnel Circular Clause (D) was deemed a necessary regulatory measure to safeguard the confidentiality of such records.

- The CC underscored the need to balance the right to privacy with the right of access to personal data. While recognizing that Public Personnel Circular Clause (D) and the provisions of Law No. 4982 impose certain restrictions to protect personal data and ensure confidentiality, the CC held that such restrictions cannot entirely preclude individuals from accessing the information within their own personnel files.

- Ultimately, the CC concluded that the applicant's right to request the protection of personal data, as guaranteed under the right to respect for private life enshrined in Article 20 of the Constitution, had been violated.

- As a remedy, the CC ordered a retrial to address the violation and rectify its consequences. Consequently, the case was referred to the Ankara 4th Administrative Court for a new judicial review.

MOROĞLU ARSEVEN

VIII. Other Important Developments

1. Artificial Intelligence Action Plan 2024–2025

The Presidential Circular No. 2021/18 regarding the "National Artificial Intelligence Strategy 2021–2025," Türkiye's first national strategy document, prepared in line with the 11th Development Plan through the collaboration of the Presidency's Digital Transformation Office and the Ministry of Industry and Technology, with the active participation of all relevant stakeholders, was published in the Official Gazette No. 31574 dated 20 August 2021 and entered into force. As of 24 July 2024, with the advancement of technology, evolving needs, and in line with the 12th Development Plan, the National Artificial Intelligence Strategy 2021–2025 was updated and announced to the public as the "Artificial Intelligence 2024–2025 Action Plan" ("**2024–2025 Action Plan**"). This update aims to ensure that the strategy maintains a flexible and adaptive structure, enabling artificial intelligence projects to be implemented in line with sound ethical principles, while enhancing the ecosystem's maturity level and competitive strength. The *National Artificial Intelligence Strategy 2021–2025*, initially announced in 2021, was structured under six main strategies. These six strategies are as follows:Yda istihdamı artırmak

1. Training artificial intelligence experts and supporting increased employment in this field.

2. Supporting research, innovation, and entrepreneurship.

3. Expanding access to quality data and technical infrastructure.

4. Developing regulations to support and accelerate socioeconomic adaptation.

5. Strengthening international collaborations.

6. Supporting and accelerating structural and workforce transformation.

The six strategies outlined above were established with 24 objectives and 119 measures. Under the 2024–2025 Action Plan, 19 actions have been defined, again based on the six strategic pillars. The implementation of the action plans will be carried out by various institutions, including the Ministry of Industry and Technology, The Scientific and Technological Research Council of Türkiye ("**TUBITAK**"), the Turkish Employment Agency ("**İŞKUR**"), the Ministry of National Education, the Presidency's Investment Office, the Presidency's Digital Transformation Office, the Data Protection Authority, and the Ministry of Justice. The highlights of the 2024–2025 Action Plan are as follows:

- Attracting talent to Türkiye in the field of artificial intelligence and increasing a skilled workforce through the TechVisa Program.

- Including data science and artificial intelligence topics in the curricula of higher education programs, and establishing associate, undergraduate, and postgraduate programs in the field of artificial intelligence.

- Defining technical and ethical standards for generative artificial intelligence models (LLMs, LAMs, etc.) to be developed domestically, and establishing a specialized committee to manage this process.

- Developing a large-scale Turkish language model and creating a Turkish Large Language Model Community to incorporate contributions from the entire ecosystem, including voluntary participants.

- Launching support programs to encourage the use of artificial intelligence products and solutions developed through domestic R&D efforts by SMEs.

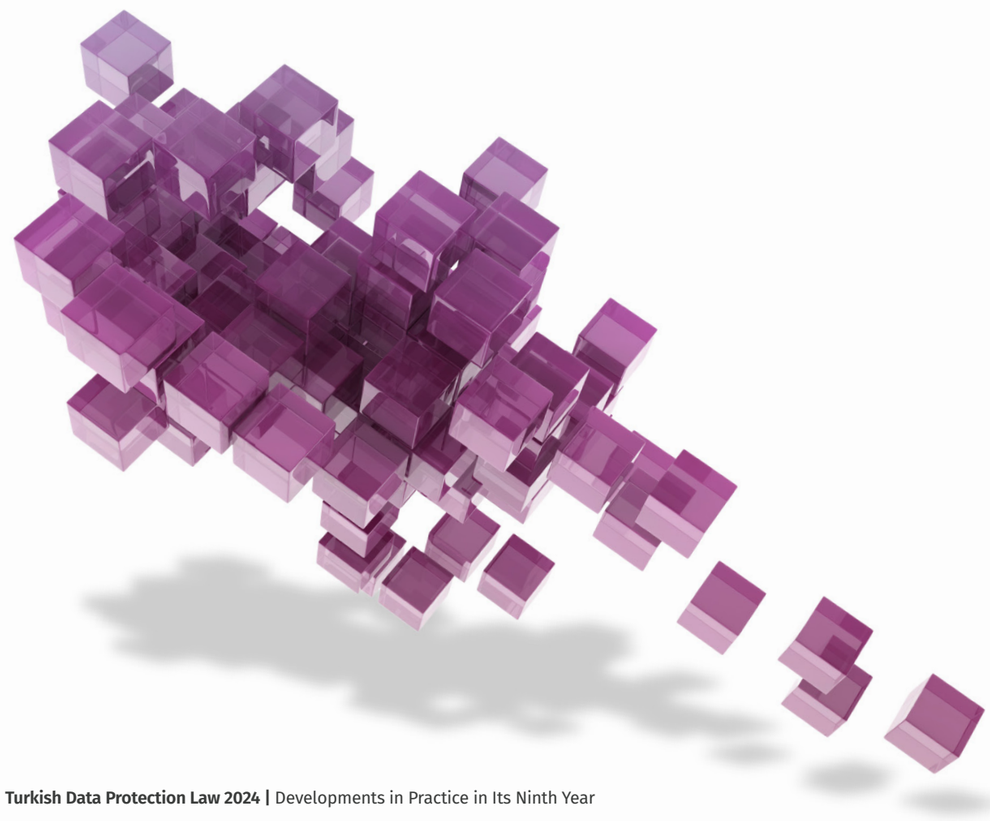
- Preparing guidelines to clarify intellectual property rights for content generated by artificial intelligence and conducting standardization efforts for the patenting of artificial intelligence products.

- Conducting needs analysis and capacity development for processor infrastructure to position Türkiye as a global player in the development of artificial intelligence products, solutions, and generative artificial intelligence models.

- Creating an inventory of data held by public institutions and organizations,

establishing a Central Public Data Space, and developing mechanisms to make this data accessible to researchers and technology developers.

- Establishing national regulations aligned with international norms governing the development, use, and market placement of artificial intelligence systems.
- Preparing a Legal Assessment Guide for Artificial Intelligence Applications.
- Developing a Value and Principles Impact Analysis Framework for Artificial Intelligence.
- Creating tools necessary for auditing trustworthy artificial intelligence.
- Developing collaborations for knowledge and experience sharing with countries or global companies that have developed their own large language models.
- Monitoring studies related to the secure and free flow of data.
- Introducing a Trusted Artificial Intelligence Seal under a certification mechanism for auditing and legal compliance of artificial intelligence applications, to be developed by TUBITAK and the Turkish Standards Institution.
- Developing policies and legislative studies for the centralized management of efforts to detect, prevent, and mitigate new-generation cyber threats, particularly those powered by artificial intelligence, against Türkiye's assets in cyberspace.



- Establishing a Türkiye Artificial Intelligence Portal under the management of the TUBITAK BİLGEM Artificial Intelligence Institute.
- Establishing Collaborative Development Laboratories for Artificial Intelligence, aligned with the thematic focus areas of the Institute, through joint funding under the TUBITAK BİLGEM Artificial Intelligence Institute.
- Preparing national occupational standards and national qualifications in the field of artificial intelligence, along with developing measurement and evaluation infrastructure within this scope.

2. Developments in Electronic Commerce Law

As an important step in protecting consumer rights in the e-commerce sector, the Advertising Board, in its meeting held on 12 March 2024, reviewed the membership, personal data processing, and targeted advertising practices of 12 different e-commerce platforms and made administrative decisions. In this regard, the Advertising Board examined the companies' membership agreements, explicit consent and privacy notices, privacy policies, and cookie usage. The evaluations revealed that practices such as the mandatory collection of personal data from consumers without a legal basis, failure to obtain explicit consent for the use of personal data for marketing purposes, inadequate guidance during the membership cancellation process, and failure to provide consumers with the ability to delete their data traces on the platform were determined to be unfair and misleading. The Advertising Board concluded that these commercial practices violated consumers' rights to be informed and make free choices and ruled that these activities, which weaken consumers' decision-making will, were unlawful. This decision taken by the Advertising Board highlighted the importance of e-commerce platforms' compliance with the law and data protection sensitivities, emphasizing that the protection of consumers' personal data and the conduct of commercial activities must adhere to the principles of transparency and fairness.

3. National Data Strategy

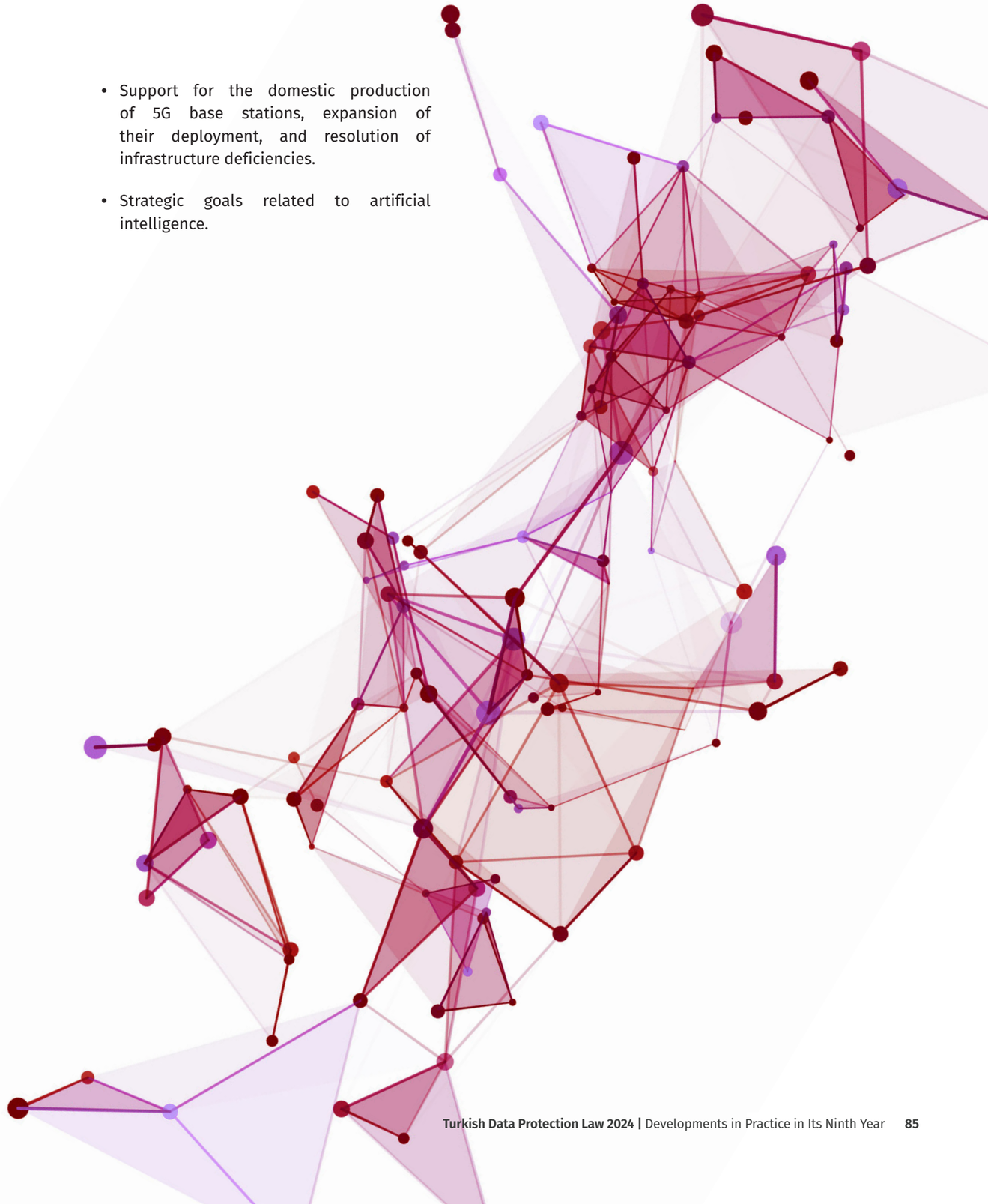
On 1 April 2024, the United Nations Development Program (UNDP) Türkiye Country Office and the Central Digital Office published the "*Data Governance Framework Proposal Report for Türkiye*" to guide Türkiye's data-driven digital transformation process. The report emphasizes the urgent need to strengthen data legislation, develop a comprehensive national data strategy, and improve sector-specific policies, while also highlighting the critical role of artificial intelligence and data analytics technologies in this process. It specifically mentions that artificial intelligence-supported analytical tools will contribute to the development of effective policies, particularly in areas such as healthcare, agriculture, education, and public services. Additionally, the importance of compliance with ethical principles and the protection of data privacy is emphasized. The report underscores the impact of increasing data volumes on Türkiye's contribution to global development and suggests that artificial intelligence and data analytics should be considered as a strategic priority, offering recommendations to enhance Türkiye's international competitiveness.

On 7 May 2024, the Higher Education Council ("**YÖK**") published a guide titled "*Ethical Guidelines for the Use of Generative Artificial Intelligence in Scientific Research and Publication Activities in Higher Education Institutions*" to establish ethical principles for the use of artificial intelligence technologies in scientific research and publication activities in higher education institutions. The guide aims to assess the risks and opportunities of generative artificial intelligence technologies and to take precautions against the ethical and legal issues they may bring. It points out that one of the most significant ethical issues that may arise in the use of generative artificial intelligence is the processing of personal data in violation of legislation, and it emphasizes the need to comply with the DP Law and other data protection regulations. YÖK has clearly stated that personal data should not be transferred to generative artificial intelligence systems unless it is anonymized or masking methods are used. Furthermore, it is stressed that detailed information about the operating principles and potential risks of these systems must be obtained before their use. The guide highlights the importance of adhering to principles of transparency, legality, and proportionality in data processing activities, noting that failure to do so could lead to personal data violations and ethical issues. Researchers are expected to act with full awareness of the nature of the data used and the purposes of its processing, and it is emphasized that violations of this obligation could pave the way for unethical practices.

4. Türkiye International Direct Investment Strategy and Action Plans (2024–2028)

The "Türkiye International Direct Investment Strategy (2024–2028) and Action Plans," prepared by the Presidency's Investment Office of Türkiye, were published in the Official Gazette No. 32616 dated 29 July 2024. The strategy and action plans emphasize the contributions of international direct investments to Türkiye's economy and provide a strategic framework for the 2024–2028 period. The Türkiye International Direct Investment Strategy (2024–2028) and Action Plans were developed with the aim of accelerating Türkiye's economic growth and creating a more attractive investment environment for international investors. Within this framework, the following strategic goals are identified:

- Completion of alignment processes under the DP Law with the EU acquis, particularly the GDPR.
- Establishment of regulations to ensure national cybersecurity, taking into account the EU Directive on the Security of Network and Information Systems (NIS Directive), new developments in cybersecurity, and best practices at the international level.
- Promotion of the development of domestic companies providing hosting (data center) services and enhancing competition, in parallel with the National Artificial Intelligence Strategy 2021–2025.
- Support for the domestic production of 5G base stations, expansion of their deployment, and resolution of infrastructure deficiencies.
- Strategic goals related to artificial intelligence.



5.National Cybersecurity Strategy and Action Plan (2024–2028)

The Ministry of Transport and Infrastructure published the "National Cybersecurity Strategy and Action Plan (2024–2028)" ("**Strategy and Action Plan**") on 7 September 2024. The Strategy and Action Plan aims to mitigate the impacts of cyber threats, enhance national capacity, establish a secure cyber environment, and position Türkiye among the leading countries globally in the field of cybersecurity.

The Strategy and Action Plan emphasizes the significance of cybersecurity for the country and outlines the strategic elements necessary for Türkiye to achieve its goals in this field. Through the Strategy and Action Plan, Türkiye aims to establish a robust defense line against cyber threats by leveraging the most up-to-date and effective technological capabilities during its digital transformation and development process. In this context:

- The Strategy and Action Plan highlights the critical importance of cybersecurity for national security, particularly emphasizing the need to protect critical infrastructure and develop domestic technologies. While maximizing the benefits of technological advancements in services and solutions, various activities are being undertaken to protect the infrastructure supporting these services against cyber risks and threats, ensuring service continuity and data security.

- The Strategy and Action Plan consists of six strategic objectives, 18 goals, and 61 action items. The goals are directly linked to defined strategic objectives to enable goal-oriented development. The defined strategic objectives include "Cyber Resilience," "Proactive Cyber Defense and Deterrence," "Human-Centered Cybersecurity Approach," "Secure Use of Technology and Its Contribution to Cybersecurity," "Combatting Cyber Threats with Domestic and National Technologies," and "Türkiye as a Global Brand in the International Arena."

- In line with these objectives, specific goals have been set, and the necessary actions to achieve them have been developed. Each action item has been assigned to relevant public institutions and organizations, with the necessary roles and responsibilities being designated. The monitoring and evaluation method for the Strategy and Action Plan focuses on assessing progress toward achieving the set goals and reviewing whether the undertaken efforts meet the defined targets. This approach ensures that the results and progress achieved during the implementation process are systematically tracked.

6. Decision on the Approval of the 2025 Presidential Annual Program

The 2025 Presidential Annual Program ("**Annual Program**") was approved by Presidential Decision No. 9074, published in the duplicate edition of the Official Gazette No. 32707 dated 30 October 2024. Within the scope of the program, macroeconomic, fiscal, and sectoral policies, as well as strategies for the implementation of these policies, have been outlined. Under the framework of the Annual Program, steps to be taken concerning amendments to the DP Law, measures to strengthen information technology infrastructure, and policies to support advancements in artificial intelligence have also been defined. Key policies and measures highlighted in this context can be summarized as follows:

- Efforts to align the DP Law with the EU acquis, particularly the GDPR, will be completed.

- Regulations to ensure national cybersecurity will be introduced, taking into account the EU Directive on Network and Information Security (NIS2), new developments in cybersecurity, and international best practices.

- Cybersecurity standards will be established in areas where they are needed.

- The National Data Strategy and Action Plan will be implemented.

- Security and service delivery standards for data centers will be developed.

- An artificial intelligence risk map will be created.

- Definitions of data elements and indicators used in health information systems will be reviewed, business rules will be established and published to enhance data quality, and compliance audits will be conducted.

- The compatibility of health indicators in the Ministry of Health's databases with international definition standards will be improved.

- Protocols for data sharing among institutions in the health sector will be established, and deficiencies in internet service integrations will be identified and addressed.

- Legislation will be enacted to enable the production and sharing of anonymized health data, and anonymized and synthetic data sets will be published for researchers.

- Public data infrastructure will be implemented to enhance institutional capacity through interagency advanced data analytics and artificial intelligence projects.

- Legal regulations for public data sharing will be introduced, and a national open data portal will be launched.

- Ethical principles for trustworthy artificial intelligence will be applied in the development of artificial intelligence applications in the public sector and in the procurement of products and services.

B. STRUCTURE AND SUPERVISORY ACTIVITIES OF THE BOARD AND AUTHORITY

MOROĞLU ARSEVEN

I. Structure and Organization of the Board and the Authority

The Authority is composed of the Board, the Presidency, and related administrative units. The organizational structure includes the Authority's President, Vice President, seven Board members, and seven departmental units under the Presidency.

Following the resignation of Dr. Ayşenur KURTOĞLU from her Board membership and the appointment of Muhammed Serdar CAFOĞLU as of 10 October 2024, the current structure

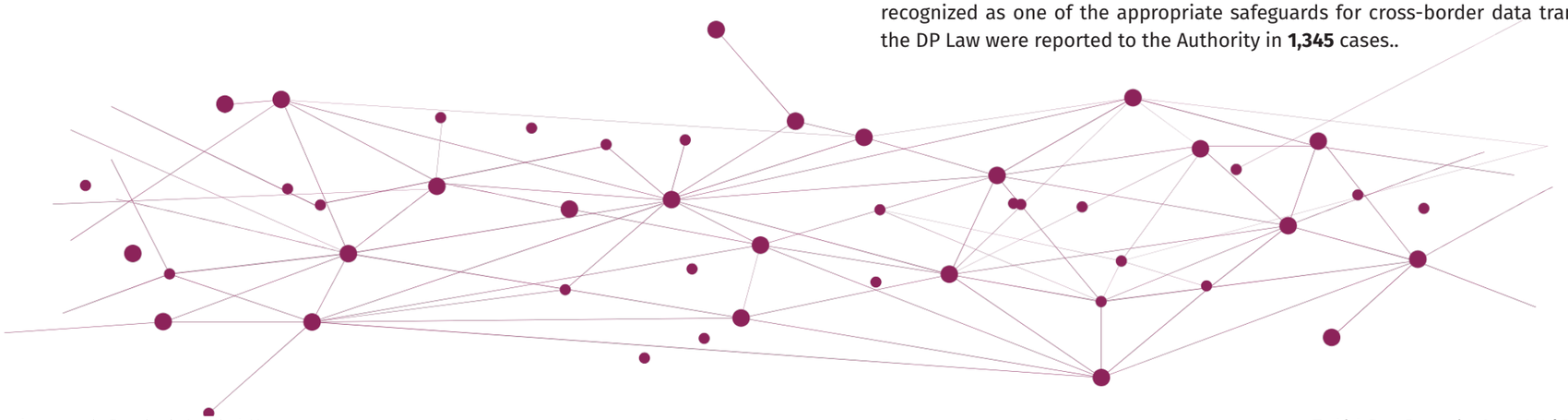
President	Prof. Dr. Faruk BİLİR
Second President	Hasan AYDIN
Board Member	Şaban BABA
Board Member	Murat KARAKAYA
Board Member	Bayram ARSLAN
Board Member	Tamer AKSOY
Board Member	Recep KESKİN
Board Member	Cennet ALAS ŞEKERBAY
Board Member	Muhammed SERDAR CAFOĞLU

Presidency

- Department of Data Management
- Department of Investigation
- Department of Legal Affairs
- Department of Data Security and Information Systems
- Department of Guidance, Research and Authority Communication
- Department of Human Resources and Support Services
- Strategy Development Department

The Authority published its first annual activity report in 2018 and continued this practice for the years 2019, 2020, 2021, 2022, and 2023. However, as of the publication date of this study, the Authority has not yet published its activity report for 2024. Instead, a summary document titled "*2024 Activity Information Note*" has been released. In this context, information regarding the Authority's activities has been compiled from the 2024 Activity Information Note, updates shared on the Authority's official website during 2024, and the 2023 Activity Report.

According to the 2024 Activity Information Note, the Board resolved **6,958** out of **8,186** notifications, complaints, and applications. A total of 281 data breach notifications were submitted to the Board, **63** of which were publicly disclosed. As a result of investigations, administrative fines amounting to **TRY 552,668,000** were imposed. Additionally, **110** legal opinions were issued under the scope of the DP Law. In relation to the cross-border transfer of personal data, three undertakings that met the required criteria were approved. SCCs recognized as one of the appropriate safeguards for cross-border data transfers under the DP Law were reported to the Authority in **1,345** cases..



MOROĞLU ARSEVEN

II. Overview of the Board's Supervisory Activities Shared with the Public in the 2023–2024 Period

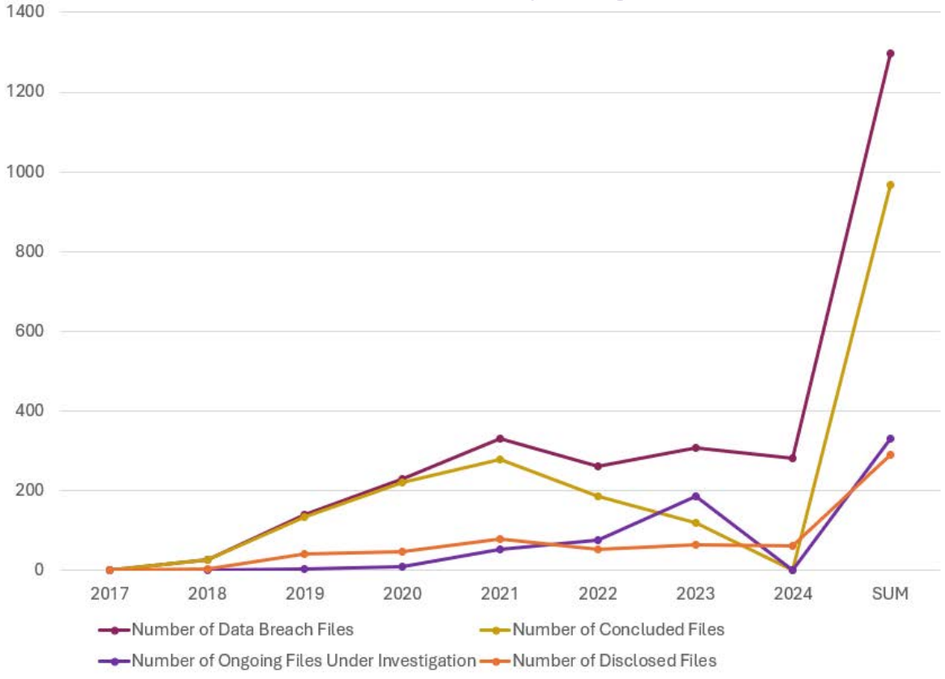
The Authority published the 2024 Activity Information Note on 30 December 2024. Compared to the activity reports published in previous years, the Activity Information Note was prepared with a narrower scope, focusing solely on specific statistical data related to 2024. Within this framework, data for 2024 has been provided in the 2024 Activity Information Note, while data for previous years has been referenced based on the 2023 Activity Report.

1 Data Breach Notifications

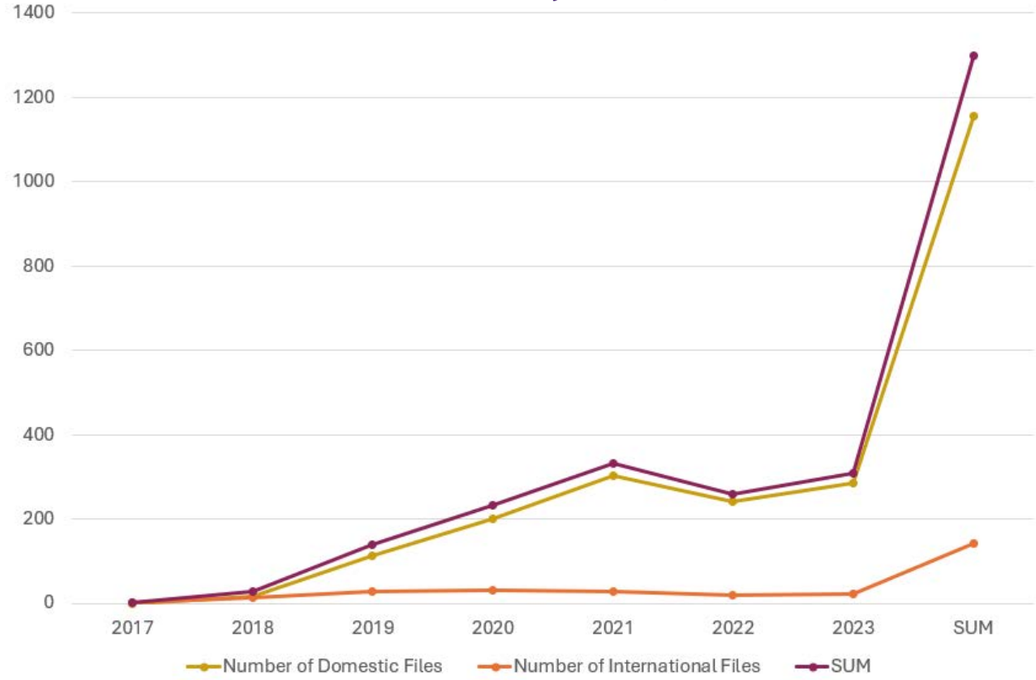
As stated in the 2024 Activity Information Note, 281 data breach notifications were submitted to the Authority in 2024, 63 of which were publicly disclosed.

The number of data breach notifications for the years 2017, 2018, 2019, 2020, 2021, 2022, 2023, and 2024[25] are presented in the tables below.

Data Breach Notifications by Investigation Status



Data Breach Notifications by Domestic/International Status[26]



[25] The 2024 Activity Information Note includes only data on the "number of data breach files" and "number of disclosed files," while other data for 2024 has not been disclosed by the Authority as of the date of this study.

[26] The 2024 Activity Information Note does not include a breakdown of "Data Breach Notifications by Domestic/International Status"; instead, it provides the total number of 281 data breach notifications without such a distinction.

MOROĞLU ARSEVEN

2

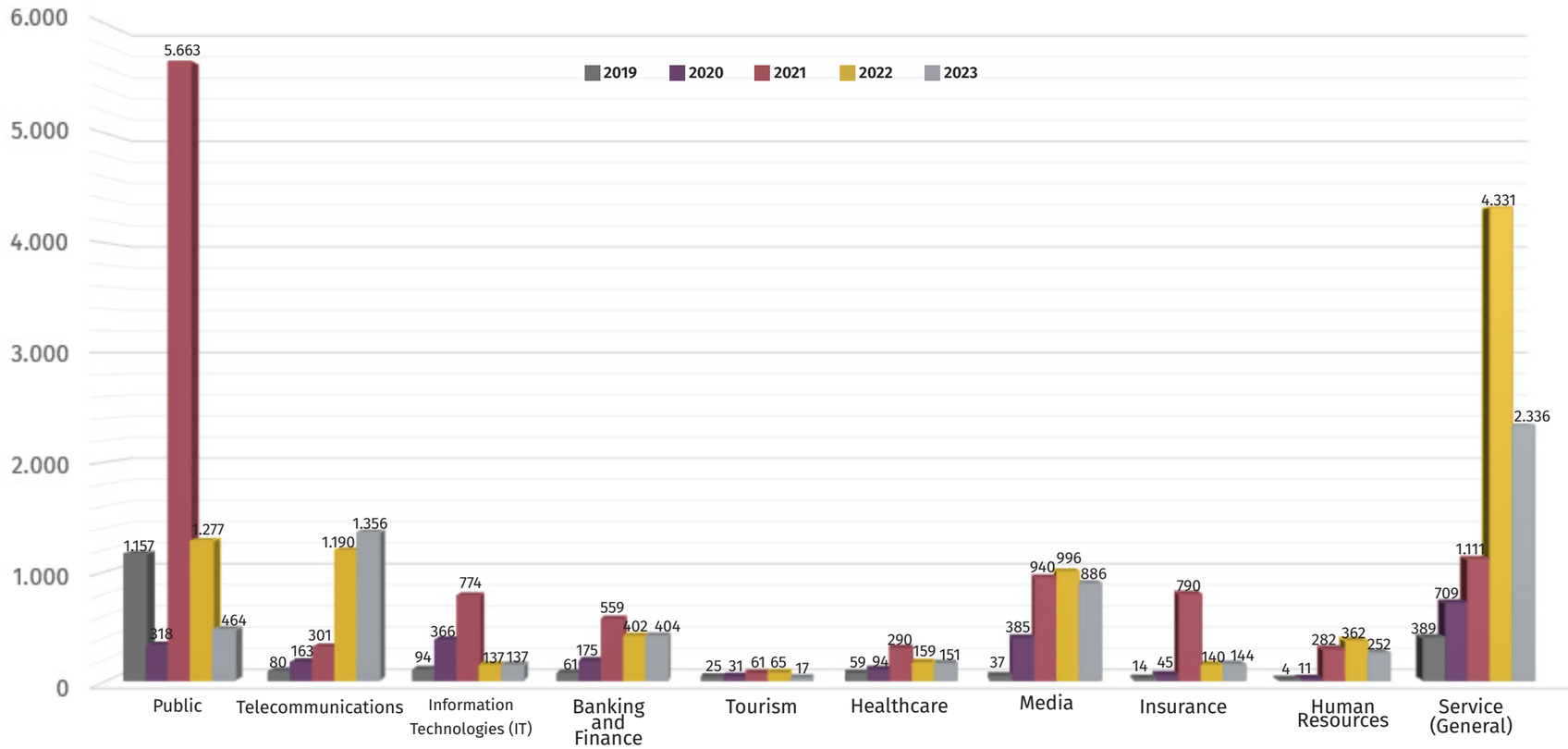
Complaints

In 2024, according to the statistics provided in the 2024 Activity Information Note, a total of **8,186 notifications, complaints, and applications** were received, of which **6,958 were concluded**.

The numbers of notifications, complaints, and applications received up to 31 December 2023 are presented below.

2.1. Distribution of Complaints by Sector[27]

The sectoral distribution of complaints for the years 2019, 2020, 2021, 2022, and 2023 is provided in the table below.

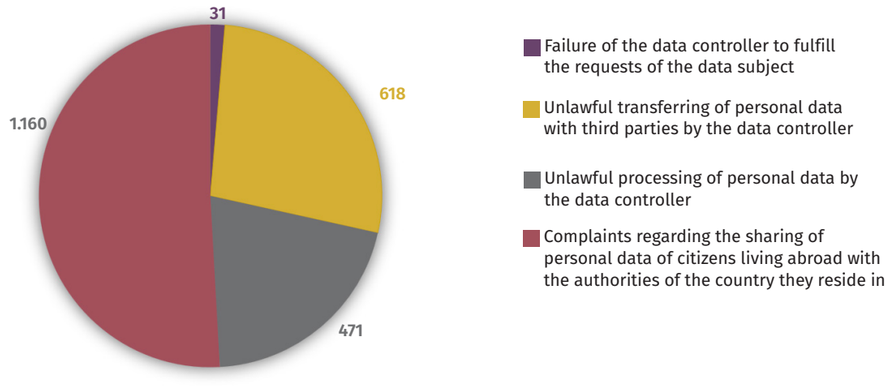


[27] This information has been referenced from the 2023 Activity Report published by the Authority.

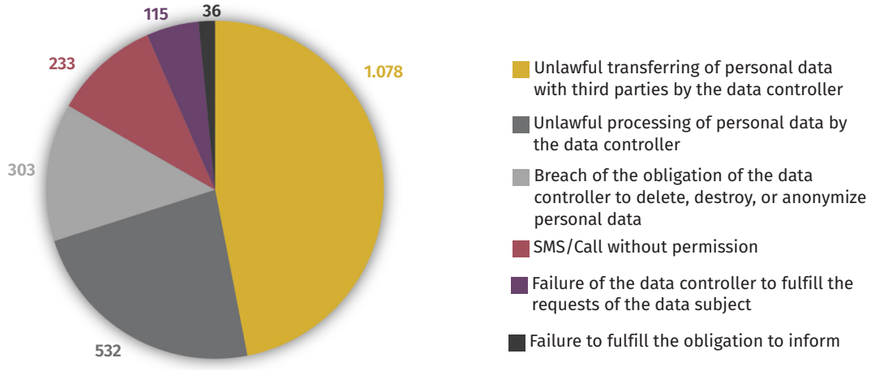
2.2. Distribution of Complaints by Subject

The subject-based distribution of complaints for the years 2019, 2020, 2021, 2022, and 2023 is provided in the table below.

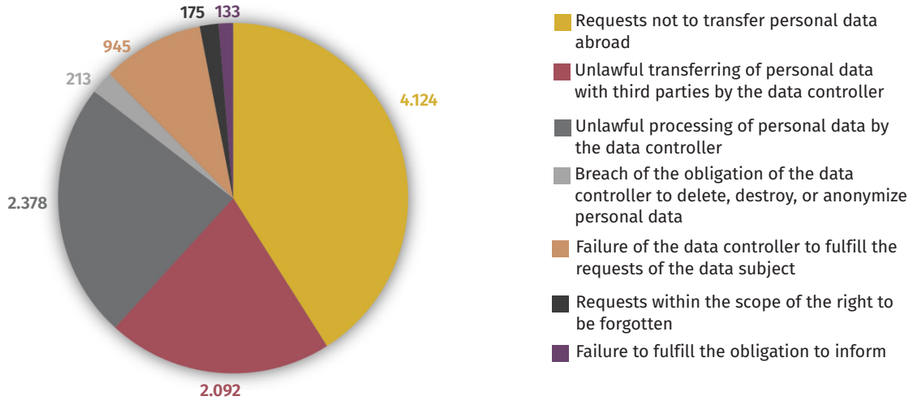
a. Distribution of Complaints in 2019[28]



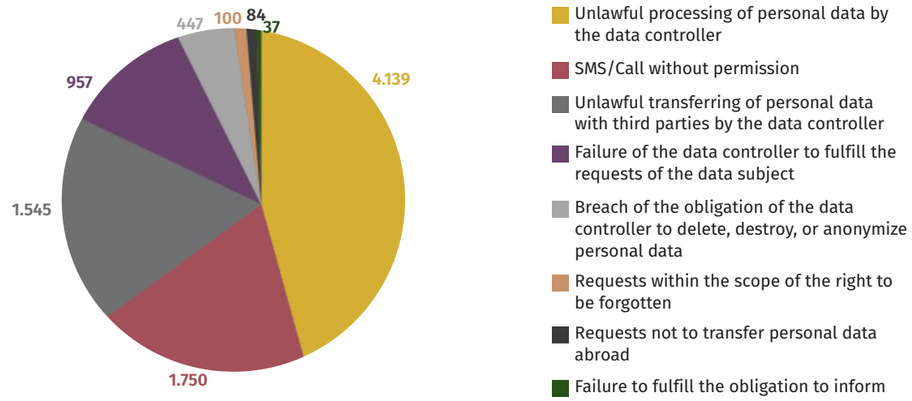
b. Distribution of Complaints in 2020[29]



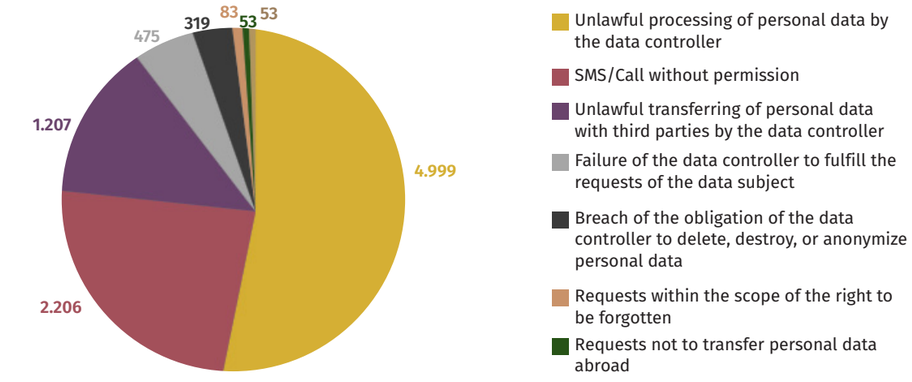
c. Distribution of Complaints in 2021[30]



d. Distribution of Complaints in 2022[31]



e. Distribution of Complaints in 2023[32]



[28] This information has been referenced from the 2023 Activity Report published by the Authority.
[29] This information has been referenced from the 2023 Activity Report published by the Authority.
[30] This information has been referenced from the 2023 Activity Report published by the Authority.
[31] This information has been referenced from the 2023 Activity Report published by the Authority.
[32] This information has been referenced from the 2023 Activity Report published by the Authority.

3

Registration and Application Numbers for VERBIS and Numerical Status of Activities Conducted via VERBIS[33]

As of the date this study was prepared, the Authority has not disclosed the number of VERBIS registrations, applications, and activities for 2024 to the public. However, in the Public Announcement on VERBIS published on the Authority's official website on 1 August 2024, it was stated that approximately 130,600 data controllers were identified as having an obligation to register and notify VERBIS, and approximately 16,350 data controllers who failed to fulfill this obligation were subjected to VERBIS examinations by the Board. It was further noted that administrative fines were imposed based on the algorithm table prepared according to annual financial balance sheet totals as a result of these examinations. As of 1 August 2024, the Board imposed administrative fines amounting to TRY 503,935,000 on domestic and international natural and legal data controllers who failed to fulfill their VERBIS registration and notification obligations.

The statistical data regarding VERBIS registrations and applications as of 31 December 2023 is as follows:

Number of Applications	Number of Applications	Number of Rejected Applications	Number of Assigned Contact Persons
226.201	188.633	7.597	213.065

Performance	31 December 2023
VERBIS Application Approval	226.201
VERBIS Application Update Procedures	7.539
Calls Regarding VERBIS Applications	84.890
Number of Notification Queries	1.644.725

[33] This information has been referenced from the 2023 Activity Report published by the Authority.

4

Commitment Letter Application

In 2024, the Board finalized three commitment letter applications, bringing the total number of data controllers with approved commitment letter applications to nine.

Below is the list of all data controllers whose commitment letter applications have been

Data Controller	Commitment Letter Application Approval Date
TEB Arval Araç Filo Kiralama Anonim Şirketi	9 September 2021
Amazon Turkey Perakende Hizmetleri Ltd. Şti. ve Amazon Turkey Yönetim Destek Hizmetleri Ltd. Şti.	4 March 2023
Turksport Spor Ürünleri San. Tic. Ltd. Şti. (Decathlon Türkiye)	22 June 2021
Türkiye Futbol Federasyonu	18 January 2022
Otokoç Otomotiv Ticaret ve Sanayi Anonim Şirketi	30 March 2023
Google Reklamcılık ve Pazarlama Limited Şirketi	17 August 2023
Celltrion Healthcare İlaç Sanayi ve Limited Şirketi	25 January 2024
Bosch Termoteknik Isıtma ve Klima Sanayi ve Ticaret Anonim Şirketi	28 May 2024

5

SCCs Notifications

As stated in the 2024 Activity Information Note, a total of 1,345 notifications were submitted to the Authority regarding SCCs, which are one of the appropriate safeguards for cross-border data transfers under the DP Law.

6

BCRs Applications

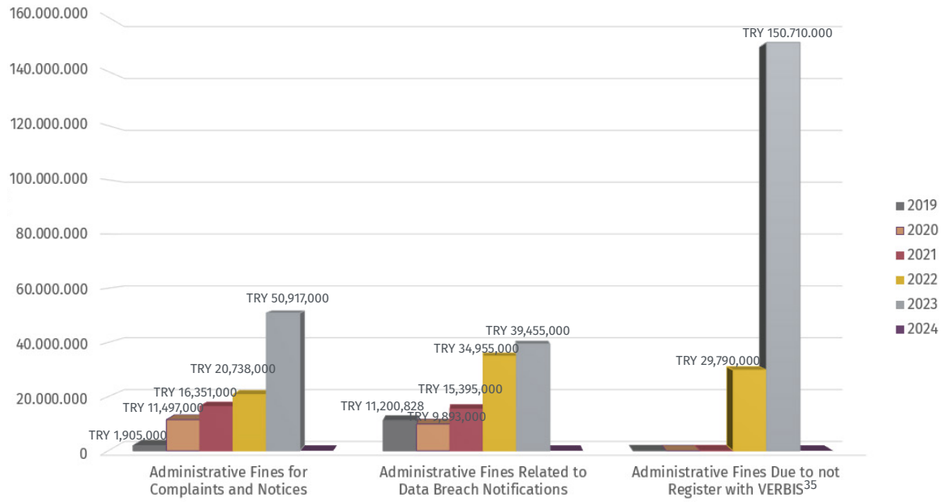
As stated in the Cross-Border Data Transfer Guidelines, a total of three BCRs applications were submitted by 2025. However, these applications were rejected due to procedural and substantive deficiencies.

7

Sanctions

According to the 2024 Activity Information Note, a total of TRY 552,668,000 in administrative fines were imposed by the Authority as a result of investigations conducted.

The administrative fines imposed for the years 2019, 2020, 2021, 2022, 2023, 2024[34] are presented in the table below.



	2019	2020	2021	2022	2023	2024
SUM	TRY 13,105,828	TRY 21,390,000	TRY 31,746,000	TRY 85,483,000	TRY 241,082,000	TRY 552,668,000

[34] According to the 2024 Activity Information Note, a total of TRY 552,668,000 in administrative fines were imposed by the Authority as a result of its investigations; however, no breakdown by subject matter was provided.
[35] The deadline for fulfilling the obligation to register and notify VERBIS was set as 31 December 2021. In the Authority's announcement dated 21 April 2022, it was stated that administrative sanctions would be imposed for non-compliance with the VERBIS registration and notification requirements. Therefore, no administrative fines were imposed during the period 2017–2021.

7.1. Review of Sanctions

The highest administrative fine published on the Authority's website:

The highest administrative fine published on the Authority's website is the TRY 3,250,000 fine imposed on an e-commerce platform under Decision No. 2024/1385, dated 8 August 2024. This fine represents the highest single penalty disclosed to the public since the Board began its operations.

The Authority has published a total of three decisions on its official website:

Pursuant to Article 16 of the Regulation on the Data Controllers' Registry, the Board is authorized to grant exemptions from the obligation to register with VERBIS, considering the criteria specified in the Regulation. In line with this authority, the Board issued Decision No. 2023/2135, dated 14 December 2023, on Exempting Village Legal Entities from the Obligation to Register with the Data Controllers' Registry. Through this decision, it was determined that village public legal entities would be exempt from the obligation to register with VERBIS.

The other two decisions are (i) Decision No. 2024/1176, dated 18 July 2024, on the Unlawful Processing of Personal Data for Subscription Establishment Purposes and (ii) Decision No. 2024/1385, dated 8 August 2024, on the Data Breach Notification Submitted to the Board by an E-Commerce Platform. In both decisions, the Board determined that "*necessary technical and administrative measures to prevent the unlawful processing of personal data*" had not been taken, as stipulated under Article 12/1 of the DP Law, and accordingly imposed administrative fines pursuant to Article 18/1(b) of the DP Law.

MOROĞLU ARSEVEN

7.2. Highest Administrative Fines

The table below lists the 21 highest administrative fines imposed by the Board and publicly announced[36] on its official website since 2018. On reviewing the decisions resulting in the highest administrative fines, it is evident that the majority of data breaches stem from issues related not to administrative shortcomings but to deficiencies in information systems, the failure to implement technical measures properly and promptly, or delays in notifying the Board.

Article 12/1: Failure to take necessary technical and administrative measures to prevent unlawful processing of personal data.

Article 12/3: Failure to audit compliance with the DP Law within the organization.

Article 12/5: Failure to notify the Board and pertaining persons within a reasonable time about the processed personal data being unlawfully obtained by others.

Article 15/5: Failure to comply with the instructions and orders of the Board for the elimination of violations.

As indicated in the table above, the majority of sanctions imposed in decisions published by the Board are based on Article 18/1 (b), regulating administrative fines due to non-compliance with data security rules outlined in Article 12 of the DP Law. The reason for this lies in the fact that the DP Law provides sanctions only for violations of Article 10, 12, 15, and 16, without specifying any penalties for breaches of Article 4, 5, and 6. Therefore, the enforcement predominantly relies on Article 18/1 (b), emphasizing non-compliance with data security regulations.

No:	Data Controller	Sector	Violated Article	Total Fine	Date
1.	Unspecified	E-Commerce	Article 12/1	TRY 3,250,000	8 August 2024
2.	WhatsApp	Information Technologies and Media	Article 12/1	TRY 1,950,000	12 January 2021
3.	Yemeksepeti	Information Technologies and Media	Article 12/1	TRY 1,900,000	23 December 2021
4.	TikTok	Information Technologies and Media	Article 12/1	TRY 1,750,000	1 March 2023
5.	Facebook	Information Technologies and Media	Article 12/1, Article 12/5	TRY 1,650,000	11 March 2019
6.	Facebook	Information Technologies and Media	Article 12/1, Article 12/5	TRY 1,550,000	18 September 2019
7.	Various Factoring Companies	Banking and Finance	Article 12/1, Article 12/5	TRY 1,500,000	03 March 2020
8.	Marriott International	Tourism	Article 12/1, Article 12/5	TRY 1,450,000	16 May 2019
9.	Amazon	E-Ticaret	Article 18/1, Article 12/1	TRY 1,200,000	27 February 2020
10.	Unspecified	Gaming	Article 12/1, Article 12/5	TRY 1,100,000	16 April 2020
11.	Unspecified	Banking and Finance	Article 12/1	TRY 1,000,000	05 May 2020
12.	Unspecified	Information Technologies and Media	Article 12/1	TRY 950,000	17 March 2022
13.	Unspecified	Automotive	Article 12/1	TRY 900,000	22 July 2020
14.	Unspecified	Healthcare	Article 12/1, Article 12/5	TRY 800,000	27 April 2021
15.	Unspecified	E-Commerce	Article 12/1	TRY 800,000	10 March 2022
16.	Unspecified	Gaming	Article 12/1	TRY 750,000	28 Septembe 2023
17.	Dubsmash Inc.	Information Technologies and Media	Article 12/1, Article 12/5	TRY 730,000	17 July 2019
18.	Unspecified	E-Commerce	Article 12/1, Article 12/5	TRY 600,000	20 April 2021
19.	Clickbus Seyahat Hizmetleri A.Ş.	Transportation	Article 12/1, Article 12/5	TRY 550,000	16 May 2019
20.	Cathay Pasific Airway Limited	Transportation	Article 12/1, Article 12/5	TRY 550,000	16 May 2019
21.	Unspecified	E-Commerce	Article 12/1	TRY 500,000	11 April 2023

[36] This study includes the decisions published on the Board's official website. In addition, there are administrative fines with higher amounts that have been reflected to the public through various news outlets.

MOROĞLU ARSEVEN

III. The Board's Decisions

1. The Board's Principal Decisions

The Board has not published any principal decisions during 2023–2024 up to the publication date of this document. You can review the latest principal decisions published by the Board in "The Turkish Data Protection Law in 2023 | Developments in Practice Over its Seven Years – Updated Edition".

2. Summaries of Key Decisions

2.1. Registry Exemption of Village Legal Entities from VERBIS Registration Obligation

In its Decision No. 2023/2135, dated 14 December 2023, the Board, following an evaluation under Article 16/2 of the DP Law and Article 16/1 of the Regulation on the Data Controllers' Registry, decided to exempt village public legal entities from the obligation to register with VERBIS. The decision was published in the Official Gazette No. 32427 dated 12 January 2024 and entered into force.

2.2. Unlawful Processing of Personal Data for Subscription Purposes

In the complaint filed by the data subject, it was stated that, while researching new tariffs due to the expiration of their internet subscription term, they accidentally accessed a website that appeared to belong to Company A Electronic Communications. After entering their mobile phone number on the site, an individual contacted them and obtained their Turkish Citizenship Number (TCKN) and other personal data. The data subject was misled with information about a port change in the current subscription infrastructure and unknowingly had a subscription established with Brand X. As a result of the complaint applications, the relevant record was converted to a passive subscription on the e-Government platform but was not entirely deleted from the company's systems. Within the scope of the investigation initiated regarding the complaint, the following findings were identified:

It was determined that Company B had no involvement in the processing of personal data or the subscription processes related to the incident in question. It was identified that Company B was merely the sole shareholder of Company D, which was responsible for managing Brand X subscription processes as part of its operational activities. Consequently, the Board decided not to take any action against Company B under the DP Law.

Company D was found to be responsible for managing Brand X subscription processes. However, it was established that the data processing activities in the incident were carried out by Company C/Dealer without the knowledge of Company D. Although Company C/Dealer was required to act in accordance with the "Solution Partnership Agreement" executed with Company D, it was determined that Company C/Dealer had acted independently, in violation of the agreement, and assumed the role of an independent data controller. In this context, it was concluded that Company D had ceased to qualify as a data controller, and no action was taken against Company D under the DP Law.

Company C/Dealer was found to have collected personal data through misleading websites and processed this data without relying on any lawful basis under Article 5 of the DP Law. The investigation revealed that Company C/Dealer had unlawfully obtained the personal data of the data subject through deceptive methods and failed to meet the processing conditions required by Article 5 of the DP Law. Furthermore, it was determined that Company C/Dealer had failed to implement necessary technical and administrative measures to ensure the security of personal data, thereby violating the obligations related to data security under Article 12 of the DP Law. For these reasons, an administrative fine of TRY 450,000 was imposed on Company C/Dealer pursuant to Article 18 of the DP Law.

The lawfulness of the subscription establishment process and the data subject's request for the deletion of subscription records were also thoroughly evaluated. It was determined that, following the complaint applications, the subscription record was converted into a passive subscription on the e-Government platform, but it was not entirely deleted from the system. Under the DP Law and the general statute of limitations provisions, the retention of records related to past subscription information during the limitation period was deemed lawful, and it was concluded that complete deletion of the record was not necessary. Therefore, no action was taken regarding the request for the deletion of the relevant record.

In conclusion, as a result of the decision rendered by the Board:

- No action was taken against Company B, as it was determined to have had no involvement in the processing of personal data or subscription processes related to the incident.
- No action was taken against Company D, as it was concluded that Company C/Dealer acted independently as a data controller in violation of their agreement, thus absolving Company D of its data controller responsibilities for the incident.
- Company C/Dealer was fined TRY 450,000 under Article 18 of the DP Law for unlawfully obtaining and processing personal data, failing to implement necessary technical and administrative measures, and violating obligations related to data security.
- The data subject's request for the deletion of subscription records was denied, as it was deemed lawful to retain such records during the statute of limitations period in accordance with the DP Law and relevant provisions.

2.3. Data Breach Notification Reported to the Authority by an E-Commerce Platform

In its Decision No. 2024/1385, dated 8 August 2024, the Board concluded that an e-commerce platform had violated the data security obligations outlined in Article 12/1 of the DP Law. The violation occurred due to the data controller's failure to implement adequate technical and administrative measures prior to the breach and delays in detecting the breach. The relevant data breach was reported to the Authority by the data controller through a personal data breach notification and other communications, with the following details provided:

- The data controller operated an e-commerce platform where users in the role of sellers could list and sell their products.
- Unauthorized individuals gained access to certain seller accounts on the platform's seller portal by acquiring usernames and passwords from other platforms and attempting to enter them on the data controller's seller portal.
- The usernames and passwords involved in the breach were not leaked from the data controller's systems; instead, unauthorized individuals used credentials obtained from other platforms to access certain accounts on the seller portal.
- The breach occurred between 2 February 2024 and 6 February 2024, but the data controller detected it on 6 February 2024 following complaints from customers and sellers.
- The breach affected a total of 673 sellers (including seller representatives and individual sellers) and 7,202 customers who had recently made purchases through the affected seller stores, as determined through log analysis.
- Out of the 673 compromised seller accounts, 107 accounts were manipulated for illicit gains, including changes to IBANs, listing new products, and lowering product prices. Additionally, customer information accessible through these accounts was also accessed.
- Out of the 7,202 affected customer accounts, suspicious orders were created on 1,213 accounts.
- The categories of personal data affected in the breach were:
  - » For sellers: identity (name, surname, TCKN, signature), contact (phone number, email address), financial (IBAN, invoice).
  - » For customers: identity (name, surname, TCKN), contact (phone number, shipping address), customer transaction (purchase history, shipping delivery date and time, recipient details), financial (invoice).

Following the Board's evaluation, significant deficiencies in the technical and administrative measures that the data controller should have implemented both prior to and during the breach were identified. The Board emphasized the following points in its decision:

- YUnauthorized individuals accessed accounts on the seller portal by testing email addresses and password credentials obtained from other platforms. During this process, a vulnerability in the data controller's systems was exploited, and attackers conducted a targeted attack using the account information they possessed.
- The data controller's application to prevent bot traffic was deemed inadequate. It was found that cyber attackers bypassed this application to gain access to the systems.
- Additional security measures, such as two-factor authentication (2FA) for login processes on the seller portal, were implemented only after the breach occurred. The Board assessed that such a measure, if implemented earlier, could have significantly mitigated the impact of the attack.
- The data controller failed to analyze log records indicating more than 400 user logins from the same IP address on 2 February 2024 and 3 February 2024, the days when the breach began. This oversight delayed the detection and intervention of the breach, which was only discovered on 6 February 2024 following complaints from customers and sellers.
- It was determined that a one-time password (OTP) system, which should have been triggered during logins from a new IP address or during the first login, was implemented only after the breach occurred. This omission allowed the breach to spread more widely.
- The Board noted that the measures implemented after the breach could have significantly limited the scope of the incident if they had been in place beforehand.

It was determined that the data controller violated the data security obligations stipulated in Article 12 of the DP Law by failing to take adequate measures to prevent unlawful access to personal data. Considering the data controller's fault, the severity of the violation, and the economic circumstances of the data controller, the Board imposed an administrative fine of TRY 3,250,000 pursuant to Article 18/1(b) of the DP Law.

C. EXPECTED DEVELOPMENTS

I. Law Amendment

As part of the Law Amendment, efforts to align the DP Law with the GDPR accelerated in 2024 and remain a key component of Türkiye's digital transformation strategy. With respect to the Annual Program (see Section A.IX.6), the alignment of the DP Law with the GDPR and the EU acquis is set to be completed. Similarly, the "Medium-Term Program (2025–2027)," prepared by the Ministry of Treasury and Finance and the Presidency's Strategy and Budget Directorate, was approved by Presidential Decision No. 8906 and published in the duplicate edition of the Official Gazette No. 32653 dated 5 September 2024. Like the Annual Program, the Medium-Term Program includes the completion of the alignment process of the DP Law with the GDPR and other EU digital economy regulations, focusing on their implications for goods and services exports. The projected timeline for completing the alignment process has been set as the fourth quarter of 2025.

This alignment process aims to strengthen Türkiye's integration into the EU's digital economy regulations. Furthermore, under the Türkiye International Direct Investment Strategy (2024–2028) (see Section A.IX.4), the completion of GDPR alignment has been identified as a priority objective. As stated in the aforementioned documents, the full alignment of the DP Law with the GDPR and the related regulations is expected to be completed in 2025.

MOROĞLU ARSEVEN

II. Regulation of Platform Data and the Right to Data Portability

On 7 July 2022, Law No. 7416 Amending the Law on the Regulation of Electronic Commerce was published in the Official Gazette No. 31889, followed by the issuance of the Regulation on Intermediary Service Providers and Service Providers in Electronic Commerce in the Official Gazette No. 32058 dated 29 December 2022. Amendments to Law No. 6563 on the Regulation of Electronic Commerce ("**E-Commerce Law**") introduced obligations for electronic commerce intermediary service providers to ensure data portability, which became effective on 1 January 2024. Accordingly, intermediary service providers with a net transaction volume exceeding TRY 10,000,000,000 in a calendar year are required to provide technical capabilities that enable the free transfer of data obtained from the sales of electronic commerce service providers and ensure free and effective access to this data and any derived processed data.

Beyond e-commerce regulations, developments concerning data usage on digital platforms have continued to emerge within the framework of competition law. On 14 October 2022, a draft amendment to Law No. 4054 on the Protection of Competition ("**Competition Law**") was shared with relevant stakeholders for feedback, aiming to address the protection of competition in digital economies. Subsequently, the Competition Authority proactively examined the intersection of data portability and competition law, imposing administrative fines on dominant undertakings such as META. For example, META was penalized for combining data collected from its core services—Facebook, Instagram, and WhatsApp. The Competition Board determined that this practice hindered competitors' activities in the personal social networking and online display advertising markets and created barriers to market entry, thereby distorting competition and violating the Competition Law. By 2024, the anticipated amendments to the Competition Law had not yet been enacted. However, the Competition Board continued imposing administrative fines on digital platforms for practices that disrupted the competitive environment through data usage and violated relevant provisions of the Competition Law.

Given the increasing role of data usage and portability in shaping the competitive environment and the dominant position of digital platforms in the market, the finalization of the draft Competition Law and its legislative process are expected to progress in 2025. Data portability in the fields of competition and e-commerce continues to dominate the agenda, with regulatory implications becoming evident. Furthermore, as mentioned in Section C.I., during the alignment of the DP Law with the GDPR, Article 20 of the GDPR, addressing data portability, is expected to be incorporated into the DP Law. In 2024, the Authority maintained its efforts in this regard by organizing a Wednesday Seminar titled "*Data Portability from the Perspective of Competition Law*" to inform the public about the topic. As such, regulations concerning data portability and the use of personal data as a critical competitive input have begun to emerge, with further developments expected in the near future.

MOROĞLU ARSEVEN

III. Regulations on Children's Personal Data

Since 2019, the Board has undertaken several awareness initiatives regarding the protection of children's personal data. However, no specific guide or public announcement has yet been published on the matter. The 2024–2028 Strategic Plan includes objectives aimed at educating children and youth about the importance of personal data and raising awareness among school-aged children and youth. In line with these objectives, the Authority continued its efforts in its April–July 2024 Bulletin (Issue 5) titled "*Privacy in the Digital Age: Protecting Children's Personal Data*."

Additionally, the Authority launched the "DP Law in Schools Project" in collaboration with the Ministry of National Education to raise awareness among children and youth about personal data, online privacy, and data protection. The project was officially announced on 25 April 2024 through the Authority's website. Under this initiative, informational events are being organized for 8th-grade students at designated primary schools, with the opening ceremony held in Adana by the Authority's President, Prof. Dr. Faruk Bilir. During these events, students are provided with age-appropriate presentations, awareness videos, and training on topics such as creating strong passwords, safe online shopping, and data security on social media platforms.

On 8 October 2024, the Authority published informative posters and brochures on its official website to enhance children's awareness of personal data security. Furthermore, on 9 October 2024, the Authority introduced child-friendly educational content titled "*Learning About Personal Data with Verican*" to teach the fundamentals of data protection in an engaging and educational manner. All these initiatives were consolidated on the Authority's "*DP Law for Children*" section, which was launched on 20 November 2024 in recognition of World Children's Day.

Looking ahead, amendments to strengthen the protection of children's personal data on online platforms (such as social media and gaming sites) are anticipated. Additionally, the Board is expected to publish a guide in 2025 detailing best practices for processing children's personal data.

MOROĞLU ARSEVEN

IV. Financial Data Access

The European Commission published the Payment Services Directive 3 (PSD3), Payment Services Regulation 1 (PSR1), and Financial Data Access Regulation (FDAR) on 28 June 2023 as part of the Financial Data Access and Payments Package. This marked a significant step toward updating regulations governing the financial sector, including payment systems, within the EU. The package aims to enhance the synchronization of the payment and financial sectors with the digital era, improve competition in electronic payments, and provide consumers with access to financial products and services that enable the secure sharing of their data. In this context, the European Data Protection Supervisor (EDPS) published Opinion No. 38/2023, evaluating the Financial Data Access Regulation under the GDPR, on 22 August 2023.

In Türkiye, while the Board had previously issued the *Good Practice Guide on Personal Data Protection in the Banking Sector*, which provided detailed explanations on personal data protection specific to the banking industry, the Authority published an updated version of the guide on its official website on 8 January 2025. The updated banking guide outlines the procedures and principles that banks must comply with under the DP Law and related secondary legislation, presenting them alongside good practice examples. The guide was revised in relation to the Law Amendment.

In addition, Türkiye's legal framework contains strict regulations to protect primary system data in the financial and payment sectors, including finance and factoring companies. To address this, the Authority organized a workshop on 23 December 2024 to develop a "*Good Practice Guide on Personal Data Protection in the Payment and Electronic Money Sector*." The guide is expected to provide explanations on the protection of primary system data and the compliance of personal data included in these systems with the DP Law. This will reinforce personal data protection in the payment and electronic money sectors under the relevant regulations.

MOROĞLU ARSEVEN

V. Artificial Intelligence

On 24 June 2024, the Artificial Intelligence Bill was submitted to the TBMM for the first time. The bill aims to promote the use of artificial intelligence systems while protecting individuals' rights and freedoms, ensure the development and utilization of these technologies within a fair and ethical framework, and create a competitive and innovative environment aligned with international standards. To assess the benefits of artificial intelligence, establish a legal framework in this field, and mitigate risks associated with its use, political parties jointly proposed the formation of a Parliamentary Research Commission on Artificial Intelligence ("**AI Commission**"), which was unanimously approved. The decision to establish the AI Commission was published in the Official Gazette No. 32683 dated 5 October 2024. The AI Commission, comprising 22 members, was granted a working period of 3 months. With the TBMM Decision published in the Official Gazette No. 32784 dated 16 January 2025, the members of the AI Commission were appointed, and the commission became fully operational. (For detailed explanations on the scope of the AI Commission's activities and the Artificial Intelligence Bill, please refer to Section A.II.2. Developments in Artificial Intelligence.)

During this process, the UNDP Türkiye Country Office and the Central Digital Office published the "*Proposal Report on the Data Governance Framework for Türkiye*," presenting strategic recommendations for Türkiye's data-driven digital transformation. The report emphasizes the critical role of artificial intelligence and data analytics technologies in this transformation. It highlights that AI-powered tools, particularly in fields such as healthcare, agriculture, education, and public services, can contribute to the development of effective policies. In parallel, the Council of Higher Education (YÖK) released the "*Ethical Guidelines on the Use of Generative Artificial Intelligence in Scientific Research and Publishing Activities in Higher Education Institutions*." This guide establishes ethical principles and data protection requirements related to the use of artificial intelligence. It aims to prevent unethical applications of AI technologies, raise awareness of potential legal issues arising from their use, and emphasize adherence to the principle of personal data protection.
Furthermore, as outlined in Section A.IX.4, Türkiye's strategic plans and objectives include detailed initiatives regarding the use of artificial intelligence. In 2025, it is expected that steps will be taken to achieve these objectives, including the enactment of the Artificial Intelligence Bill, and the development of best practices, guides, opinions, and public announcements under the scope of DP Law regulations.

MOROĞLU ARSEVEN

VI. Cyber Security

As of January 2025, significant developments have taken place in the field of cybersecurity, and activities in this area have gained momentum. With Presidential Decree No. 177, published in the Official Gazette on 8 January 2025, the establishment of the Cybersecurity Directorate was approved. Operating under the Presidency, this directorate will assume key responsibilities, including the formulation of national cybersecurity policies, execution of regulatory frameworks, and conducting public awareness initiatives. Following the establishment of the Cybersecurity Directorate, the Cybersecurity Bill was submitted to the National Defense Committee of the Grand National Assembly of Türkiye (TBMM) on 10 January 2025 and was approved. The bill is expected to be enacted within 2025. (For detailed information on the scope of the Cybersecurity Bill and the roles and responsibilities of the Cybersecurity Directorate, refer to Section A.II.3. Legislative Developments in Cybersecurity.)

MOROĞLU ARSEVEN

APPENDIX 1 KEY TERMS

Personal Data is any information relating to an identified or identifiable natural person. Any information that can be used to identify a person is personal data. For example, a database of a customer's name and address, IP address, email address, or customer email address is personal data.

Special Category Personal Data is data about a real person's race, ethnicity, political opinion, philosophical belief, religion, sect or other beliefs, disguise and dress, membership of associations, foundations or trade unions, health, sexual life, criminal convictions, and security measures. Biometric and genetic data is personal data of a special nature. The definition of special category personal data in the DP Law in relation to clothing, criminal convictions, and security measures is more comprehensive than the protection of biometric and genetic data in EU regulations for the protection of special quality personal data.

Data Controller refers to a natural or legal person who determines the purposes and means of processing personal data and is responsible for the establishment and management of the data recording system.

Data Processor means a natural or legal person who processes personal data on behalf of a data controller, based on the authority given by the data controller.

Explicit Consent means the informed consent on a particular subject given by a data subject by free will. The DP Law envisages the processing of personal data or special category personal data with explicit consent as the rule. However, a specific method for obtaining explicit consent is not regulated under DP Law. In this context, data controllers can receive explicit consent in writing, electronically, or verbally. In any case, the burden of proof for obtaining explicit consent rests with the data controller.

Processing of Personal Data refers to the obtaining, recording, storing, preserving, changing, rearranging, disclosing, transferring, taking over, or making available of personal data, fully or partially, automatically or by non-automatic means, provided that it is a part of any data recording system. It also refers to any operation performed on data such as classification or prevention of use.

Data Controllers Registry Information System (VERBIS) is the information system created and managed by the Presidency of the Personal Data Protection Agency, accessible over the internet, that data controllers must use in applications to the Data Controllers Registry and other related transactions.

MOROĞLU ARSEVEN

APPENDIX 2 STEPS TO BE IMPLEMENTED IN CROSS-BORDER DATA TRANSFER PROCESSES (CROSS-BORDER DATA TRANSFER GUIDELINES)

6698 Personal Data Protection Law Article 9 - Transfer of Personal Data Abroad (After The Amendment)

Personal data may be transferred abroad if there are provisions stipulated in international agreements or other laws.

If there are no provisions stipulated in international agreements or other laws

Provided that one of the conditions specified in Articles

If there is an Adequacy Declaration

Personal data may be transferred abroad.

If one of the appropriate safeguards is in place

- **Standard Contract***
- **Bindind company rules approved by the Authority.**

Personal data may be transferred abroad.

- **Existence of an agreement that is not an international contract.**
- **A commitment letter**

+
Approval for the transfer granted by the Authority

Personal data may be transferred abroad.

If there is no Adequacy Declaration

If none of the appropriate safegurards are in place

If there is one of the exceptional transfer cases

Personal data may be transferred abroad.

If there is none of the exceptional transfer cases

Personal data cannot be transferred abroad.

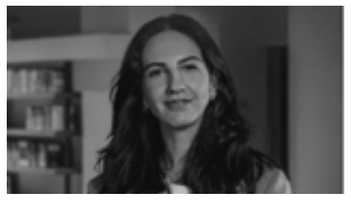
[37] Only Available in Turkish.

* The standard contract must be reported to the Authority by the data controller or data processor within five business days after its signing.

MOROĞLU ARSEVEN

Authors

BURCU TUZCU ERSİN, LL.M.
Partner
btuzcu@morogluarseven.com
D: +90 (212) 377 47 50
T: +90 (212) 377 47 00



BURCU GÜRAY
Partner
bguray@morogluarseven.com
D: +90 (212) 377 47 25
T: +90 (212) 377 47 00

CANSU ÖZGÜVEN, LL.M.
Senior Associate
cozguven@morogluarseven.com
T: +90 (212) 377 47 00

AYŞEGÜL DAĞHAN
Associate
adaghan@morogluarseven.com
T: +90 (212) 377 47 00

MOROĞLU ARSEVEN

www.morogluarseven.com

Abdi Ipekçi Caddesi 19-1
Nişantaşı, İstanbul, 34367

T: +90 212 377 4700
F: +90 212 377 4799
info@morogluarseven.com