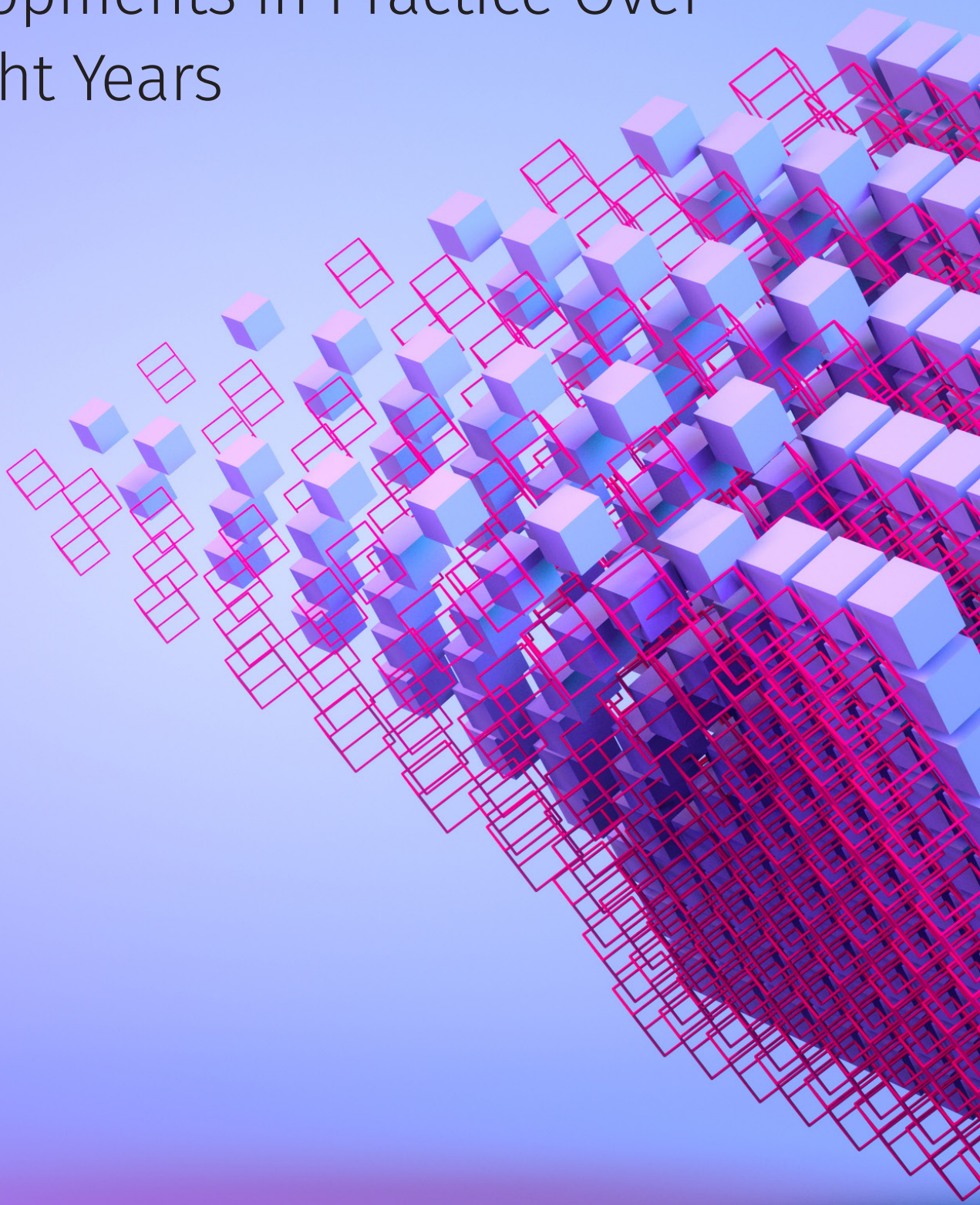
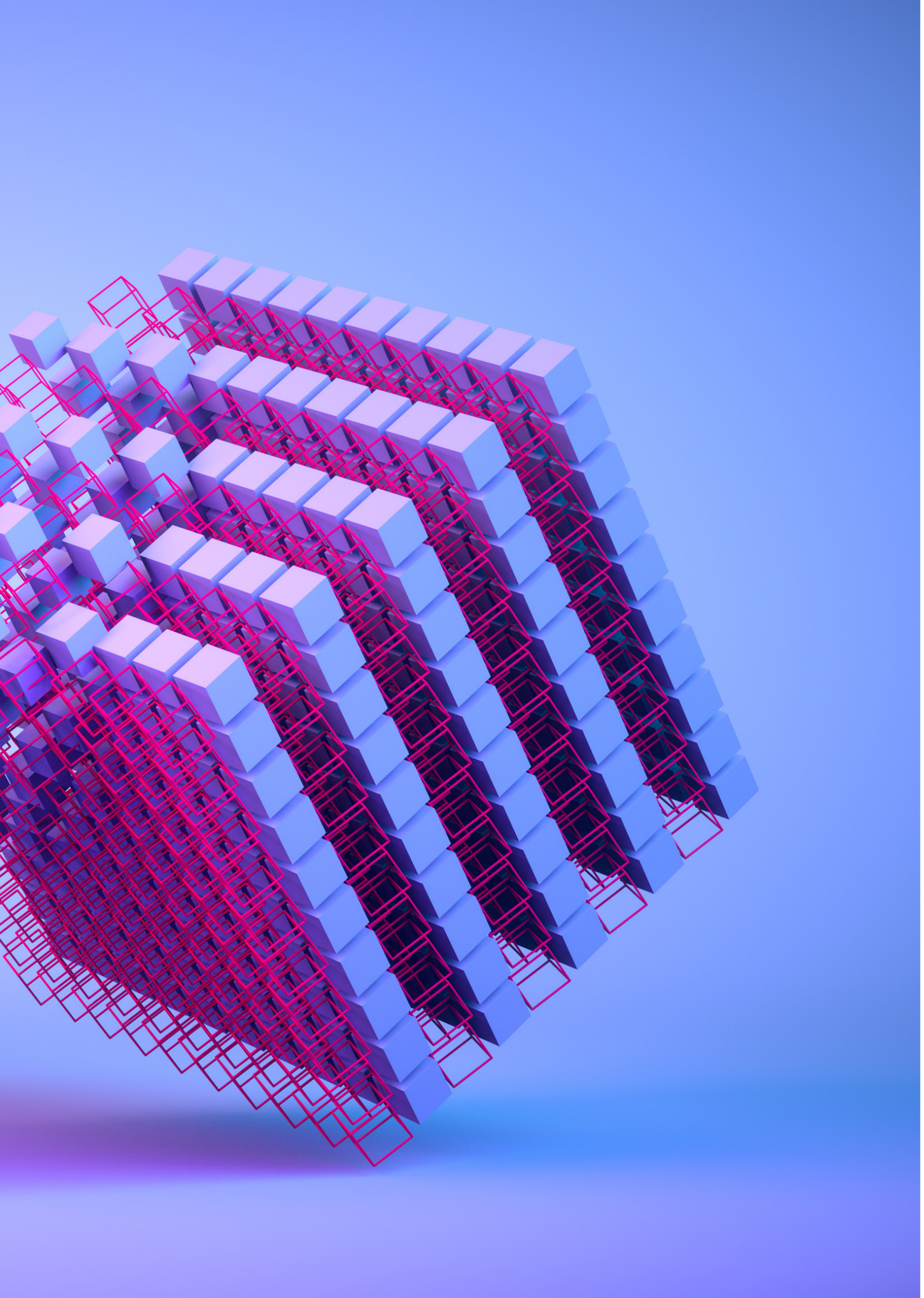
The Turkish Data Protection Law in 2023

Developments in Practice Over its Eight Years



MOROĞLU ARSEVEN



Preface

With reference to the Personal Data Protection Law numbered 6698, this study, written in the law's fifth year of enactment, and shared with you in a fourth edition this year, pertains specifically to the period between 1 January 2023 and 31 December 2023, marking its eighth year of implementation. It encompasses the aspects that require attention in relation to compliance with the Personal Data Protection Law, changes in practices, and the approach of the Personal Data Protection Board during this period. We, Moroğlu Arseven, take pleasure in presenting our work to you.

This study has been prepared based on data found in the activity report of the Personal Data Protection Board for 2022, published on 12 April 2023, and public announcements, works, and decisions published on the official website of the Personal Data Protection Board as of the date of publication.

Contents

MOROĞLU ARSEVEN

MOROĞLU ARSEVEN

A. MAJOR DEVELOPMENTS IN LEGISLATION AND PRACTICE

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 Law on Personal Data Protection numbered 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 numbered 5237.

Within 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.

II. Legislation and Regulations on Data Protection and Privacy

In 2023, while there were no direct developments within the scope of the DP Law, several regulations were enacted in other laws and secondary legislation. The relevant changes are listed below in the order of regulations and circulars.

1. The Regulation on Issuing Identity Cards to Disabled Individuals and Establishing the National Disabled Data System

The Regulation on Issuing Identity Cards to Disabled Individuals and Establishing the National Disabled Data System, published in the Official Gazette dated 12 May 2023 and numbered 32188, aims to provide identity cards to disabled individuals and to create a National Disabled Data System to enable such individuals to benefit from rights and services. Accordingly, the regulation outlines the procedures and principles for issuing disabled identity cards ("**Identity Cards**") to adults with a minimum of a 40% disability rate or children with special needs, and it establishes the guidelines for the National Disabled Data System.

The Regulation on Issuing Identity Cards to Disabled Individuals and Establishing the National Disabled Data System outlines the conditions under which an Identity Card will be destroyed and mandates that the destruction process must be completed within one month. Provisions have been established to address situations such as the use of cards containing alterations, erasures, or scratches, individuals using another person's identity card, those who issue cards with incorrect information, individuals continuing to use their cards despite an obligation to return them, or those intentionally altering their cards. Penalties and criminal investigations will be initiated against individuals involved in such activities.

Within the scope of the Regulation on Issuing Identity Cards to Disabled Individuals and Establishing the National Disabled Data System, the National Disabled Data System is defined as a database where personal data regarding disabled individuals is processed when transferred from other institutions and organizations or obtained during identity card procedures. Furthermore, the necessary services for the National Disabled Data System will be provided by the Ministry of Family and Social Services, and the technical work for establishing the Data System will be conducted by the Ministry's General Directorate of Information Technologies.

Moreover, the Regulation on Issuing Identity Cards to Disabled Individuals and Establishing the National Disabled Data System comprehensively addresses the principles and procedures regarding data security, processing, and transfers of personal data within the framework of the National Disabled Data System. In alignment with these principles and procedures:

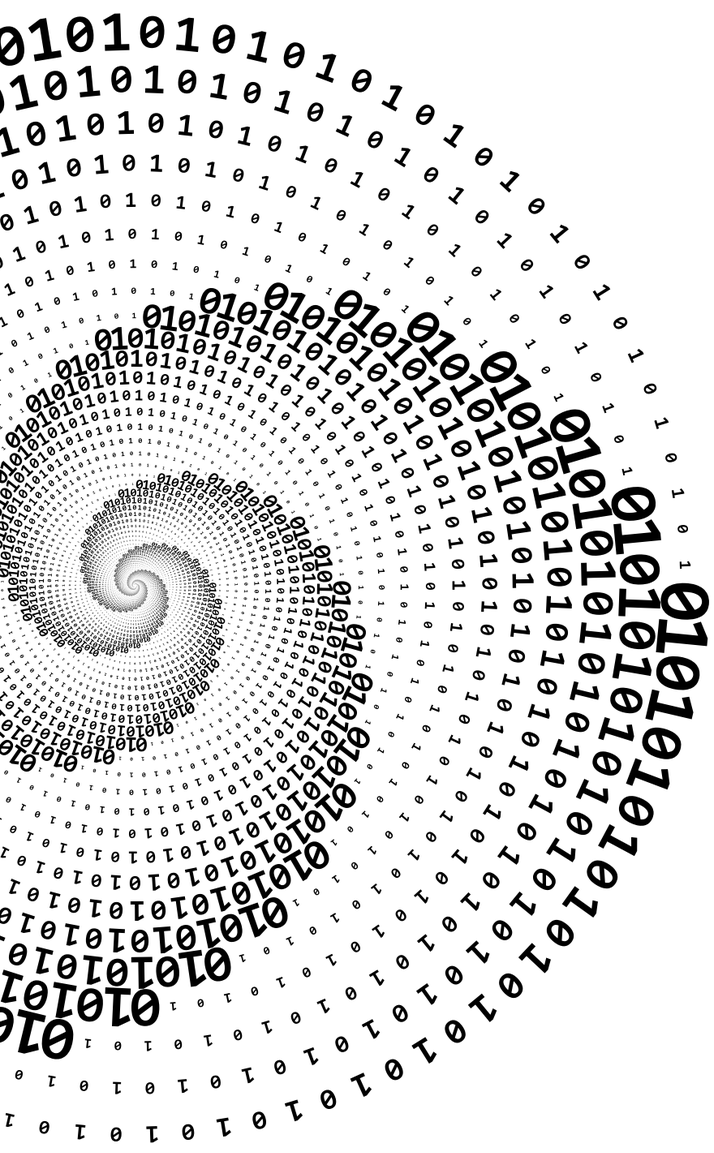
- The transferring party assumes responsibility for ensuring the accuracy and currency of information conveyed to the National Disabled Data System.
- As the data controller, the Ministry of Family and Social Services will take necessary measures to ensure the accuracy and currency of personal data transferred to it by other individuals, institutions, or organizations providing services to individuals with disabilities.
- The confidentiality of personal data within the National Disabled Data System is paramount. To prevent the unlawful processing and unauthorized access to data and to ensure the preservation of personal data, the Ministry of Family and Social Services will implement all necessary technical and administrative measures to achieve an appropriate level of security. The Information Technologies General Directorate will be authorized to implement these measures.
- The fundamental principle within the National Disabled Data System is the confidentiality of personal data. To prevent unlawful processing and unauthorized access to personal data, as well as to ensure the preservation of such data, the Ministry of Family and Social Services will undertake all necessary technical and administrative measures to establish an appropriate level of security. The Information Technologies General Directorate is authorized to oversee the implementation of these measures.
- All processes involving personal data, including processing, transfer, deletion, erasure, and anonymization, will be conducted in accordance with the provisions of the DP Law and relevant legislation.
- There is an obligation to sign a protocol for the transfer of data through continuous or one-time information sharing, or web service requests with the Ministry of Family and Social Services.
- The responsibility for ensuring the confidentiality and security of personal data transferred by the Ministry of Family and Social Services will rest entirely with the requester of the data transfer, without any limitations regarding duration.
- Personal data transferred by the Ministry of Family and Social Services cannot, under any circumstances, be made available or disclosed to third parties.
- Special categories of personal data can only be transferred to third parties under the conditions stipulated by the DP Law, and explicit consent from the data subjects is a prerequisite for such transfers.

2. The Regulation Regarding the Amendment of the Regulation on Remote Identification Methods to be Used by Banks and the Establishment of Contractual Relationships in the Electronic Environment

The Regulation Amending the Regulation on Remote Identification Methods to be Used by Banks and the Establishment of Contractual Relationships in the Electronic Environment was published in the Official Gazette dated 25 May 2023 and numbered 21201, with the purpose of making changes to the procedures and principles related to it. It is set to become effective on 1 June 2023.

The notable details included in the relevant regulation are as follows:

- The remote identification process will be designed in accordance with the general principles outlined in the Regulation on Banking Services Accessibility published in the Official Gazette dated 18 June 2016 and numbered 29746, ensuring accessibility to banking services. The controls specified in the Regulation Amending the Regulation on Remote Identification Methods to be Used by Banks and the Establishment of Contractual Relationships in the Electronic Environment will be tailored based on the specific conditions of individuals with disabilities.
- In case there is a need for assistance during the video call stage of remote identification for individuals with disabilities, third-party assistance may be sought, and the customer representative can generate photos and/or screenshots showing the front and back of the identity document of the assisting third party along with the individual with disability's own identity document.
- In determining the identity of a legal entity, the identity of the individual will be established in accordance with the Regulation on Remote Identification Methods to be Used by Banks and the Establishment of Contractual Relationships in the Electronic Environment, and the authorization to represent the legal entity will be verified. If the person's identity is already verified as a customer of the same bank and they have logged into any session through internet banking or mobile banking distribution channels, the verification through near-field communication with the identity document, as stipulated in the Regulation on Remote Identification Methods to be Used by Banks and the Establishment of Contractual Relationships in the Electronic Environment, will be considered fulfilled.
- The authorization of an individual to represent a legal entity will be verified by matching the information obtained from the person with the current data retrieved from Central Registration System ("MERSIS") and/or the Trade Registry Gazette. If deemed necessary by the bank, the customer representative will acquire a sample of the power of attorney circular provided by the individual, demonstrating their authorization to represent the legal entity. The signature sample obtained from the power of attorney circular will be compared with the signature sample found on the individual's identity document and/or MERSIS. Additionally, the validity of the power of attorney circular will be confirmed using the date and registry number. The confirmation of the signature, as regulated by the Banking Regulation and Supervision Agency ("BRSA"), can be conducted through both MERSIS records and the signature on the individual's new ID card. Authorized individuals representing legal entities will be able to perform remote banking transactions through remote identification. In this context, inclusive changes to the definition of "Customer" in the Financial Crimes Investigation Board ("FCIB") Communiqué No:19 have been implemented following the publication of the Regulation Amending the Regulation on Remote Identification Methods to be Used by Banks and the Establishment of Contractual Relationships in the Electronic Environment.



- Furthermore, the information obtained regarding the legal entity will be confirmed by matching with current data queried from the databases of MERSIS, the Trade Registry Gazette, and the Revenue Administration.
- The BRSA will have the authority to determine the procedures and principles for the implementation of processes stated to be performed by customer representatives in the Regulation on Remote Identification Methods to be Used by Banks and the Establishment of Contractual Relationships in the Electronic Environment, concerning financial, factoring, and financial leasing companies using artificial intelligence-based methods in a manner similar to the remote identification processes.

3. Regulation Amending the Regulation on Pre-School Education and Primary Education Institutions of the Ministry of National Education

The Regulation Amending the Regulation on Pre-School Education and Primary Education Institutions of the Ministry of National Education was published and entered into force on the same day, as announced in the Official Gazette dated 14 October 2023. According to this amendment, photos of students taken during educational activities, social and cultural events, as well as excursions and observation activities both within and outside the school premises, cannot be shared on social media platforms and communication groups without written permission from the parents and the supervision of the guidance counselor. Consequently, photos of children in activities at pre-school education and educational institutions can only be shared on social platforms with the consent of parents or the child.

4. The Circular Regarding the Use of Open-Source Software in the Public Sector Numbered 2023/13

In order to promote the use of open-source software in the public sector and achieve savings in information technology expenses, reduce dependency on software vendors, and enhance cybersecurity, the Presidency of the Republic of Turkiye published "The Circular Regarding Use of Open-Source Software in the Public Sector numbered 2023/13" in the Official Gazette dated 29 July 2023 and numbered 32262. In this regard, the fundamental points outlined below have been set out:

- An "Open-Source Software Transition Analysis and Roadmap Report," conforming to the template announced on the official website of the Digital Transformation Office and an "Open-Source Software Transition Analysis Guide," should be prepared, providing an inventory of commercially licensed software used in accordance with the template and submitted to the Digital Transformation Office. This report should identify which of these commercial software applications can be replaced with their open-source equivalents.
- Measures should be taken to allocate the necessary financial resources and workforce for the activities to be carried out in accordance with the created Open-Source Software Transition Analysis and Roadmap Report.
- During the procurement process of goods and services, preference should be given to open-source software ("OSS") alternatives instead of commercial licensed software. However, this regulation may not be applied in cases where OSS alternatives are not technically and economically feasible. In such cases, detailed technical and economic justifications for not choosing OSS alternatives for the envisaged commercial licensed software should be provided in the project proposal forms submitted to the Strategy and Budget Presidency for budget requests of this nature.
- Existing OSS developed and customized by software companies operating in Turkiye and personnel employed in Turkiye will be considered in the OSS transition process, even if they do not use OSS licenses in terms of software licensing procedures. These software solutions will be preferred over commercial licensed software if they meet the needs of the relevant public institutions and organizations in their technical and financial aspects, and if suitable OSS alternatives are not available.

MOROĞLU ARSEVEN

III.Documents Published by the Board in 2023

1.Academic Perspective on Personal Data Protection, DP Law Academy Compilation Study

As of 8 August 2023, the Authority has published a book titled “An Academic Perspective on Personal Data Protection: DP Law Compilation Study” consisting of works on the protection of personal data by academic experts in various fields of the law. The book covers studies related to the protection of personal data, privacy, data protection law, and the security of personal data. It includes assessments on both the fundamental concepts specified in the DP Law and evaluations related to the protection of personal data in other legal areas. The book is structured around topics such as the Right to Protection of Personal Data; Protection of Personal Data and Ethics; General Concepts; General Principles under the Personal Data Protection Law; Explicit Consent; Obligation to Respond to Applications Made by Data Subjects; Application and Complaint Procedures; Compliance with the Board’s Decisions; Crimes Related to Personal Data; Current Technology and Personal Data; Deletion, Destruction, or Anonymization of Personal Data; Sustainable Personal Data Security Governance; Blockchain and the Protection of Personal Data; Evaluations on the Implementation Issues of the Personal Data Protection Law in Artificial Intelligence; Protection of Personal Data in Civil Law Relations; Processing of Personal Data in the Field of Intellectual Property; Protection of Personal Data within the Framework of Civil Procedure Law; Processing of Personal Data in Labor Law; and Processing of Personal Data in the Health Sector.

2. DP Law Bulletins

As of April 2022, the Authority has been publishing DP Law Bulletins through videos as part of awareness and information-sharing efforts with the public on personal data protection. Starting from July 2023, under the title “DP Law Bulletin,” the bulletins are also being published in written form on the official website of the Authority. The DP Law Bulletin includes selected topics, opinion columns, articles, global developments, the activities of the Authority, and statistical information (complaints and reports received within a specific time frame, data breach notifications, administrative fines imposed, legal opinions, and approved commitments for transferring personal data abroad). Two bulletins have been published this year: (i) July 2023 Issue: 1 (Rethinking Privacy in the Era of Producer Artificial Intelligence), and (ii) July-September 2023 Issue: 2 (Traces Left in the Shadows: Right to be Forgotten).

3. 5. Anniversary of the Personal Data Protection Authority

The document titled “5th Anniversary of the Personal Data Protection Authority” was published on the official website of the Authority on 23 November 2022. This document provides detailed information about the organization’s structure and the public announcements made by the Authority over the five years. Additionally, numerical data regarding complaints, notifications, and applications submitted to the Authority, data breach notifications, imposed administrative fines, and, finally, details on corporate promotion, awareness, and consciousness-raising activities are presented in detail in the document.

MOROĞLU ARSEVEN

IV.Guidelines Published by the Board in 2023

1.Guide on Points to Consider in the Processing of Genetic Data

The "Guide on Points to Consider in the Processing of Genetic Data" ("**Genetic Data Guide**"), initially published as a draft by the Authority on 24 August 2022, was finalized and shared with the public on 13 October 2023. The Genetic Data Guide provides detailed information on (i) the definition of genetic data; (ii) data controllers, data processors, data subjects, and general principles in the processing of genetic data within the scope of the DP Law; (iii) the evaluation and international transfer of genetic data within the framework of the processing conditions for personal data specified in the DP Law; (iv) the responsibilities of the data controller and technical and administrative measures for the security of genetic data in the processing of genetic data; and (v) recommendations and suggestions for the processing of genetic data.

Genetic data, which is recognized as special category personal data under Article 6 of the DP Law, has gained a comprehensive definition for the first time with the Genetic Data Guide. The guide refers to the definition under the General Data Protection Regulation ("**GDPR**") of the European Union, ultimately stating that genetic data is "all or part of the information obtained from the living organism's genome, cell nucleus, or mitochondria, encoding all DNA, RNA, and protein sequences." Genetic data can encompass a single nucleotide polymorphism (SNP) or a comprehensive sequence of the entire genome. This information includes all hereditary or non-hereditary genomic changes obtained from DNA and/or RNA derived from a living organism. Additionally, the guide emphasizes the following points for genetic data:

- The need for analysis to be meaningful or informative.
- The value and significance of raw data and biological samples even before analysis, considering their potential to identifiably link to a real person.
- The possibility of analyzing samples from deceased data subjects years later in a way that could identifiably link to a real person.

Additionally, according to the Regulation on the Deletion, Destruction, or Anonymization of Personal Data, it is generally not possible to anonymize DNA samples or genetic data truly and completely. It is emphasized that with every anonymization method used, it is not feasible to completely sever the connection between the data obtained and the data subject. Therefore, instead of using the term anonymization, the concept of de-identification may be more appropriate for genetic data.

The Genetic Data Guide highlights that Genetic Disease Evaluation Centers must obtain a license from the Ministry of Health to operate, according to the Regulation on Genetic Disease Evaluation Centers. These centers are acknowledged to be data controllers for the Ministry of Health and universities, and they are allowed to conduct genetic tests only in cases of medical necessity or for medical-purpose scientific research, provided that appropriate genetic counseling services are offered.

The Genetic Data Guide emphasizes that, in the processing of genetic data, the data of relatives with genetic connections outside the data subject can be processed. Therefore, the processing of data from other data subjects may result in a different purpose.
Genetic data should be processed in accordance with the general principles of the DP Law. Within this framework, the processed genetic data should be stored only for the necessary duration and promptly destroyed according to the personal data storage and destruction policy when no longer needed. According to the Regulation on Genetic Disease Evaluation Centers, reports and records in the centers should be kept for a minimum of 30 years, electronic records must be backed up indefinitely, and samples and slides should be stored for at least two years under appropriate conditions.

According to Article 6 of the DP Law, the processing of genetic data is possible without the explicit consent of the data subjects in the cases specified in the law only. If the processing of genetic data is limited to health reasons only, and if it aligns with the purposes of protecting public health, preventive medicine, medical diagnosis, treatment, care services, and the planning and management of health services, it can be carried out without obtaining explicit consent, but only by individuals or authorized institutions bound by confidentiality obligations.

In accordance with Article 16 of the Regulation on Personal Health Data, studies involving genetic data should be conducted using data that does not make the data subject identifiable to the extent possible (a principle of processing genetic data as a last resort). This involves minimizing the risks related to personal data security through methods such as the use of pseudonyms. Thus, it is stated that this can be considered allowable within the scope of Article 28 of the DP Law.

[1] For detailed information on the draft guide on "Points to Consider in the Processing of Genetic Data," please refer to the "Draft Guide on Points to Consider in the Processing of Genetic Data" in the updated version of "Turkish Data Protection Law 2023: Developments in Practice in the Seventh Year."

The Regulation on Genetic Diseases Assessment Centers specifies that the sending of samples abroad within the scope of the regulation can be carried out by being registered through licensed genetic diseases assessment centers approved by the Ministry of Health. Additionally, human-derived biological samples for examination purposes will be recorded in the Ministry of Health's tracking system. Consequently, the sending of samples abroad for non-working tests will only be allowed through the "International Biological Material Transfer System," ensuring the safety and appropriateness of the process under the control of the Ministry of Health, and only by licensed Genetic Diseases Assessment Centers and medical laboratories. Furthermore, according to the Regulation on Medical Laboratories, the authority to send samples abroad for examination purposes can only belong to licensed medical laboratories. The entry and exit of human-derived biological samples for examination purposes can only be carried out with the approval of the Ministry of Health.

In addition, the Genetic Data Guide emphasizes that providing general explanations alone is not sufficient for informing data subjects whose genetic data is processed. In this regard, data subjects must be specifically informed about which genetic data is collected for what legal reasons and purposes, the significance of this data, and the potential consequences of a breach (the risks associated with the processing of genetic data). It is crucial to provide additional information to data subjects about the processing activities and outcomes of genetic data, making it clear that processing genetic data may grant access not only to the data of the data subjects concerned but also to the data of other family members.

Moreover, it is emphasized that the concept of "informing" mentioned in the Patient Rights Regulation is distinct from the "obligation to inform" that must be carried out before processing the personal data of the patient who qualifies as the "data subject" under the DP Law, and does not substitute for explicit consent.

Additionally, data controllers processing genetic data are obligated to register with VERBİS and to take necessary technical and administrative measures. Attention is drawn to compliance with the issues outlined in the Personal Data Protection Board Decision dated 31 January 2018, numbered 2018/10, regarding "Adequate Measures to be Taken by Data Controllers in the Processing of Special Categories of Personal Data." Data controllers are also advised to take the following measures specifically for processing genetic data.

Technical Measures

- Cloud Storage of Genetic Data: The Genetic Data Guide recommends avoiding the storage of genetic data in cloud systems. If processing genetic data in a cloud is necessary, attention should be paid to the following:

  - Detailed records of the genetic data stored in the cloud should be maintained.
  - Backups should be taken outside the cloud.
  - Remote access to genetic data in the cloud should be encrypted with cryptographic methods ensuring sufficient security.
  - Standardized and secure cryptographic algorithms included in the standardized cryptographic algorithm suite should be used in applications, devices, and systems.
  - Industry standards and best practice examples for standardized and secure cryptographic algorithms should be considered.
  - If the use of cryptographic algorithms not included in the standardized cryptographic algorithm suite is necessary, an analysis and evaluation of whether they provide a sufficient security level should be conducted by an authorized crypto analysis laboratory before use.
  - The encryption and key management policy should be clearly defined.
  - Access to cryptographic keys should be restricted to authorized personnel with clearance (crypto security certificate).
  - Where possible, separate encryption keys should be used, especially for each cloud solution received.

- When devices are delivered for maintenance, repair, or other purposes to service providers, or in cases of returning leased devices to the service providers, data storage units on the devices should be removed, or all data should be handed over to the laboratory in hard disk format. A written commitment should be obtained from the service providers stating that there is no data on the service provider's device or server.

- Before establishing the data controller system and after any changes, test environments should ideally be used to test the system through synthetic data.

- Data controllers should test the system in the created test environments using synthetic data before establishing it and after any modifications.

- In testing activities where real data is used, data controllers must use genetic data in accordance with the principle of data minimization. Data controllers should implement measures that alert the system administrator in case of unauthorized access attempts and, despite all security precautions, unauthorized access to the system, as well as measures that protect and report genetic data.

- Data controllers should use certified equipment and licensed and up-to-date software in the system, ensure patch management, prefer open-source software whenever possible, and promptly implement necessary updates in the system.

- Data controllers should be able to monitor and restrict user operations on the software processing genetic data. All actions performed on the program/system processing genetic data should be logged in a separate system and regularly securely maintained. It is important to ensure that the administrator responsible for the log system is different from those responsible for other systems.

- Hardware and software security tests of systems processing genetic data should be conducted periodically. Any changes made to the systems should be implemented only after the necessary security tests have been completed.

- Data controllers must adhere to the measures outlined in the Information and Communication Security Guidelines, as per the Directive numbered 2019/12, and the Information and Communication Security Guide prepared under the coordination of the Presidency Digital Transformation Office.

Administrative Measures

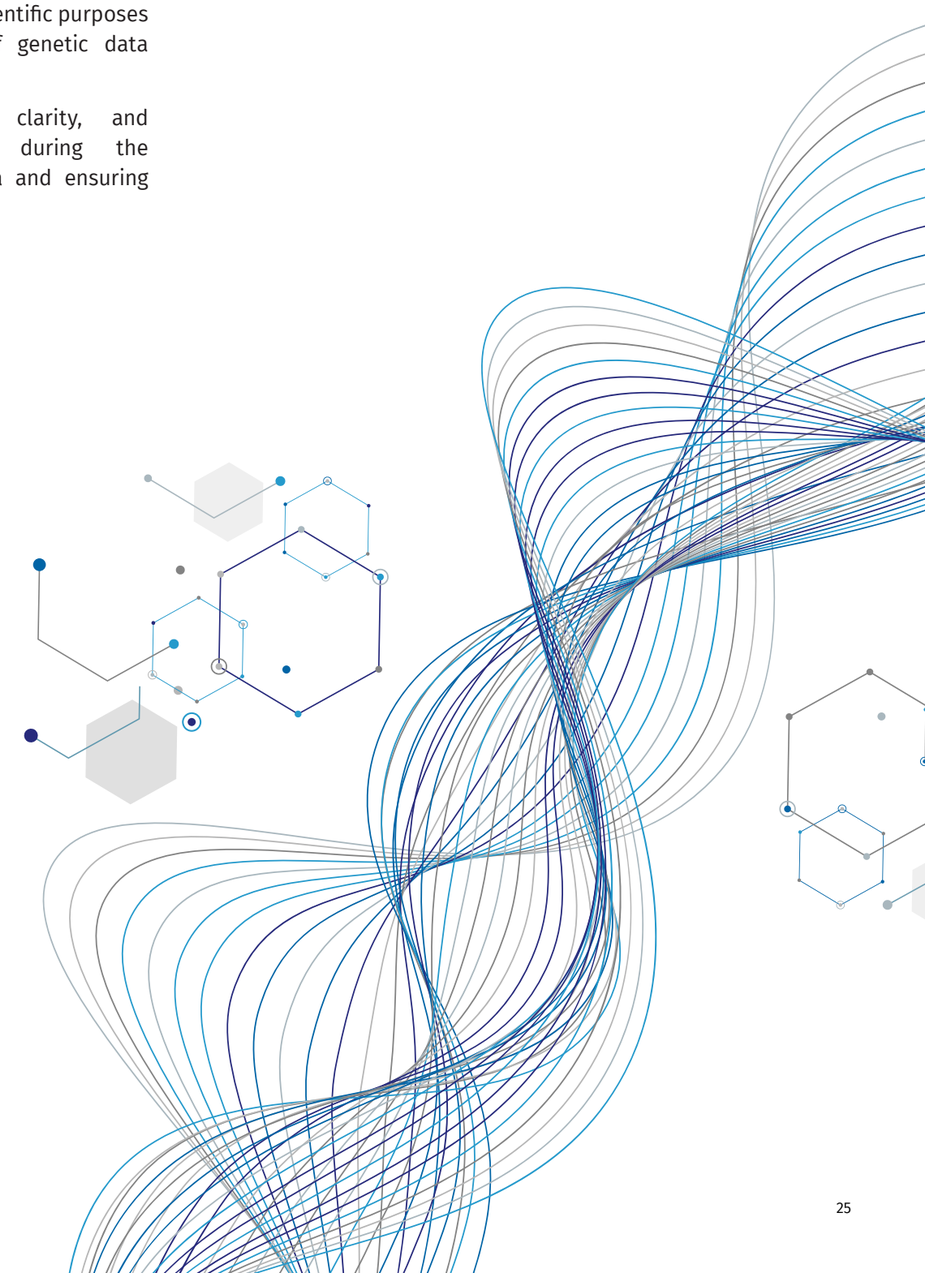
- Although not explicitly covered by Turkish legislation, the Genetic Data Guide emphasizes concepts found in the GDPR, including the establishment and management of genetic data based on the "Privacy by Design" principle and the application of Data Protection Impact Assessments.

- Genetic data should be safeguarded in a manner that prevents access by anyone other than authorized personnel who have received relevant training and have entered into confidentiality agreements.

- A Personal Data Processing Inventory should be prepared, and notification must be made to VERBİS.
- Separate processing policies, emergency procedures, and reporting mechanisms should be established for genetic data processing processes.
- Genetic data in electronic environments should be regularly backed up using a secure backup system, and data set backups must be kept off the network.
- The obligation to inform, in accordance with the legislation, should be fulfilled in detail, and explicit consent from the data subject should be obtained if necessary.
- Data controllers should measure and monitor their preparedness for a potential data breach continuously through internal random and periodic audits and risk analyses related to genetic data processing activities.
- In service contracts with data processors involved in genetic data processing processes, the data controller should include security measures deemed necessary and conduct regular audits or inspections at specified intervals to ensure that the selected data processor has implemented the required technical and administrative measures.
- The data controller should record and document their compliance with all the mentioned principles and criteria, and this information should be disclosed to the public.

The "Information and Communication Security Measures" subject, outlined in the Presidential Circular numbered 2019/12, emphasizes the secure storage of critical information and data, such as population, health, communication records, genetic, and biometric data, within the country to prevent disruption to the public order. In line with national and international standards and information security criteria, the Presidency Digital Transformation Office has published the "Information and Communication Security Guide" to ensure the security of critical data that could potentially disrupt the public order. Additionally, the "National Cyber Security Strategy," introduced through the Presidential Circular numbered 2020/15, further supports these efforts. In this regard, the Genetic Data Guide recommends implementing the following measures for genetic data:

- Determining procedures based on the processing purposes of genetic data and making detailed regulations regarding the conditions for transfer as specified in Article 9 of the DP Law.
- Taking necessary measures to prevent the misuse of processed genetic data's confidentiality and usage beyond its intended purpose.
- Supporting local laboratories and conducting efforts to procure local medical devices to minimize the sending of genetic data tests abroad.
- Making administrative regulations for the local storage of genetic data and supporting the national information infrastructure.
- Encouraging the development of national genetic data banking for scientific purposes and the establishment of genetic data storage centers.
- Enhancing transparency, clarity, and accountability practices during the processing of genetic data and ensuring public awareness.
- Providing necessary training for personnel involved in genetic data processing on the protection of personal data or ensuring it is fulfilled by the "Patient Rights Unit."
- Informing data subjects about the results when sending genetic data abroad, and increasing societal awareness.



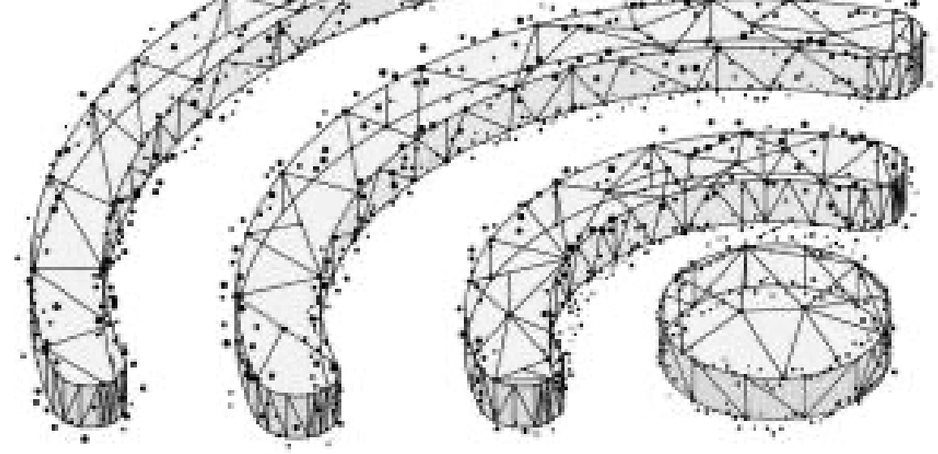
2. Recommendations for the Protection of Privacy in Mobile Application

The Board released the "Guidelines for the Protection of Privacy in Mobile Applications" ("**Mobile Application Guide**") on 22 December 2023. In the Mobile Application Guide, emphasis is placed on the critical importance of safeguarding individuals' personal data in mobile applications, given the extensive use of various sensors such as microphones, cameras, accelerometers, GPS, Wi-Fi, and Bluetooth on mobile devices commonly used by users, as well as the widespread use of cloud services by mobile application developers. Accordingly, the Mobile Application Guide addresses existing and potential risks related to the protection of privacy in mobile applications and aims to provide general recommendations of a non-specific nature to data subjects and data controllers regarding the processing of personal data activities carried out through mobile applications.

In mobile applications, various types of personal data, including special categories of personal data, may be processed for purposes such as enhancing user experience, providing functionality, improving the services offered, and creating marketing strategies. This data may encompass identity information (name, surname, ID number, date of birth, etc.); membership details (username, password, etc.); contact information (home address, phone number, email address, etc.); financial information (IBAN, credit card number, etc.); online identifiers (IP address, MAC address, IMEI and IMSI numbers, fingerprint extraction through the installed application list on the device, etc.); user interactions (search history, in-app purchases, etc.); location information; phone book or friend lists in applications; biometric data (facial recognition data, fingerprint data, voiceprint biometrics, etc.); health data if the application is health-related (heart rate, sleep pattern, etc.); visual data collected by granting access to the device's camera and gallery; auditory data collected through voice commands or messaging applications; and text data collected from messaging platforms.

In mobile applications, various entities, including the application provider, application developer, advertising network, application store organization, operating system provider, library provider, and device manufacturer, are involved in the processes of processing personal data. Examples are provided in the Mobile Application Guide regarding the circumstances in which the relevant parties may be considered data controllers within the process:

- The application provider is generally considered a data controller when they use users' personal data for their own purposes.
- It is emphasized that there may be multiple data controllers regarding the collected personal data in mobile applications. For instance, if a third-party service provider is involved in the mobile application for implementing two-factor authentication to prevent fraud, or if a third-party service such as advertising networks is integrated into the application, multiple data controllers may arise.
- When applications installed on a mobile device are used, the operating system provider may be considered a data controller if they aggregate data and use personal data collected from the applications on the user's device for their own purposes.



- In a scenario where the application provider and developer are separate entities, based on the contract between the application provider and developer, if the application developer assumes only a technical role in personal data processing and does not process personal data for their own purposes, the application developer may be considered a data processor.
- Personal data collected from mobile applications is generally stored in the cloud, and, when cloud services used by the application developer are involved, the application developer may also be considered a data processor.

Recommendations for Individuals

The Mobile Application Guide provides guidance for individuals on what to consider before installing a mobile application:

- The application should be downloaded to the device through platforms deemed trustworthy, such as application stores.
- Before installing an application, users should gather information about the application developer and ensure the accuracy of the application name.
- To gain insights into the functionality and reliability of the application, users should check user reviews and the ratings received by the application from users.
- Before downloading the application, users should check what permissions are requested for accessing data and review the application's privacy policy.
- In cases where the application requests more personal data than is necessary for providing the service, users should assess whether there is a genuine need for this information and, if necessary, explore alternative applications.

The Mobile Application Guide also provides considerations to be aware of during the use of a mobile application:

- It is highlighted that during the use of the application, additional permissions may be requested for accessing data that is not necessary for the specific functionality of the application. Users are advised to reject access requests and to explore alternative applications if there are concerns about the protection of privacy.
- Permissions granting continuous access to location, audio, and visual data on mobile device tools should be evaluated based on the intended use of the data.
- Users are advised not to use their social media accounts to log in to applications. It is noted that logging into an application using the user's social media account information may allow the application to collect information from the relevant social media account in certain situations.
- The importance of avoiding easily guessable passwords, creating different passwords for each account whenever possible, and enabling two-factor authentication is emphasized.
- It is recommended to keep applications up to date, as applications with outdated software are at a higher risk of being vulnerable to attacks. Therefore, it is advised to regularly update the applications in use.

Recommendations for Data Processors

i. Ensuring Compliance with General Principles

Principle of Legality and Fairness: Application developers and providers are expected to question whether there is a legal basis for processing before commencing any processing of personal data. They should maintain honesty and transparency regarding the personal data processed in mobile applications, enable individuals to exercise their rights, and implement processes and designs that support the use of these rights. It is emphasized that transparency should be maintained regarding third-party processes utilized in the mobile application, and, if there is no legal basis for processing personal data through the integrated third-party service, this service should not be used in the application. Examples of applications that violate the principle of legality and fairness are also provided:

- In mobile applications that operate with voice commands supported by voice control assistants, transparency regarding the processed personal data is essential. For instance, it is noted that, if the feature of the mobile application is automatically activated on the device when first used, it may be contrary to the principle of legality and fairness. On the other hand, measures such as accessing the microphone only when the user actively uses the device, rather than when the mobile phone is on a table or in the user's pocket or bag, are suggested to meet the user's reasonable expectations in the processing of personal data.
- A mobile application that tracks individuals' physical activity levels by counting steps and monitoring sleep patterns and dietary habits may process data to create statistical information about these data for the purpose of reminding users to exercise. This can be considered compatible with the intended use of the mobile application. However, it is emphasized that, if the mobile application provider offers health insurance services and uses the personal data collected through the mobile application to calculate insurance premiums, it may violate the principle of fairness due to exceeding the user's reasonable expectations.

Principle of Being Accurate and Up to Date When Necessary: Within the scope of mobile applications, it is stated that users should be provided with the opportunity to correct their personal data, and the application should be designed to facilitate this option for users. It is emphasized that outdated personal data may pose a risk of identity theft. Examples of applications that may violate the principle of accuracy and timeliness, while also compromising individual privacy, are also provided:

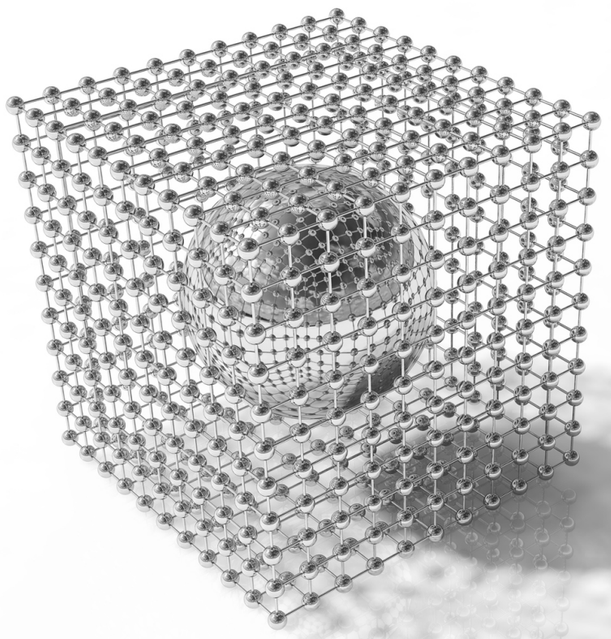
- In a scenario where a user enters their email and phone number information when signing up for a mobile application, but no verification is performed for this information in the application, and users are not provided with the opportunity to update this information from within the application, a risk of personal data being disclosed to a third party is highlighted. For example, if a user accidentally enters an incorrect email address during registration, and order information related to a purchase made through the mobile application is sent to this email address, it could lead to the exposure of personal data to an unintended recipient.
- It is emphasized that, in a situation where a user changes their phone number after some time and requests a password reset through the mobile application due to forgetting the password, there is a risk of the reset code being sent to the old phone number entered by the user during the password reset process, even if that number is no longer in use. This could pose a risk of the code being transmitted as a message to a third party.

Principles of Specific, Clear, and Legitimate Processing, and Processing Connected, Limited, and Proportional to the Purpose: In mobile applications, personal data should be processed exclusively for the purpose of the application. Furthermore, the processing of such personal data should be connected, limited, and proportional to the purpose, ensuring predictability for users. In this regard, if it cannot be explained how personal data is related to the functions or activities offered through the mobile application, such data should not be collected. Additionally, personal data obtained by the mobile application should not be subject to processing activities exceeding the intended use of the application. The Mobile Application Guide provides examples of the application of principles such as specific, clear, and legitimate processing, as well as processing being connected, limited, and proportional to the purpose:

- A mobile application designed for contact tracing for the purpose of combating infectious diseases can achieve its intended use by only processing proximity data (information indicating how close individuals have been to each other, collected through Bluetooth technology). Therefore, tracking of the exact location and

movements of the users by the application, with the aim of identifying if a user has had close contact with another user who has an infectious disease, would be unnecessary and could be considered a violation of the principle of processing being connected, limited, and proportional to the purpose.

- In cases where processing activities within the scope of the services provided by the mobile application can be carried out using personal data stored only in the local storage of the device on which the mobile application is used, not transmitting such personal data to the data recording systems of the mobile application provider would be in accordance with the principle of processing being connected, limited, and proportional to the purpose.



Principle of Retention for the Duration Defined by Relevant Legislation or Necessary for the Purpose of Processing:

For personal data processed through mobile applications, clearly defined retention and disposal periods justified by identified business needs or legal obligations should be established. These data should not be stored for a longer period than necessary. The storage period for personal data stored by a mobile application developer in the cloud should be determined, taking into account any maximum retention period specified in sector-specific legislation applicable to the use of the mobile application. If there is no such maximum retention period, a retention period connected to the purpose of processing these data should be established. Additionally, it should be stated that, once the retention period expires, the personal data are expected to be securely destroyed using all necessary technical and administrative measures. The Mobile Application Guide also gives a good practice example for compliance with the principle of retention for the duration defined by relevant legislation or necessary for the purpose of processing:

- Depending on the nature of the service provided through the mobile application, the retention periods for the personal data of categorized active and inactive users should be determined according to their statuses. For instance, a good practice example in this regard could be the transformation of a user's status to inactive if they do not log into the application for a specific period, and a shorter retention period for the personal data of inactive users compared to active users (excluding legal obligations).

ii. Ensuring Transparency

The Mobile Application Guide emphasizes the following considerations to ensure transparency:

- The privacy policy and, if separately prepared, the privacy notice should be positioned in a way that is easily accessible to both existing users and potential users considering downloading the application.
- While informing users about updates related to the application, they should also be informed about any changes that concern the processing of their personal data.
- Users should be made aware of the default privacy settings of an application, and user-friendly mechanisms with easy-to-understand interfaces should be provided to help them manage their privacy.
- To enable users to make informed decisions about using an application, information should be provided in compliance with Article 4 of the DP Law.
- In mobile applications provided by providers based abroad, actions such as making references to Turkiye, providing goods and services with indications that they are offered to individuals in Turkiye, presenting introductory descriptions indicating that the service is provided to people in Turkiye, offering the Turkish language option for services, and providing the option for product delivery to Turkiye are considered as targeting individuals in Turkiye. Similarly, performing activities such as behavioral advertising, online tracking through unique identifiers, and conducting geolocation activities for marketing purposes would indicate monitoring the behaviors of individuals in Turkiye. When targeting or monitoring the behaviors of users in Turkiye through mobile applications, it is important to consider the obligation of VERBİS registration and notification under Article 16 of the DP Law concerning the personal data processed through the mobile application.

iii. Processing Personal Data of Children in Mobile Applications

In relation to mobile applications targeting children or widely used by them, it is recommended to establish systems that verify the user's age and to conduct processing activities for children through a separate policy and procedure.

iv. Determining the Conditions for Processing Personal Data

The Mobile Application Guide emphasizes that determining the conditions for data processing is a prerequisite for fulfilling the obligation of ensuring transparency. In personal data processing activities carried out through mobile applications, obtaining the explicit consent of the user will be necessary when processing personal data that is not required for the main function of the application. In this regard:

- It is stated that, unless the user gives explicit consent, the collection of the user's location data for targeted advertising purposes should not take place when there is no need to access the user's location for any feature or function of an application requested by the user.

- Users should be allowed to use the application even if they choose to disable permissions for optional functions such as accessing the microphone or location that are not deemed necessary for the functionality of the application.

v. Ensuring Data Security

It is stated that mobile applications should be designed in accordance with the principles of privacy by design and privacy by default and should be made available in a way to ensure the protection of personal data at the highest level. In this regard:

- The importance of privacy-focused settings being open by default when mobile applications are first used, without the need for additional action by individuals, is emphasized for compliance with the principle of honesty in the processing of personal data.
- To prevent unauthorized access to devices where mobile applications are used, it is recommended to use authentication methods on the devices. Moreover, the creation of control mechanisms for users regarding simultaneous logins from different devices is considered a beneficial practice.
- Users are encouraged, if possible, to use multi-factor authentication methods.
- Regarding access to mobile applications, users are advised to create strong passwords, and implementing a password security policy by regularly changing user passwords is emphasized. Preventing the reuse of previously used passwords when creating new passwords is also considered a good practice.
- Passwords are recommended to be stored securely with adequate security measures and to be preserved by passing through up-to-date "hashing" functions to mitigate the risk of cyber attacks.
- Regular patch management and software update processes are recommended, and keeping the software up-to-date to address vulnerabilities in mobile applications is advised.
- The necessity of conducting appropriate software tests before the release of developed mobile applications is highlighted.
- Limiting the number of unsuccessful login attempts for user account logins in mobile applications and using methods such as CAPTCHA, arithmetic operations, etc., on pages with user entry as a measure against bot attacks are suggested.
- Before the release of applications, a risk assessment is recommended, taking into account the data protection and security features of the targeted operating systems.
- To ensure data security during the storage and transmission of personal data in mobile applications, it is suggested to use encryption with a well-configured encryption layer during network communication and to protect through encryption using secure management of relevant encryption keys.

V. Draft Guidelines

The Authority has not shared any guide drafts with the public as of the end of 2023. The guide draft of Loyalty Programs within the scope of Personal Data Protection Legislation, dated 16 June 2022 from the previous year, is still in the draft stage. It has not been finalized by the Authority and shared with the public.

MOROĞLU ARSEVEN

VI. Public Announcements Made by the Board in 2023

In 2023, the Board released a total of seven public announcements. These public announcements cover explanations of the amounts of administrative fines for 2023, data subjects and data controllers affected by the earthquake that occurred on 6 February 2023, the data processing processes of political parties and independent candidates during election periods, the submission of complaints through a power of attorney in electronic form to the Board, investigation of data breaches in public institutions, exceptions related to the VERBIS obligation, and sending verification codes to data subjects via SMS during shopping in stores. Although these public announcements do not have legal binding force, they are significant in reflecting the Authority's legal assessments and approach regarding the respective matters.

Details regarding the published public announcements are provided below in chronological order.

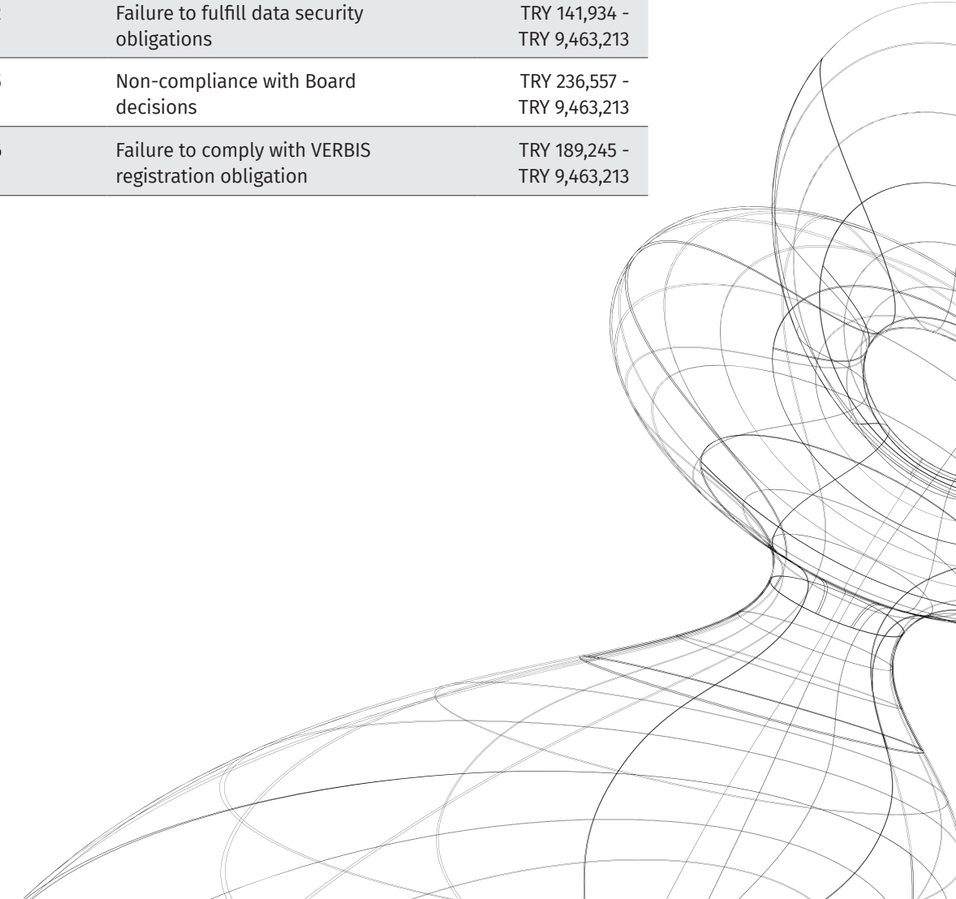
1. Administrative Fines under the Law on the Protection of Personal Data numbered 6698 (for 2023 and 2024)

As of 17 January 2023, the administrative fine amounts regulated under Article 18 of the DP Law, in accordance with Article 17/7 of Law on Misdemeanors numbered 5326, effective from the beginning of each calendar year and increased by the revaluation rate announced for 2023, as per the provisions of Article 298 of the Tax Procedure Law numbered 213, are as follows:

Article of DP Law	Violated Article of the DP Law	Explanations	Administrative Fines for 2023
18/a	10	The failure to fulfill the obligation of informing	TRY 29,852 - TRY 597,191
18/b	12	Failure to fulfill data security obligations	TRY 89,571 - TRY 5.971,989
18/c	15	Non-compliance with Board decisions	TRY 89,571 - TRY 5.971,989
18/ç	16	Failure to comply with VERBIS registration obligation	TRY 89,571 - TRY 5.971,989

As of 5 January 2024, the revised amounts, increased at the officially determined revaluation rate for 2024 (58.46%), have also been published:

Article of DP Law	Violated Article of the DP Law	Explanations	Administrative Fines for 2024
18/a	10	The failure to fulfill the obligation of informing	TRY 47,303 - TRY 946,308
18/b	12	Failure to fulfill data security obligations	TRY 141,934 - TRY 9,463,213
18/c	15	Non-compliance with Board decisions	TRY 236,557 - TRY 9,463,213
18/ç	16	Failure to comply with VERBIS registration obligation	TRY 189,245 - TRY 9,463,213



2. Public Announcement for Data Subjects and Data Controllers Affected by the Earthquake

Due to the two major earthquake disasters that occurred on 6 February 2023, centered in the Pazarcık and Elbistan districts of Kahramanmaraş, a state of emergency was declared for a period of three months in the provinces of Adana, Adıyaman, Diyarbakır, Gaziantep, Hatay, Kahramanmaraş, Kilis, Malatya, Osmaniye, and Şanlıurfa, as announced in the Official Gazette dated 8 February 2023, with the Presidential Decree numbered 6785. On 9 February 2023, the official website of the Authority announced that the extraordinary conditions caused by the earthquake would be taken into account in the evaluation of the periods specified in the DP Law and relevant sub-regulations for the following data subjects or data controllers:

- Those located in the provinces where a state of emergency was declared due to the earthquake or in other provinces affected by the earthquake.
- Those represented by lawyers working under the bar associations of the provinces where a state of emergency was declared due to the earthquake, or working under the bar associations of the provinces affected by the earthquake.

3. Public Announcement Regarding the Processing of Personal Data by Political Parties and Independent Candidates During Election Activities

On 23 March 2023, the Board issued a public announcement regarding the processing of personal data by political parties and independent candidates during the general elections for the Turkish Grand National Assembly and the Presidency held in Turkiye. In this regard, the Board emphasized the points to be considered in the processing of personal data by political parties and independent candidates within the scope of election activities. Accordingly, the Board highlighted that political parties, in accordance with relevant laws, process personal data in relation to activities such as establishment, membership, candidate selection for elections, election of authorized bodies, and their notification to the relevant authorities. Thus, political parties are considered data controllers for the personal data they process due to their activities.

The public announcement emphasized that, in the processing of personal data by political parties and independent candidates, compliance with the conditions specified in Article 5 and Article 6 of the DP Law based on the nature of the processed personal data is required. Pertaining to this, the Board prepared an information note emphasizing the necessity of acting in accordance with these aspects in personal data processing activities during election processes.

4. Public Announcement Regarding the Submission of Complaints on Behalf of Others to the Authority Electronically

As of 27 March 2023, an official announcement on the Authority's website states that, under the existing system, complaint letters can be submitted to the Authority by hand, mail, or courier, as well as electronically through the 'Complaint Module' available at www.kvkk.gov.tr. Pertaining to this, to facilitate the faster and more effective submission and tracking of complaints made by proxy, it has been publicly shared that, as of 27 March 2023, the 'Complaint Module' system is available for attorneys to submit complaints on behalf of others. This complaint module can be accessed through the internet link https://sikayet.kvkk.gov.tr .

5. Public Announcement Regarding Data Breach in Public Institutions

On 19 June 2023, the Authority issued a Public Announcement acknowledging various news reports on television channels and social media platforms claiming the leakage of citizens' personal data from public institutions. However, the Authority stated that, as of the date of this Public Announcement, there had been no reported data breach notifications from public institutions regarding the mentioned breach. Additionally, due to similar news reports in the media in the past, the Board initiated an ex officio examination with its decision dated 9 March 2023, numbered 2023/341, and emphasized ongoing coordinated efforts with relevant public institutions on this matter.

6. Public Announcement Regarding Amendment to the Exception Criteria for VERBIS Registration Obligation

On 25 July 2023, the Authority released an official public announcement detailing modifications to the criteria exempting certain entities from VERBIS registration obligations. In response to current economic conditions in Turkiye, the Board revised the provision from its decision dated 17 July 2018 (2018/87), changing the threshold for annual financial balance totals. Specifically, the phrase "legal or natural persons with fewer than 50 employees and an annual financial balance total of less than TRY 25,000,000, not primarily engaged in processing special category personal data" now reads as "legal or natural persons with fewer than 50 employees and an annual financial balance total of less than TRY 100,000,000, not primarily engaged in processing special category personal data." This amendment, which solely addresses the annual financial balance amount without altering the employee count, stipulates that if a data controller's annual financial balance reaches TRY 100,000,000, they become subject to VERBIS registration obligations, as outlined in the corporate tax return for legal entities and the income tax return for individuals for the completed calendar year.

7.Public Announcement Regarding Processing of Personal Data by Sending Verification Codes to Data Subjects via SMS During Shopping in Stores

On 13 November 2023, the Authority released an official Public Announcement on the processing of personal data by sending verification codes to data subjects via SMS during shopping in stores, particularly emphasizing the accurate implementation of the DP Law and the necessity of obtaining explicit consent for commercial electronic messages. The Authority's examinations revealed that necessary information was not provided before or in the SMS containing the verification code, and explicit consent was not lawfully obtained.

In order to ensure the legality of personal data processing processes for sending commercial electronic messages, it was emphasized that obtaining explicit consent and fulfilling the obligation of informing must be done comprehensively. Accordingly:

- The purpose and content of SMS messages to be sent during cashier transactions in-store must be clearly and comprehensibly communicated to the data subject. This information must be provided as part of layered transparency.
- Practices combining different transactions (e.g., membership agreement approval, explicit consent for personal data processing, commercial electronic message approval) with SMS messages during payment transactions must be discontinued, and explicit consent must be obtained separately for each transaction.
- Processes for obtaining explicit consent and fulfilling the obligation of informing by data controllers must be carried out separately from each other.
- SMS messages sent to obtain explicit consent for sending commercial electronic messages must include all the elements specified in the DP Law.
- Explicit consent for processing personal data for sending commercial electronic messages must not be presented as a mandatory element for completing the purchase. Otherwise, it may compromise elements of explicit consent, such as "being based on information and given with free will."
- Explicit consent for processing personal data for sending commercial electronic messages must be requested after completing the purchase, preventing it from being perceived as a necessary element of the transaction.

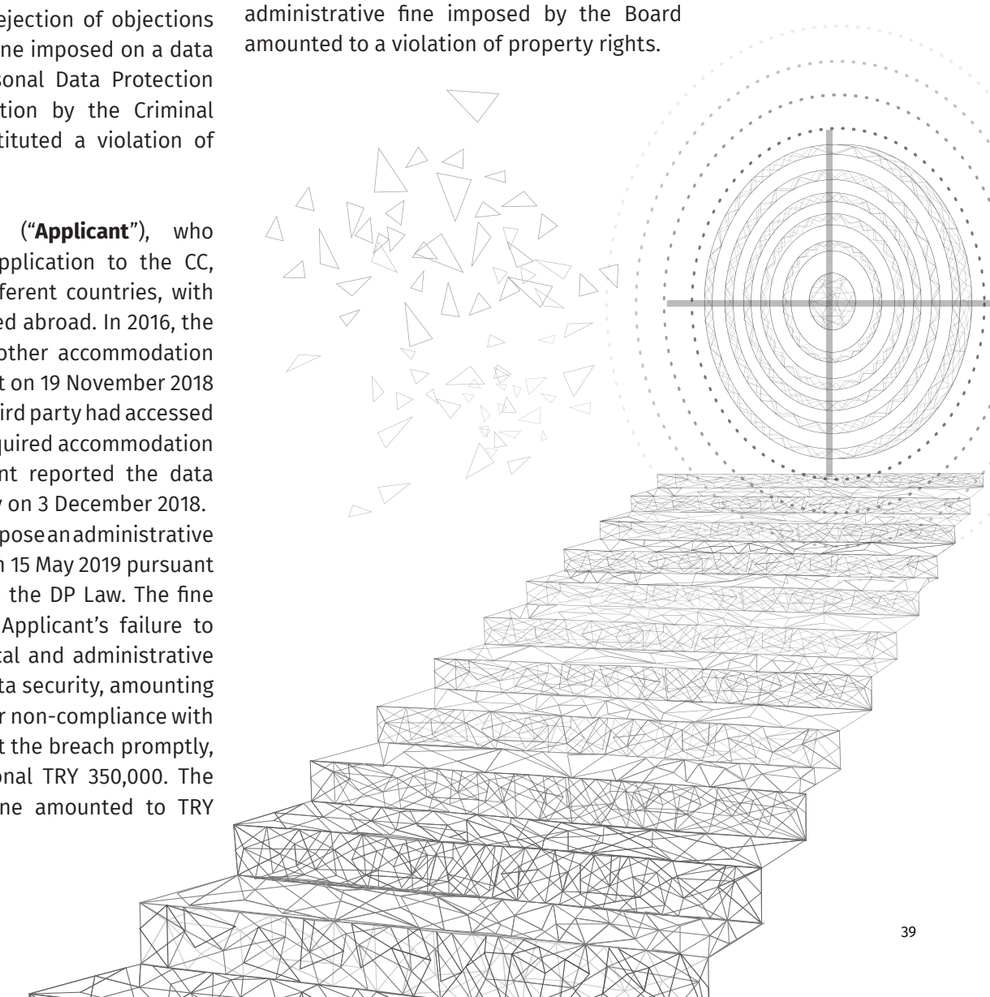
VII. Constitutional Court Decisions

1.The Decision of The Constitutional Court with Application Number 2020/7518 and Decision Date 12 October 2023

The decision of the Constitutional Court with application number 2020/7518 and decision date 12 October 2023, was published in Official Gazette dated 15 December 2023 and numbered 32400. In the decision, the Constitutional Court ("CC") determined that the rejection of objections to the administrative fine imposed on a data controller by the Personal Data Protection Board without evaluation by the Criminal Peace Judgeship constituted a violation of property rights.

The data controller ("**Applicant**"), who made an individual application to the CC, operated hotels in different countries, with its headquarters located abroad. In 2016, the Applicant acquired another accommodation company and found out on 19 November 2018 that an unauthorized third party had accessed the database of the acquired accommodation company. The Applicant reported the data breach to the Authority on 3 December 2018. The Board decided to impose an administrative fine on the Applicant on 15 May 2019 pursuant to Article 12 of Law on the DP Law. The fine was imposed for the Applicant's failure to take necessary technical and administrative measures to ensure data security, amounting to TRY 1,100,000, and for non-compliance with the obligation to report the breach promptly, resulting in an additional TRY 350,000. The total administrative fine amounted to TRY 1,450,000.

The Applicant applied to the Istanbul Anatolian 1st Criminal Peace Judgeship to have the imposed administrative fine lifted, but the application was rejected. Despite the Applicant's objection, the request was definitively denied by the decision of the Istanbul Anatolian 2nd Criminal Peace Judgeship. Subsequently, within the statutory period, the Applicant filed an individual application to the CC claiming that the administrative fine imposed by the Board amounted to a violation of property rights.



In the individual application made to the CC, the Applicant argued the following:

- That the accommodation company where the data breach occurred was to be considered the data controller, asserting that the administrative fines were not applicable to the Applicant, and contending that the principle of the personal nature of administrative penalties was violated.
- That the decision of the Board regarding the administrative fine was not properly notified, lacked sufficient justification, and the objection was rejected without adequate and necessary examination by the appellate court.
- That all technical and administrative measures were taken, the breach was promptly detected and reported, and there was no restrictive time frame in the DP Law for such reporting. The Applicant argued that the failure of the appellate courts to consider this was contrary to the principles of legality in both the offense and the penalty.
- That the imposition of the maximum administrative fine was disproportionate and infringed on the Applicant's property rights.

The noteworthy points in the decision of the CC with Application Number 2020/7518 and Decision Date 12 October 2023 can be outlined as follows:

- The imposition of administrative fines led to a depletion of the Applicant's assets, and it was acknowledged that this money constituted property for the Applicant. Accordingly, it was stated that the imposition of administrative fines on the Applicant for not taking necessary technical and administrative measures to ensure data security and for not promptly reporting data security breaches constituted an interference with the right to property.
- The CC deemed it necessary to assess the situation in light of the principle of "proportionality", even though it was argued that there was no specific timeframe in the DP Law for the detection and reporting of data breaches.
- It was noted that property rights can be limited for the purpose of public interest. In order to be constitutionally permissible, interference with property rights must be suitable and necessary to achieve its purpose. While public authorities have some discretion in choosing the means of interference, it was emphasized that there must be very strong reasons when the selected means do not meet the necessity criteria due to the absence of alternative means or the ineffectiveness of existing alternatives in achieving the intended legitimate purpose. In this regard, it was stated that the decisions of appellate courts must contain relevant and sufficient justification.
- The distinction between the protection of personal data and the protection of data security was emphasized. The protection of personal data primarily corresponds to safeguarding fundamental rights and freedoms during the processing of personal data, while the protection of data security involves taking technical and administrative measures to protect the data itself.
- It was emphasized that all necessary technical and administrative measures must be taken to ensure an appropriate level of security for the protection of personal data. When assessing the appropriateness of the security level, the risks posed by the processing activities, including accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access to personal data, should be taken into account. Moreover, it was highlighted that the determination of the appropriate security level depends not only on the size or financial status of the company but also on the nature of the data being protected. Accordingly, the data controller is obliged to conduct or ensure necessary audits within its organization to ensure compliance with the provisions of the DP Law.
- While authorities have some discretion in determining the measures to be implemented for ensuring data security, it was emphasized that this discretion is not unlimited. In particular, if the preferred means significantly exacerbate the interference concerning the intended purpose, the interference is not necessary.
- The CC concluded that the entity where the data breach occurred, considered the data controller, was the accommodation company.
- The CC acknowledged that the arguments presented by the Applicant regarding the decision given by the Board, which were submitted during the objection to the Criminal Peace Judgeship, were important and should have been addressed throughout the entire legal process. The CC determined that the Criminal Peace Judgeship's failure to examine these arguments in any way did not fulfill the procedural safeguards for the protection of property rights and constituted a violation of property rights.

MOROĞLU ARSEVEN

VIII. Documents Published by the Republic of Turkiye Presidency Digital Transformation Office

The Presidency of the Republic of Turkiye Digital Transformation Office ("**Digital Transformation Office**") operates with the aim of consolidating various activities related to digital transformation, cybersecurity, national technologies, big data, and artificial intelligence conducted separately under different institutions in line with evolving technologies, societal demands, and trends in public sector reforms. Accordingly, it is essential to examine the activities related to data within the scope of the Digital Transformation Office's efforts in Turkiye's digital transformation processes. Below are the significant initiatives undertaken by the Digital Transformation Office in 2023.

1.Information and Communication Security Compliance and Audit Monitoring System

On 4 January 2023, the Information and Communication Security Compliance and Audit Monitoring System ("**BİGDES**") was implemented. BİGDES was created with the aim of submitting the results of compliance audits related to the Information and Communication Security Guide, which must be carried out by institutions and organizations within the scope of the directive numbered 2019/12 to the Presidency of the Digital Transformation Office. Thus, it is intended to monitor activities related to compliance with the Information and Communication Security Guide, compliance audits related to the Information and Communication Security Guide, and the installation and operation of the Information Security Management System. Authorized personnel designated by institutions and organizations will have access to the system through e-Government Gateway authentication. Institutions and organizations covered by the Information and Communication Security Guide are required to complete their audit activities and upload the results to the system by 31 March 2023.

2. Chatbot Applications and ChatGPT Example Report

On 13 June 2023, the Digital Transformation Office released a report titled "Chatbot Applications and ChatGPT Example." In this regard, the report covers the definition, classification, purposes, and benefits of chatbot applications for customers. Simultaneously, it addresses potential attack risks, threats to security, privacy, and data protection related to these applications.

In the report, the Digital Transformation Office has localized the term "chatbot" as "Turkish conversational robots" and defined them as algorithm-based software that interacts through conversational interfaces, automatically performing certain tasks. Chatbots analyze user queries using artificial intelligence algorithms to generate logical responses. Moreover, their usage, especially in marketing and customer relations, is increasing day by day in various fields such as health, finance, education, marketing, entertainment, and websites, making it easier to reach a wide customer base.

The report scrutinizes potential attack risks for chatbots and highlights threats to security, privacy, and data protection. Major security threats include phishing emails, unauthorized changes, denial of service, information disclosure, service denial, and privileges escalation. The report suggests that security threats can be mitigated by mechanisms such as authentication, authorization, end-to-end encryption, self-destructing messages, user communication data, and back-end systems. Authentication, for instance, protects user data and devices in cases of lost or unlocked phones or computers. End-to-end encryption is a communication system where only the communicating parties can read the messages. The report concludes that, through these mechanisms, the potential risks of chatbots can be prevented, and the benefits obtained can be maximized.

B. STRUCTURE AND SUPERVISORY ACTIVITIES OF THE BOARD AND AUTHORITY

I. Structure and Organization of the Board and the Authority

The Personal Data Protection Authority consists of the Personal Data Protection Board and the Presidency. The Board is organized as seven members of the Board and seven presidential units, apart from the President and the Second President of the Authority.

As of 6 April 2023, the General Board's structure, with the appointment of Cennet ALAS ŞEKERBAY, is as follows:

Genel Kurul	
President	Prof. Dr. Faruk BİLİR
Second President	Hasan AYDIN
Board Member	Şaban BABA
Board Member	Murat KARAKAYA
Board Member	Bayram ARSLAN
Board Member	Dr. Ayşenur KURTOĞLU
Board Member	Tamer AKSOY
Board Member	Recep KESKİN
Board Member	Cennet ALAS ŞEKERBAY

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 has been conducting Wednesday Seminars since 2018 and podcast broadcasts since 2021 and continued these initiatives in 2023. Additionally, various seminars, events workshops, training sessions, and events were organized in 2023, including the following:

- 28 January Personal Data Protection Day Event
- April 7 Personal Data Protection Day Event
- 6th E-Safe Personal Data Protection Summit
- 2nd Personal Data Protection Conference
- Wednesday Seminars covering topics such as:
  - Purposeful Perspective in Processing Personal Data: Principle of Proportionality
  - Joint Data Controllership as a Form of Responsibility
  - Data Transfer Abroad: European Union and Key Differences
  - Processing Personal Data Through Cookies
  - Digital Fingerprint in Terms of Personal Data Protection
  - Blockchain Technology in the Context of Personal Data Protection
  - Administrative Sanctions in DP Law under the Misdemeanors Law
  - Protection of Personal Data in Insurance Law
  - Protection of Personal Data in Employer-Employee Relations
  - Personal Data Security and Privacy Protection in IoT (Internet of Things) Applications
  - Personal Data Security in Cloud Computing
  - Risk-Based Approach
  - Evaluation of Targeted Advertising Practices in Terms of Personal Data Protection Law

- Podcast broadcasts covering subjects such as:

- International and National Regulations in the Field of Personal Data Protection
- Purpose and Scope of Law No. 6698 on the Protection of Personal Data
- Deletion, Destruction, or Anonymization of Personal Data

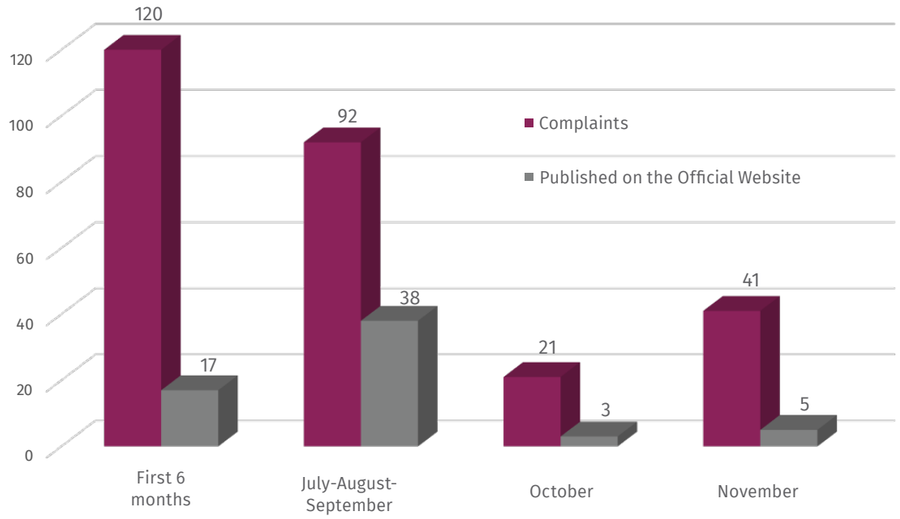
Additionally, as of September 2023, it was announced that a new podcast series titled "A Little Awareness Is Enough" has started broadcasting through the podcast channel. In this series called "GDPR Agenda," the aim is to inform the audience about developments related to the protection of personal data globally and in Turkiye.

The Authority published its first annual activity report for 2018 and continued this practice for the years 2019, 2020, 2021, and 2022. As of the date of publication of this guide on the developments in Turkish data protection law in 2023, the Authority has not yet released its activity report for 2023. General information about the Authority's activities can be found under the "DP Law Bulletin" section on the official website. In this regard, Statistical information up to 2022 is sourced from activity reports, while data for 2023 is gathered from DP Law Bulletins, specifically the issues titled "July 2023: Issue 1 (Rethinking Privacy in the Age of Artificial Intelligence)" and "July-September 2023: Issue 2 (Traces Left in the Shadows: Right to be Forgotten)," as well as content shared in monthly video formats for October and November 2023.

As of November 2023, a total of 274 data breach notifications and 8490 complaint applications have been recorded, with two commitment applications approved, granting permission for overseas data transfers. Within the scope of this study, publications available on the official website of the Authority have also been taken into account, and 74 decision summaries have been shared with the public in 2023.

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

1. Data Breach Notifications



2. Statistical Data Regarding the Activities of the Board

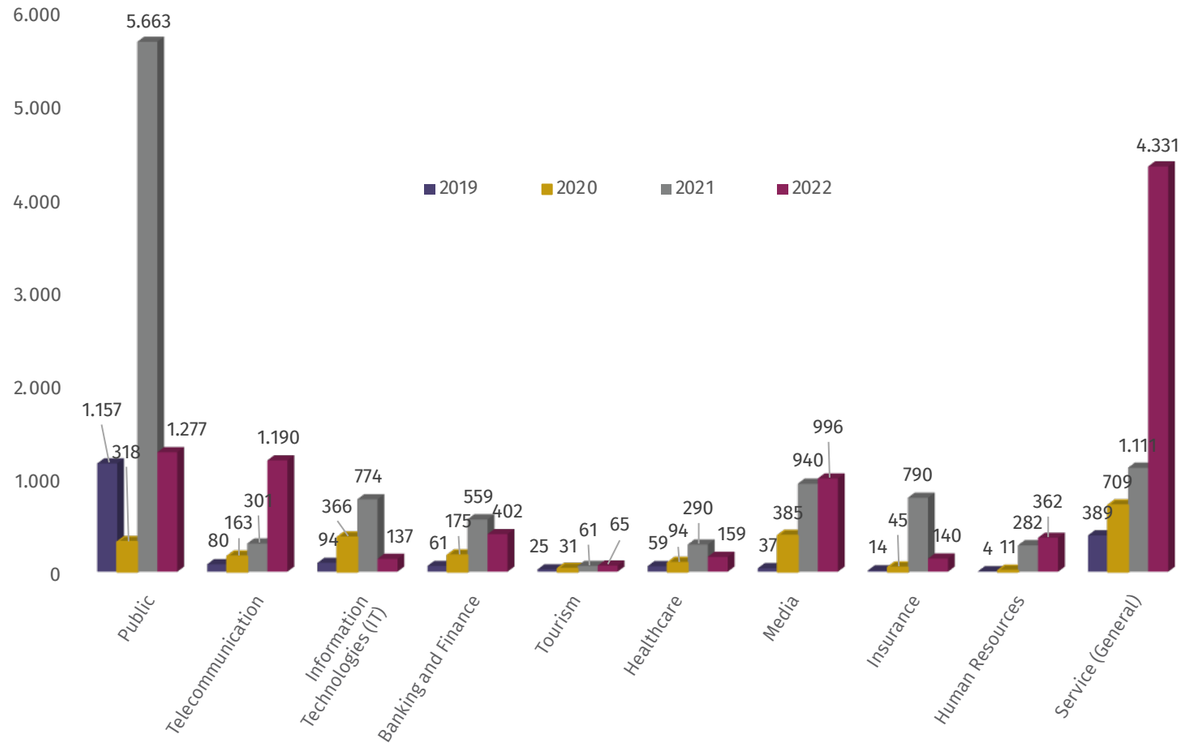
As of the date this study was prepared, the Board has not yet published the 2023 Annual Activity Report. Statistical data covering the eleven-month period from January 2023 to November 2023, obtained through the DP Law Bulletins, has been included.

Additionally, based on the information disclosed in the Authority's published Activity Reports for the years 2019, 2020, 2021, and 2022, the statistical data is as follows:

3. Complaints

3.1. Distribution of Complaints by Sector

As of the date of this study, the distribution of complaints by sector has not been publicly disclosed by the Authority. The distribution of complaints for 2019, 2020, 2021, and 2022 by sector is presented in the table below[2]:

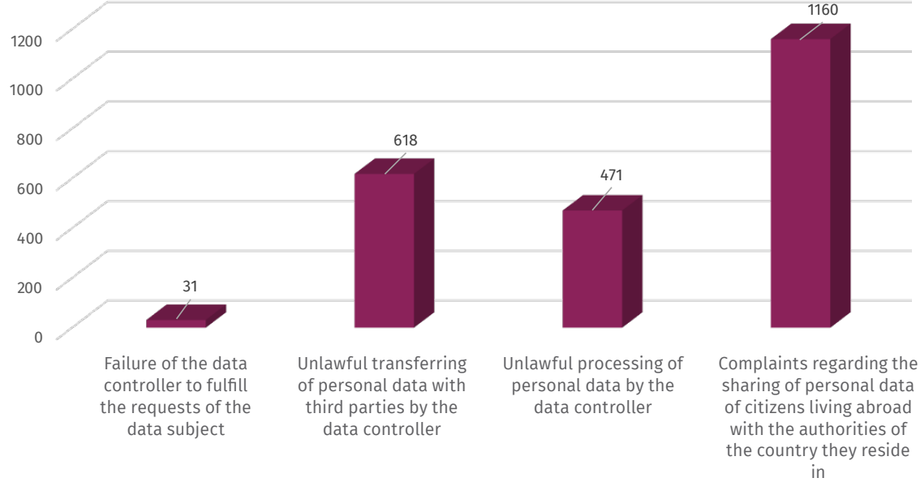


[2] The information was obtained from the 2022 Activity Report published by the Authority.

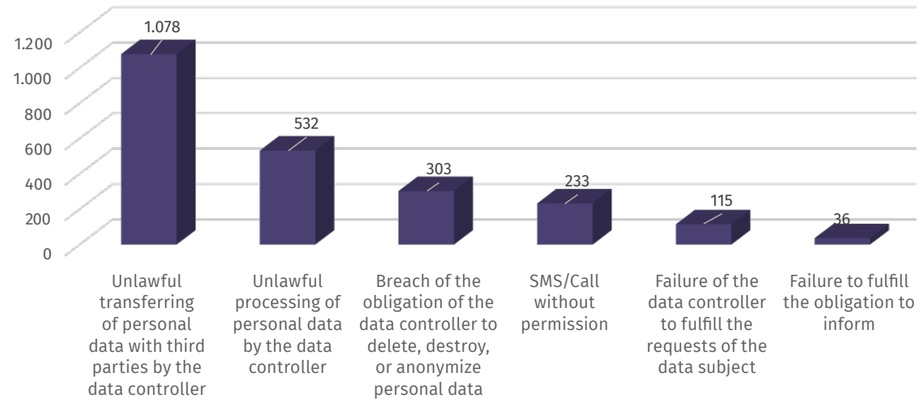
3.2. Distribution of Complaints by Subject

As of the date of this study, the distribution of complaints by subject has not been publicly disclosed by the Authority. The distribution of complaints for 2019, 2020, 2021, and 2022 by subject is presented in the table below:

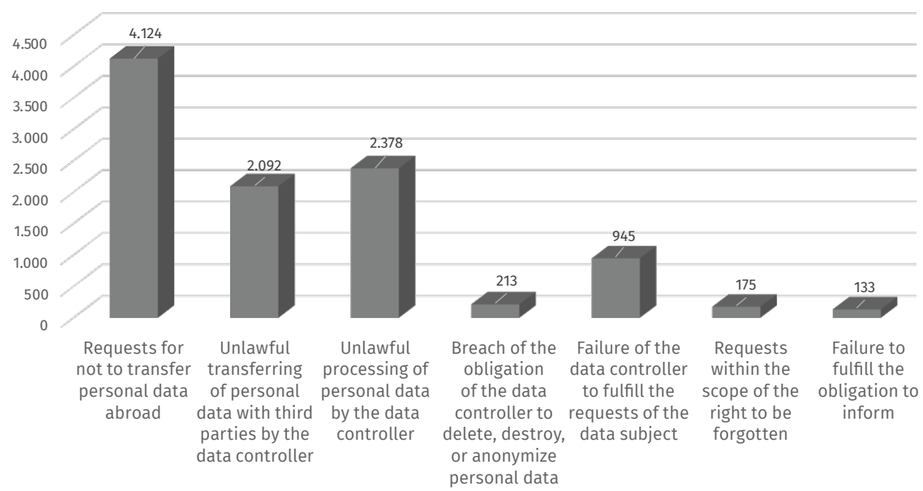
a) Distribution of Complaints in 2019[3]



b) Distribution of Complaints in 2020[4]



c) Distribution of Complaints in 2021[5]

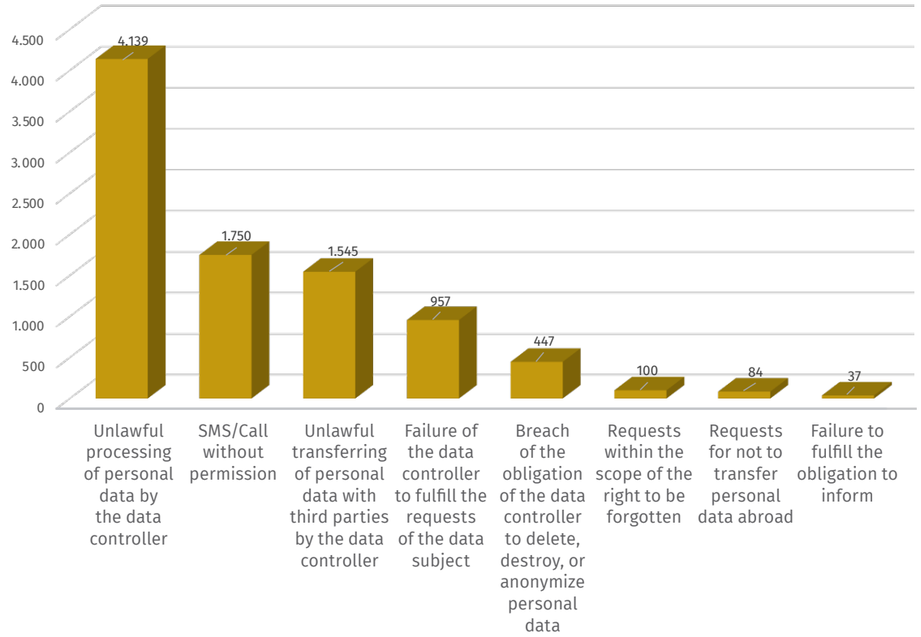


[3] Sourced from the 2022 Annual Report officially released by the Authority.

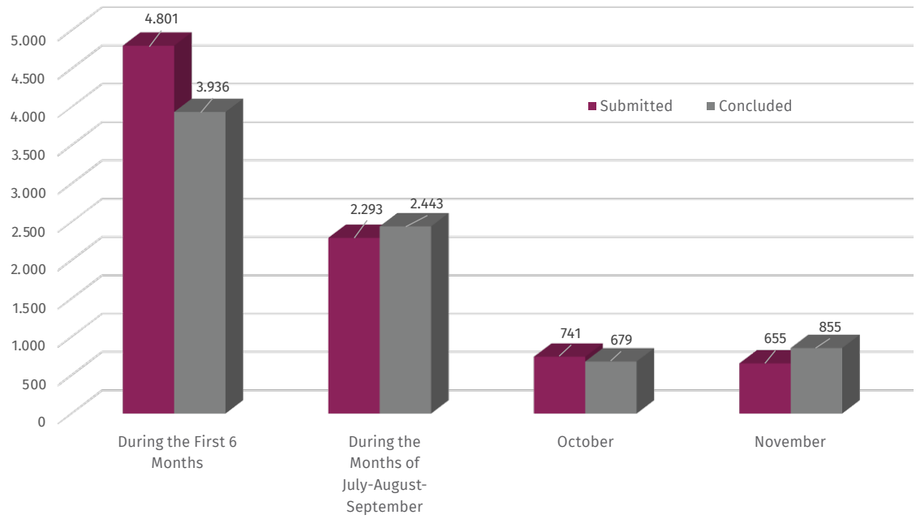
[4] Sourced from the 2022 Annual Report officially released by the Authority.

[5] Sourced from the 2022 Annual Report officially released by the Authority.

d) Distribution of Complaints in 2022[6]



e) Complaints and Reporting Notifications in 2023[7]



[6] Sourced from the 2022 Annual Report officially released by the Authority.
[7] Sourced from the DP Law Bulletins available on the official website of Authority.

4. Registration and Application Numbers for VERBIS and Numerical Status of Activities Conducted via VERBIS[8]

As of the date of publication of this study, the Authority has not disclosed the number of registrations, applications, and activities on VERBIS to the public. As of 31 December 2022, the statistical data regarding the registrations and applications to VERBIS are as follows:

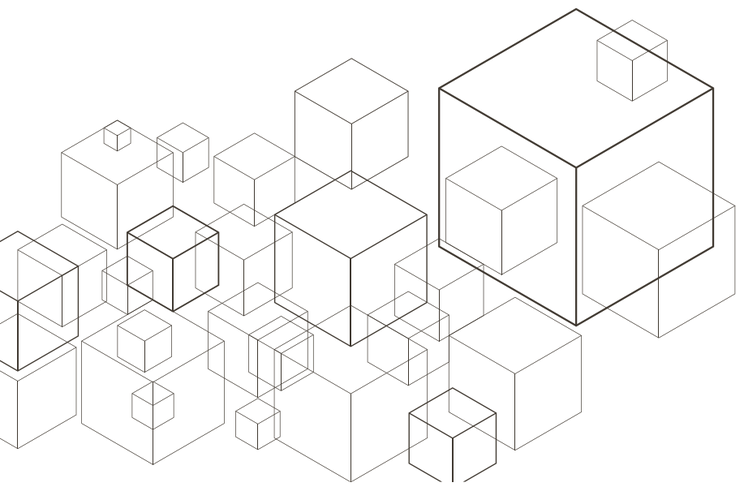
Number of Applications	Number of Approved Applications	Number of Rejected Applications	Number of Assigned Contact Persons
208,500	174,458	7,211	197,101

Performance	31 January 2022
VERBİS Application Approval	174,458
VERBİS Application Update Procedures	6,681
Calls Regarding VERBIS Applications	84,281
Number of Notification Queries	1,645,200

5. Commitment Letter Application

As of the end of 2023, the Board has concluded two commitment letter applications, and the total number of data controllers with approved commitment letter applications has reached six. Below, you can find the list of data controllers whose commitment letter applications have been approved:

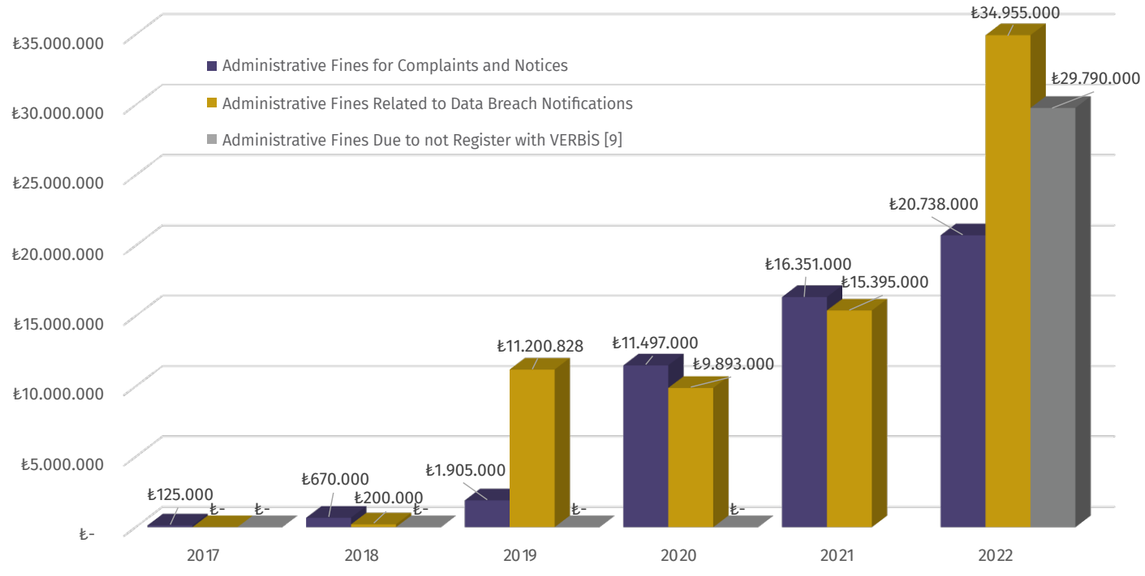
Data Controllers	Commitment Letter Application Approval Date
TEB Arval Araç Filo Kiralama Anonim Şirketi	9 September 2021
Amazon Turkey Perakende Hizmetleri Ltd. Şti. ve Amazon Turkey Yönetim Destek Hizmetleri Ltd. Şti.	4 March 2023
Turksport Spor Ürünleri San. Tic. Ltd. Şti. (Decathlon Türkiye)	22 Jun 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

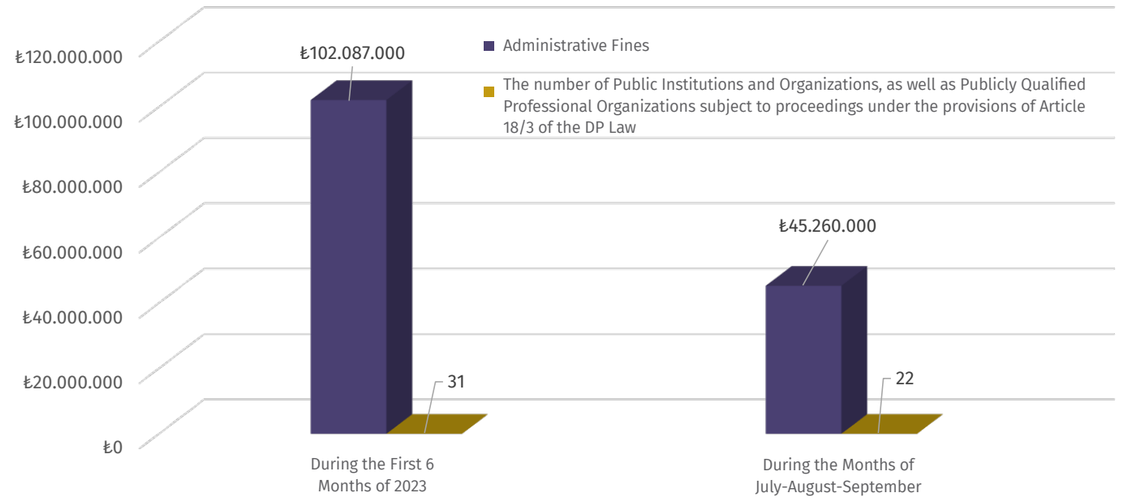


[8] Kurum tarafından yayımlanmış olan 2022 Faaliyet Raporu'ndan alınmıştır.

6. Sanctions

6.1. Administrative Sanctions





[9] The deadline for registration and notification obligations to the VERBIS was set as December 31, 2021; however, according to the announcement dated April 21, 2022, by the Authority, administrative sanctions will be imposed for non-compliance with the registration and notification obligations to VERBIS. Therefore, no administrative fines have been applied during the period of 2017-2021.

6.2. Review of Sanctions

- Administrative Fines totaling TRY 300,000,000 Between 2017-2022
  - The highest administrative fine published on the Board's website is the fine of 1,950,000 TRY imposed on WhatsApp under Decision 2021/28 dated 12 January 2021. This fine represents the highest penalty announced and imposed in a single instance since the Board's inception.

- 74 Summary/Short Decisions Published in 2023
  - Breach of necessary technical and administrative measures to prevent the unlawful processing of personal data resulted in 46 administrative fines.
  - Failure to promptly notify the Board and data subjects of the unlawful processing of personal data led to three administrative fines.
  - Non-compliance with general data protection principles resulted in seven administrative fines.
  - Failure to comply with Article 11, regulating the rights of data subjects, resulted in six administrative fines.
  - 21 decisions were made stating that there was no violation of the DP Law.

Among the decisions officially shared with the public on the institution's official website, it is observed that the Board has not imposed any administrative fines for non-compliance with its instructions and orders to remedy violations.

- Decisions Published According to Sectors

As compiled from the decisions published containing sector information on the Authority's official website in 2021, the distribution of the decisions made based on sector is as follows:

- 10 decisions in Banking and Finance
- 2 decisions in the Public Sector
- 12 decisions in Retail and Electronic Commerce ("**e-commerce**")
- 7 decisions in IT, Telecommunications, and Media
- 1 decision in Industry
- 2 decisions in Human Resources
- 10 decisions in Healthcare
- 4 decisions in Law
- 3 decisions in Marketing
- 17 decisions in Other Sectors[10]

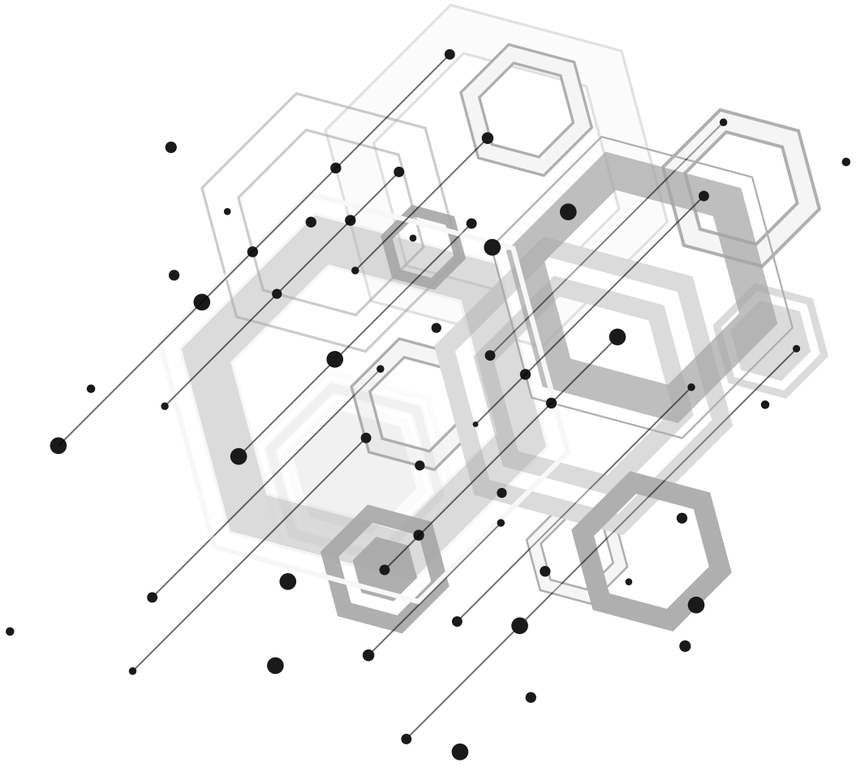
Additionally, sector information is not specified in six decisions.

[10] The data controllers subject to the decisions operate in the fields of logistics, education, cryptocurrency, construction, betting, pharmaceuticals, foreign exchange, sports facilities, and gaming.

6.3. Sanctions in Decisions Published According to the Relevant Articles of the DP Law

The distribution of decisions published on the Authority's official website in 2023 according to the relevant legal provisions is as follows:

Administrative Sanctions under Article 18 of the DP Law	No
Administrative Fine Due to Violation of Information Obligation - Article 18/1 (a)	2
Administrative Fine Due to Non-compliance with Data Security Rules - Article 18/1 (b)	41
Administrative Fine Due to Non-compliance with Board Decisions - Article 18/1 (c)	0
Administrative Fine Due to Non-compliance with Record-keeping Obligations - Article 18/1 (ç)	0
Disciplinary Provisions for Public Institutions and Official Authorities - Article 18/3	3
SUM	**46**



MOROĞLU ARSEVEN

6.4. Highest Administrative Fines

The table below lists the top 20 administrative fines imposed by the Board based on decisions announced to the public since 2018. On reviewing the five highest fines, it is observed that the Information Technology and Media sector ranks first as the sector with the highest number of fines. On reviewing the relevant decisions, it is understood that in four out of these five decisions, the violations are attributed more to shortcomings in information systems and failures to timely notify the Board, rather than administrative deficiencies related to data breaches.

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

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.

III.The Board's Principal Decisions

The Board has not published any principal decisions in 2023. You can review the latest principal decisions of the Board for 2022 here.

IV. Summaries of Key Decisions

1.Decisions Regarding the Banking and Finance Sector

1.1. Board Decision dated 10 February 2022, numbered 2022/107, regarding the processing of the data subject's mobile phone number by a savings finance company without relying on any data processing condition and sending SMS messages including advertising content

In the decision, a financial company, as data controller, sent commercial messages to the mobile phone number of the data subject. As a result of the examination conducted by the Board, it was emphasized that, in addition to complying with the legislation on sending commercial electronic messages, such messages must also take place within the framework of a data processing condition under Article 5 of the DP Law. Although it was stated in the case that the data subject's registration in the Consent Management System ("**CMS**") was performed by the data controller, it was not determined whether there was a relationship between the data subject and the data controller that would constitute the basis for registration in the CMS or whether explicit consent was obtained for the processing of the personal data of the data subject. Therefore, the Board decided to impose an administrative fine of TRY 75,000 on the data controller.

1.2. Board Decision dated 3 August 2022, numbered 2022/768, regarding the transfer of personal data of the data subject by the data controller bank to an insurance company without obtaining explicit consent

The data subject filed a complaint alleging that the data controller, an insurance company, had repeatedly contacted them using a mobile phone number obtained through a bank as the data controller. The data controller claimed that, according to the insurance agency agreement between them and the insurance company, they served as an authorized agent for the sale and marketing of the insurance company's products. The data controller also asserted that the data subject had given consent for receiving commercial messages related to campaigns, services, and products, and they contacted the data subject within this context.

However, in the defense presented by the data controller, no conclusive evidence or documentation was provided to prove that explicit consent had been obtained within the scope of the complained data processing activity under the DP Law. Additionally, the data controller failed to submit the required confidentiality agreement, as per the Regulation on the Sharing of Confidential Information, to be exempt from the obligation to keep confidential information. In light of these shortcomings, it was determined that the conditions for data transfer specified in Article 8 of the DP Law were not met, leading to the imposition of an administrative fine of TRY 250,000.

1.3. Board Decision dated 1 August 2023, numbered 2023/932, regarding the processing of a phone number not provided by the data subject as the contact number to the Bank through informing related to credit transactions

The data subject, through their mobile phone number, applied for an individual loan online, claiming to be a customer of the data controller bank. The data subject received text messages related to the credit application and with different content on a phone number registered in their name but not used for transactions with the bank. The complainant indicated that the bank had obtained the mobile phone number from the Credit Bureau ("CB") and, on checking the CB's website, confirmed that the phone number registered with the relevant organization was the same as the one provided to the bank. The data controller explained that the CB, under the auspices of the Turkish Banking Association ("TBA") Risk Center, houses all operational and technical activities on behalf of member banks, and in this regard, it is the official credit bureau providing all relevant data flows to credit institutions that could contribute to decision-making in the credit assessment processes of banks. The data controller asserted that CB, as an official credit bureau with member status, shares limited and proportionate credit information among financial institutions for specific purposes.

In this regard, the data controller stated that the processing of the alternative mobile communication number obtained from CB records was based on legal grounds, namely, the necessity for the data controller to fulfill its legal obligations, an explicit provision in law, and the necessity for the legitimate interests of the data controller. The Board found that during the credit request process, the mobile communication information declared by the customer and verified through reasonable methods (SMS OTP) was recorded. Access to this alternative communication information was stated to be automatically or manually accessed by responsible team members in the bank through necessary technical and administrative measures within the framework of the data transfer agreement signed between the data controller and the CB during the application security/fraud prevention process, where banks are legally obligated.

As this situation is regulated under Article 73/4 of the Banking Law numbered 5411 and other banking regulations, the Board concluded that there was no action to be taken under the DP Law against the data controller. If there are claims about the accuracy or currency of the information provided by the CB to the banks, the Board recommended that the data subject should initially address these requests and claims to the CB.

2. Decisions Regarding the Information Technology, Telecommunications, and Media Sector

2.1.Board Decision dated 17 March 2022, numbered 2022/249, regarding the transfer of personal data of the data subject to foreign countries by a technology company without explicit consent

The data subject, who became a member of the data controller's system via the website, filed a complaint as there was no cookie policy on the website, although the privacy notice indicated that data would be transferred abroad. The data subject stated that there was no explicit consent for such a transfer and, on contacting the email address on the website to inquire about the data transferred abroad, received no response within the legal timeframe.

The data controller argued that they had created a specific email address for data subject inquiries, and that the inquiry was inadvertently overlooked. The data controller also mentioned that the information about personal data processed through cookies was available in the privacy notice, and the information was conducted in compliance with the regulations. The data controller provided services using cloud service technologies located abroad, and the notification about the transfer abroad mentioned in the privacy notice occurred due to the storage of data on servers abroad to ensure effective protection.

The Board, considering the primary responsibility of the data controller to inform the data subjects before processing personal data, noted that effective measures had not been taken, and that the oversight of the data subject's inquiry was not justified. The Board emphasized that the transfer of data abroad is no different from the data processing activity, and there are additional conditions for the transfer of data abroad. It was also mentioned that the ways to commit to providing adequate protection in countries with sufficient protection were outlined, and the data controller did not have an approved commitment application. The Board found that the data controller did not obtain explicit consent from the data subjects for the transfer abroad. Considering these factors, the Board decided to impose an administrative fine of TRY 950,000, stating that the transfer abroad was not carried out in accordance with the DP Law.

2.2. Board Decision numbered 2023/134 regarding TikTok Pte. Ltd.

TikTok was subject to an ex officio investigation by the Board due to non-compliance with the principles of obtaining explicit consent under the DP Law, the unlawful acquisition of personal data, and complaints regarding security vulnerabilities in the software. In the course of the investigation, TikTok's defense letter, Privacy Policy, and Terms of Service were examined. The findings of the investigation include the following:

- Before updating the Privacy Policy in January 2021, profiles of users aged 13-16 were by default set to public, posing a risk, as there were no restrictions on accessing profiles of users in this sensitive age group, and no measures were taken to identify and mitigate these risks.
- Personal data of children under three years old were displayed, and data about children were collected without the consent of parents/guardians.
- The Privacy Policy did not provide clear information on the purposes and processing conditions of personal data, resulting in a violation of the principles of being "processed for specific, explicit, and legitimate purposes" and "relevant, limited, and proportionate to the purposes for which they are processed."

MOROĞLU ARSEVEN

- During the account creation process on TikTok, users were deemed to have accepted the Terms of Service and Privacy Policy if they continued to create an account. However, the Terms of Service section did not have the approval text prepared in Turkish, making the content not easily understandable to users, who could accept the terms without fully understanding them.
- TikTok's Privacy Policy, designed to fulfill the obligation to inform, was used as an explicit consent form.
- Personal data processing activity for profiling purposes using cookies was conducted without obtaining explicit consent from the data subjects.

As a result, TikTok was found not to have taken all necessary technical and administrative measures to ensure an appropriate level of security to prevent the unlawful processing of personal data, and was fined TRY 1,750,000. Additionally, TikTok was instructed to translate its Terms of Service into Turkish within one month, to bring the Privacy Policy into compliance with the DP Law within three months, and to provide adequate information in accordance with the principles and procedures specified in the Communiqué on the Procedures and Principles to be Complied with in Fulfilling the Obligation to Inform within one month.

2.3. Board Decision dated 10 November 2022, numbered 2022/1201, regarding the request for the removal of search results including the name and surname of the data subject, related to an announcement accessible on the official website of the Official Gazette

The Board's Decision dated 10 November 2022, numbered 2022/1201, regarding the request for the removal of search results including the name and surname of the data subject, related to an announcement accessible on the official website of the Official Gazette. The data subject lodged a complaint alleging that the page accessed through a search engine with their name on it linked to https://www.resmigazete.gov.tr/arsiv/*****.pdf, should be removed within the scope of the right to be forgotten, but the necessary action was not taken. The data controller argued that a balance test had been conducted between the privacy interest of removing the name from search results and the right to access information, including freedom of expression, and concluded that the balance was in favor of keeping it in search results due to the importance of the public interest. However, the data controller failed to provide evidence or documents proving that the data subject had given explicit consent for this processing activity.

The Board evaluated the case, stating that the indexing of content containing personal data on web pages in a certain systematic way constitutes a "personal data processing activity." Considering that the operator of a search engine determines the purpose and means of processing the data it collects from websites, the Board determined that the company operating the search engine held the status of "data controller".

Furthermore, the Board, in its assessment of the specific case regarding the removal of search results from the search engine, emphasized that the content was not related to the data subject's business life, and the purpose of processing the data in the content was not to present it to the public but to notify the data subject. Therefore, the Board concluded that there was no public interest in publishing the content. Additionally, the Board noted that the content was more than 20 years old, making it outdated, and highlighted the potential for bias despite the acquittal confirmed by a court decision. The Board decided to instruct the data controller to remove the URL address https://www.resmigazete.gov.tr/arsiv/*****.pdf from the index so that it could not be associated with the data subject's name and surname in search results related to the data subject's name.

3. Decisions Related to the Health Sector

3.1.Board Decision dated 29 June 2022, numbered 2022/630, regarding the sharing of photos taken during surgery by the data controller, a doctor working at the hospital, on social media without the explicit consent of the data subject

The data subject filed a complaint due to the sharing of photos taken during aesthetic nose surgery by a doctor employed within the data controller's organization on the doctor's social media account without obtaining explicit consent. The Board determined that the data subject had given explicit consent in the context of the data processing activity, with the data controller hospital being the party for which the explicit consent was given, but there was no explicit consent for the sharing of photos by the doctor. However, the Board noted that the data subject was aware of the photos being shared on the doctor's social media account and, accordingly, imposed an administrative fine of TRY 100,000 on the data controller hospital for failing to take necessary administrative and technical measures to prevent the sharing by the doctor. The Board also decided to inform the data subject that the data subject could pursue legal action under the Turkish Penal Code against the doctor.

3.2. Board Decision dated 22 June 2022, numbered 2022/594, regarding the transmission of the results of addiction-forming substance tests, which are special category personal health data, to the email address of a third party working at the workplace of the data subjects without obtaining explicit consent from the data subjects by a data controller, a private healthcare institution

The complainant stated that data subjects were forced to undergo a drug test by the employer without explanation, and the results were sent to the email address of a third party working at the workplace without explicit consent being given. As a result of the examination conducted by the Board, it was understood that the processing of special category personal data belonging to the data subjects by the data controller healthcare institution, in sending them to the email address of a third party working at the workplace of the data subjects, did not meet the data processing conditions specified in the DP Law, and explicit consent had not been obtained. In this regard, it was determined that a data breach had occurred due to the failure of the data controller to take all necessary technical and administrative measures to ensure an appropriate level of security to prevent the unlawful processing of personal data. The impact of the breach was not limited to the data subjects concerned, as the data processing activity involved processing special category personal health data of data subjects, and the data controller provided health services to approximately 600 employees in many cities. Considering these factors, an administrative fine of TRY 75,000 was imposed on the data controller.

3.3. Board Decision dated 11 May 2023, numbered 2023/787, regarding a complaint asserting that obtaining explicit consent from patients for the processing of personal data, including health data, by a hospital within the scope of advertising and promotional activities was unlawful

In the case, a complaint was filed stating that the data controller hospital's practice of obtaining explicit consent from patients for the processing of personal data, including health data, within the scope of advertising and promotional activities, was unlawful. The data controller stated that informative photo and video shoots were conducted with patients having certain diseases to create social awareness about lesser-known diseases and to inform the public about the characteristics and treatment process of these diseases with the aim of promoting public health. These images were shared on the company's website and social media accounts. According to the examination conducted by the Board, the 'Informed Consent Form for the Protection of Personal Data Specific to Photo/Video Shooting' presented to patients by the data controller required explicit consents to be obtained from patients for recording photo/video shoots for the purpose of carrying out marketing, advertising, and promotion processes, and stated that these recordings could be transferred to third parties, national, local, and international press organizations, and social media platforms.

As a result of its evaluation, the Board determined that, even though explicit consent had been obtained for the processing of personal health data with the aim of creating social awareness about lesser-known diseases, it was not mandatory to process personal health data, as it was possible to provide information about these diseases without processing any personal data. Therefore, alternative methods without processing personal data were available to achieve the intended purpose, and processing personal data was not necessary. In this regard, the Board concluded that the personal data processing activity violated the principle of proportionality. Moreover, despite the existence of explicit consent from the data subjects, considering sectoral regulations that prohibit private hospitals from making promotional advertisements to generate demand and the Private Hospitals Regulation, which states that private hospitals cannot make promotional advertisements with a demand-creating nature, the Board emphasized that explicit consent could not be put forward as a data processing condition in the case. Therefore, the Board imposed an administrative fine of TRY 250,000 on the data controller hospital.

3.4. Board Decision dated 2 May 2023, numbered 2023/692, regarding the requirement of obtaining explicit consent for the provision of health services offered by a private healthcare institution

In the case, the data subject filed a complaint with the Board because data subjects who wanted to schedule appointments on the website of the data controller, a healthcare institution, were unable to create an appointment unless the statement "I allow the use of my personal data for being informed about ... Health Group services and announcements, and for contacting me," was affirmed by checking a checkbox next to it. Before the Board's examination began, the data controller revised its website, allowing the provision of explicit consent not to be based on a service condition. However, the Board, despite the rectification of the unlawfulness, pointed out that the appointment service, which was a preliminary

step for data subjects to receive services, was linked to the requirement of explicit consent for the promotion of the data controller. This is because requiring an explicit consent statement for processing activities that solely benefit the data controller due to the promotion of its services and that are not directly related to the health service to be provided would impair the will of the data subjects in this regard. Moreover, although there are processing conditions other than the explicit consent processing condition for the personal data that should be processed in the appointment application form within the scope of the service, the Board emphasized that basing it on the explicit consent processing condition would be deceptive and an abuse of rights. Consequently, the Board imposed an administrative fine of a total of TRY 300,000, considering this situation as a violation of the principle of compliance with the law and honesty rules. Additionally, the Board instructed the data controller to remove the phrase "I approve the processing of my personal data in accordance with the Personal Data Protection Law" at the bottom of the appointment application form, which created the impression that consent was given to the privacy notice by reading it. The data controller was required to prove only the reading of the privacy notice by implementing a checkbox stating this, and the results had to be reported to the Board.

3.5. Board Decision dated 2 May 2023, numbered 2023/695, regarding the Unlawful Access to the Data of the Data Subject in the e-Nabız System by a Private Medical Center

The data subject filed a complaint due to the unlawful processing of their health data by a physician, an employee of a medical center where they had not previously received health services, who had accessed the health information through the e-Nabız system. The data controller stated that the secretary of the employed physician had accessed the data of the data subject from the e-Nabız system without the hospital being informed and consenting, stating that the data subject's privacy sharing settings were selected as "Allow All Doctors Connected to the Ministry of Health to View My Data," and that doctors could access the health data. In the course of the investigation conducted by the Board, it was determined that, although the data subject may have set the option as "Allow All Doctors Connected to the Ministry of Health to View My Data," granting access to their own records did not authorize other health personnel/doctors to process this data for purposes other than the intended one. It was understood that necessary arrangements (privacy agreements, access authorization definitions, etc.) for restricting access permissions were not provided. As a result, it was concluded that access to the data subject's information in the e-Nabız system had occurred without relying on any of the conditions for personal data processing stipulated in the DP Law. It was further determined that the data controller had not taken the necessary measures to ensure the protection of the physician's e-Nabız password and did not provide evidence of providing training to the physician and relevant employees on the protection of personal data. In light of these considerations, the Board decided to impose an administrative fine of TRY 200,000 on the data controller for failing to take reasonable measures to prevent unlawful access to personal data.

3.6. Board Decision dated 11 May 2023, numbered 2023/767, regarding the processing of special category personal data of a married couple through publication in a newspaper

The data subjects, due to adverse events while receiving healthcare from a private hospital, filed complaints against the treating doctor to the Ministry of Health, the Chief Public Prosecutor's Office, and the hospital. Additionally, after the treatment date, a high-circulation newspaper published a news article containing special category personal data of the data subjects. The data subjects alleged that the warning letter they had sent to the hospital was used as a source. The data subjects argued that the publication of personal data that had to remain confidential between the doctor and the patient in a newspaper constituted a violation of the law, as there was no public interest and, therefore, it could not be considered within the scope of freedom of expression and press freedom.
Moreover, the data subjects complained to the Board about numerous defamatory and offensive comments on social media made by the author of the article and the journalist who shared the news. To determine the lawfulness of the news, the Board emphasized that news should contribute to a public debate on general interest, be real and up-to-date, and maintain a balance between substance and form. In this regard, it was noted that was appropriate to determine whether the news merely served unnecessary curiosity or rather the protection of high moral and legal values, leading to social interest, enlightenment, and discussion, and shedding light on a certain problem and suggesting solutions.

The Board highlighted that the element of truth should be understood as conformity to the form of the event or news at the time it is presented, not its concrete reality. The language, expressions, and images used in the report should be in proportion to the form required by the news, avoiding expressions and words that might convey a different meaning to an average reader. It was emphasized that, when evaluating the balance between freedom of expression and personality rights, the overall content of the report should be considered, and the conflict of interests should be assessed by considering factors such as the contribution of the writing or statements to a discussion of general interest, the recognition level of the targeted person, the purpose of the text, the prior behavior of the relevant person toward the media, the method and accuracy of the obtaining of the information, the content, form, and consequences of the publication, and the severity of the sanctions applied due to the published report.

After the examination, the Board concluded that the report extensively detailed the incident between the parties, deviating from the essence intended to be narrated, and included unnecessary details such as all the details of the health problems of the individuals, words spoken during the incident, and the locations of the events, thus violating the privacy rights of the individuals involved. Furthermore, it was stated that, although there might be public interest in the making of the report, there was no benefit in the public knowing the details, and the publication of such personal data did not serve a situation concerning the general public or an issue discussed in public opinion. Therefore, the balance between the substance and form of the report was not maintained.

Consequently, the Board decided that due to the violation of the right to personality and the confidentiality of private life of the data subjects, the freedom of expression exception under Article 28/1(c) of the DP Law could not be prioritized. In this regard, as the special category personal data included in the report was processed without relying on a valid processing condition within the scope of the DP Law, an administrative fine of TRY 100,000 was imposed on the data controller for failing to take necessary technical and administrative measures to prevent the unlawful processing of personal data, prevent unlawful access to personal data, and ensure the security of personal data.

3.7. Board Decision dated 6 July2023, numbered 2023/1130, regarding the Sharing of the Data Subject's Medical Report and Medication Records with the Former Spouse by the Pharmacy

The data subject filed a complaint alleging that their hospital report and medication records were removed from the Medula system by a pharmacist and given to their ex-spouse during a custody dispute. The data controller stated that the pharmacy employee, unaware of the divorce and the animosity between the parties, had provided the reports to the data subject's ex-spouse for the purpose of assisting the data subject.

The data controller also stated that the data subject had given consent for their ex-spouse to collect medications, submit prescriptions to the pharmacy, and process prescription transactions on behalf of the data subject for a period of four years. It was emphasized that the data subject had not indicated any objection to the situation to the pharmacist.

The Board concluded that the pharmacist, as the data controller, had shared special category personal data belonging to the data subject obtained through the Medula system with a third party, their ex-spouse, without relying on any processing conditions stipulated in the DP Law. In this regard, it was assessed that the data controller had not fulfilled its obligation to take all necessary technical and administrative measures to ensure an appropriate level of security to prevent the unlawful processing of personal data, as required by the DP Law. As a result, an administrative fine of TRY 50,000 was imposed on the data controller within the scope of the DP Law, and the data controller, the pharmacist, was warned to exercise maximum care and diligence in complying with the regulations.

4. Decisions Regarding the Retail and E-Commerce Sector

4.1. Board Decision dated 7 July 2022, numbered 2022/653, regarding the request of the data subject for the disclosure of credit card and mobile phone information related to the online shopping service provided by the data controller

The data subject, in relation to online shopping carried out through the online shopping platform provided by the data controller company, requested an application to provide credit card information entered and contact information given for order delivery. However, the data controller stated that some of the orders for which the data subject requested order information were made from the data subject's membership account to a third party, and, therefore, due to the orders in question belonging to third parties and the absence of credit card information within the data controller, the application was rejected.

The Board determined that the credit card information was stored in the systems of the mobile payment technology provider intermediary company, and, therefore, the credit card information was not retained within the data controller. Moreover, the Board, in the decision, referred to the principles of the European Data Protection Board's "Guidelines 01/2022 on the Rights of the Data Subject - Right of Access," stating that access to personal data should not be provided to the data subject if the rights and freedoms of others are negatively affected, and the right of access to personal data takes precedence. In conclusion, the Board concluded that, due to the absence of the data subject's personal data, access to the phone number by the data controller under the right of access to personal data could not be provided to the data subject. However, the Board instructed the data controller to provide the data subject with the phone number given for the delivery of orders from the data subject's membership account through identity verification mechanisms.

4.2. Board Decision dated 18 May 2022, numbered 2022/491, regarding the continued publication of photographs of the data subject, who worked as a catalog model for a clothing store, on the data controller's website without explicit consent after the termination of the business relationship

The data subject filed a complaint due to the continued publication of photographs of products for which the data subject had modeled on the website of the data controller, without explicit consent, despite the termination of the business relationship with the clothing store. Following its examination, the Board found that the processing of the photographs of the data subject, based on the contract between the data subject and the data controller, fell under Article 5/2(c) of the DP Law. The Board deemed it appropriate for the data controller to retain the photographs for a limited period until the stock of the clothing items was depleted and concluded that there was no need for further action within the scope of the DP Law.

4.3. Board Decision dated 3 August 2022, numbered 2022/774, regarding the transmission of order information of a third party who made a purchase from an e-commerce site to the email address of the data subject

The data subject lodged a complaint stating that the personal data and order information of a third party making a purchase from an e-commerce site were sent to their email address. The situation came to light when they contacted customer service, and due to a name similarity, the email address was deleted. However, the data controller continued to receive promotional emails. The data controller argued that the notification was mistakenly sent to the data subject due to the name similarity and that there was no request from the data subject to stop sending emails. After its examination, the Board found that the personal data was processed without relying on any processing

conditions specified in Article 5 of the DP Law and that the data controller had failed to fulfill its obligations regarding data security. Considering the potential for loss of rights in the event of sending emails to the wrong recipient, the Board decided to impose an administrative fine of TRY 120,000 on the data controller.

4.4. Board Decision dated 22 March 2023, numbered 2023/426, regarding the request for e-Government passwords by a company offering the opportunity for shopping with consumer financing loans

The data subject, in the complaint, stated that while purchasing a television with a consumer financing loan from the company, the data subject had requested information on their e-Government password, but e-Government passwords were then obtained from many people other than themselves. The data controller, on the other hand, stated that the request for the e-Government password was made to invite the customer to the nearest branch to confirm their employment records through the insurance service statement. It was emphasized that the information could be obtained through the e-Government system, but the company did not request the e-Government password and did not know the e-Government password of the data subject. As a result of the examination conducted by the Board, a strong conviction was formed that access to the e-Government passwords of the data subjects had been obtained. It was concluded that by requesting e-Government passwords, access could be provided to considerable amounts of personal data, including special categories of personal data. Therefore, since the request for e-Government passwords in installment purchases did not rely on any data processing conditions specified in Article 5 of the DP Law, an administrative fine of TRY 400,000 was imposed on the data controller.

4.5. Board Decision dated 11 April 2023, numbered 2023/567, regarding the mandatory storage of credit/bank card information for making purchases on an e-commerce website

The data subject filed a complaint against the data controller due to a lack of lawful data processing conditions and non-fulfillment of the obligation to inform when making purchases on an e-commerce site. As a result of the examination conducted by the Board, it was understood that shopping could not be completed without card information being saved in the system, and after completing the purchase, the card information was stored in the wallet section. Referring to the Recommendation Decision 02/2021 on the Processing Conditions for Processing Credit Card Data Only to Facilitate Subsequent Online Purchases adopted by the European Data Protection Board (EDPB) on 19 May 2021, the Board stated that the processing condition for continuing to process card information for the purpose of facilitating subsequent purchases was considered consent. It was emphasized that the continued processing of card information by the data controller for the purpose of facilitating subsequent purchases indicated the emergence of a new data processing purpose. In this regard, the Board concluded that obtaining explicit consent from data subjects is necessary for the continued processing of card information after the completion of a current purchase transaction. It was considered that the practice of first saving the card information and then allowing customers to remove the card information from their accounts could lead to misleading the data subjects, contrary to the principle of "lawfulness and fairness." Similarly, the Board found that this data processing process violated the principles of "processing for specific, explicit, and legitimate purposes" and being "limited to what is necessary in relation to the purposes for which they are processed." As a result, the Board decided to impose an administrative fine of TRY 500,000.

4.6. Board Decision dated 18 May 2023, numbered 2023/845, regarding the unlawful processing of personal data by sending a short message to the data subject's phone by a courier employee

The data subject filed a complaint alleging that, after a courier delivered an order placed through an online shopping site, the courier had sent a harassing message to the data subject's mobile phone, and in this regard, the data controller had failed to ensure the security of personal data and allowed its employee to disturb the data subject. The data controller argued that the person who committed the act was not an employee of the company, and that the incident occurred without the company's knowledge. It stated that the personal data of the data subject was processed due to the transportation service.

In accordance with Article 66 of the Turkish Code of Obligations numbered 6098: "An employer is obliged to remedy the harm caused by the employee during the performance of the assigned tasks to others. The employer is not held responsible if it can prove that it exercised due diligence in selecting the employee, giving instructions related to the job, supervising, and preventing the occurrence of harm. However, in a business where individuals are employed, the employer is obliged to remedy the harm caused by the activities of the business unless it can prove that the working order of the business is suitable for preventing the occurrence of harm." The Board found that the employer would not be held responsible if it could prove that it exercised necessary care to prevent the damage. Additionally, in accordance with Article 2/6 and Article 2/7 of Labor Law numbered 4857: "The relationship established between the main employer and the subcontractor, who hires and assigns workers for auxiliary tasks related to the production of goods or services in the workplace or in a section of the main business, or in tasks requiring expertise due to the nature of the business and technological reasons, is defined as the main employer-subcontractor relationship. In this relationship, the main employer, together with the subcontractor, is jointly responsible for the obligations arising from this Law, the employment contract, or the collective labor agreement to the subcontractor's workers related to that workplace. The rights of the main employer's workers cannot be restricted by continuing to employ them through the subcontractor, and a subcontractor relationship cannot be established with someone previously employed in that workplace. Otherwise, generally, if the main employer-subcontractor relationship is deemed to be based on a simulated transaction, the workers of the subcontractor are considered employees of the main employer from the beginning. The assignment of work to subcontractors is not allowed except for jobs requiring expertise due to the nature of the business and technological reasons." The Board emphasized the joint responsibility of the main employer for the obligations arising from the employment relationship of the subcontractor's workers concerning that workplace. In this regard, the Board concluded that the data controller was responsible for the unlawful data processing incident according to the relevant provisions of the Turkish Code of Obligations and the Labor Law. Considering that there was no relationship between the data controller and the courier, as claimed by the data controller, and that necessary training was not provided to the employee, the Board decided to impose an administrative fine of TRY 250,000 on the data controller for failing to take necessary technical and administrative measures to ensure an adequate level of security and to prevent the unlawful processing of personal data.

MOROĞLU ARSEVEN

5. Decisions Regarding the Marketing Sector

5.1. Board Decision dated 3 August 2022, numbered 2022/776, regarding the processing of a child's personal data by a marketing company without obtaining the clear consent of the parent for promotional brochure delivery

In the case, a promotional brochure for a product owned by a marketing company was sent to an 8-year-old child (the data subject) via mail by an individual entrepreneur. The marketing company stated that there was a contractual relationship between the individual selling the products and the company, providing the option to purchase and sell company products. According to the company, the person selling the products acted as an independent business owner/entrepreneur within the scope of this contract, and there was no instruction from the company to the entrepreneur to send brochures. The entrepreneur, on the other hand, stated that, although the parent of the data subject provided their own address and contact information through the e-commerce website, the order was placed using the name of the child and the brochure was sent to them as part of this order. As a result of its evaluation, the Board concluded that there was no interest of the marketing company in the personal data processing activity under examination and, therefore, there was no action taken. However, it was noted that the brochure sent for promotional purposes to the data subject was not sent along with the order specified in the invoice. The Board decided to impose an administrative fine of TRY 30,000 on the data controller, the individual entrepreneur, for the sole brochure delivery, which was conducted without relying on any data processing conditions within the scope of the DP Law.

5.2. Board Decision dated 1 September 2022, numbered 2022/861, on the processing of personal data by a marketing company, involving the sending of commercial electronic messages without obtaining the explicit consent of the data subject, obtained from work-related emails obtained through internet search engines

The data subject filed a complaint against a data controller company with which they had no affiliation, alleging the receipt of campaign and advertisement-themed emails sent by the data controller to the data subject's email address without providing information on how their personal data was obtained. The data controller stated that they produced and marketed software for law firms, and they had obtained the email addresses of lawyers working in law firms through internet searches to conduct promotional activities for their software products. They stated that only the name, the name of the law firm where the data subject worked, and the email address were recorded in their systems, and the email content was intended for the promotion of a software product related to the data subject's profession. The Board emphasized that, according to Article 5/2(d) of the DP Law, the processing of personal data without explicit consent is possible when the data subject has publicly disclosed the data themselves. However, the Board clarified that public disclosure does not imply that such personal data can be processed for any purpose, emphasizing that it can only be processed in connection with and limited to the purpose of public disclosure. In this regard, the Board determined that the email address of the data subject, disclosed within the context of professional communication, did not express an intention for public disclosure related to marketing/advertising actions. Additionally, the Board highlighted that the Law on the Regulation of E-Commerce numbered 6563 allows the sending of commercial electronic messages to tradesmen and merchants without prior consent, but this provision cannot be applied to lawyers, as lawyers cannot act as tradesmen or merchants according to the Law on Lawyers. Therefore, sending commercial messages without obtaining consent from the lawyer data subject was deemed in violation of the law. As a result, the Board concluded that the data processing activity took place without any legal basis under Article 5 of the DP Law and imposed an administrative fine of TRY 150,000.

6. Decisions Regarding the Human Resources Sector

6.1. Board Decision dated 7 April 2022, numbered 2022/328, regarding the data controller providing payroll services sending a warning letter containing the personal data of the data subject to other employees

The data subject filed a complaint alleging a violation of personal data by the data controller, who had sent a warning letter containing the data subject's Turkish Republic Identification Number and address to them and seven other data subjects, stating that they had been placed on unpaid leave. The data controller explained that the data subject was an employee of another company within the same group and that they provided payroll services to employees of different companies within the group. Due to the mandatory nature of using unpaid leave during the COVID-19 pandemic, the information of the data subject was shared with them by the company. They further stated that the decision to extend unpaid leave had to be communicated through a warning letter, and in the warning letter, which had multiple recipients, the details of each recipient were included, and the personal data was shared via a notary public.

The Board determined that the data controller admitted to including the data subject's and seven other employees' information in the same warning letter. This sharing of personal data in a collective manner was considered a violation, and the Board decided to impose an administrative fine of TRY 100,000 on the data controller.

7. Decisions Regarding the Gaming Industry

7.1. Board Decision dated 23 December 2022, numbered 2022/1358, on failure to provide information and obtain explicit consent for cookies on a website

The data subject filed a complaint against a gaming platform for not providing information about its cookie processing procedures and not obtaining explicit consent for non-essential cookies. Following an examination, the Board found that the website used numerous cookies without providing any information about them. Additionally, it was noted that explicit consent was not obtained for non-essential cookies that track user activities for purposes such as advertising or statistics. As a result, the Board decided to impose an administrative fine of TRY 300,000 on the data controller.

7.2. Board Decision dated 28 September 2023, numbered 2023/1645, regarding the unlawful processing of personal data by a data controller holding the position of distributor and sole authorized representative of an extensively participated online game in Turkiye

The data subject applied to the data controller, a company serving as the distributor of an extensively participated online game in Turkiye, expressing the intent to exercise their rights under the DP Law. However, the data subject claimed that their requests were left unanswered by the data controller, and the information provided regarding the absence of international data transfers was incomplete and misleading. Furthermore, after examining the information text and privacy policy on the website, the data subject stated that it was understood that personal data was being transferred abroad. The data controller indicated that their company's partnership structure consisted entirely of foreign national shareholders. The company's operations were based on preparing digital game contracts between various parties in the industry, such as player-developers, player-publishers, player-player, licensor-licensee, trademark owner-trademark user, and so on. Therefore, the presence of foreign partners necessitated the international transfer of personal data from a procedural perspective. The data controller emphasized that all servers used for gaming services were located in Turkiye. Additionally, the processed personal data, including "email address, IP address," and, if the secure login application was selected, "mobile phone number," was stated to be processed in accordance with Article 5/2(c) of the DP Law to fulfill legal obligations arising from relevant legislation such as the Law on the Regulation of Broadcasts Made on the Internet and the Fight Against Crimes Committed Through These Broadcasts numbered 5651, Article 419/3 of the Turkish Code of Obligations, the Law on the Regulation of Electronic Commerce numbered 6563, the Turkish Penal Code, and the DP Law, without causing harm to the fundamental rights and freedoms of the data subject for the purpose of providing legal compliance and legitimate interests. Moreover, the data controller asserted that only the email address was processed within the scope of gaming services, players could enter the game with pseudonyms, and email addresses did not contain individuals' real names. Information such as gaming purchase records, movement records, item records, character information, server information, and so on, was claimed not to make a real person identifiable or determinable. Additionally, special software was used to detect cheating and fraudulent activities, aiming to identify codes consisting of zeros and ones in cheating and fraud programs. The software scanned only the code of declared cheating and fraud programs and did not transfer any personal data abroad.

The Board conducted an on-site examination by visiting the offices of the data controller and another company from which services were procured, and as a result, it concluded that there was no data transfer abroad with the systems used. Furthermore, it was understood during the investigation that the special software in question was used to determine whether game users engaged in cheating or fraud and did not involve unlawful processing activities to access personal data on players' computers. The "Privacy Policy" and "User Agreement" prepared by the foreign-origin major shareholder company, a significant shareholder of the data controller, were examined, revealing information about the potential transfer of personal data abroad. In this regard, the Board reviewed the information registered in VERBİS by the data controller. It was determined that identity, communication, and transaction security data were declared to be transferred abroad.

During the examination of the Information Note and Privacy Policy, it was observed that the "Registration Privacy Notice" and the "Personal Data Protection Policy" prepared by the data controller contained ambiguous expressions, while the "Privacy Policy" was prepared by the foreign-origin company, which was the major shareholder of the data controller. When examining the text titled "Privacy Policy," it was understood that this document was an online privacy policy presented to visitors, users, and customers by the company, the major shareholder of the data controller, and that this company was a separate data controller. However, it was determined that this text was not in compliance with Article 10 of the DP Law and the Communiqué on the Procedures and Principles to be Followed in Fulfilling the Obligation to Inform. In this regard, it was emphasized that this text, which was presented to data subjects during membership registration and assumed to be accepted in the user agreement, should be made compliant with the DP Law or removed, for consistency with other texts. Moreover, it was found that the text titled "Personal Data Protection Policy" was presented separately, and its content did not overlap with the other two texts.

In addition, under the cookie policy published on the data controller's website, two options were presented: "only use necessary cookies" and "allow all cookies." It was understood that by presenting the option "allow all cookies," a collective explicit consent was sought for each cookie type outside the necessary cookies category, and the option to choose was not provided to the data subjects. In the Cookie Banner and Cookie Policy, it was indicated in the cookie table that various cookies were used in the "necessary cookies" category by third-party cookie providers. It was noted that the third-party cookie provider was a foreign-based company and that, due to the absence of elements of "being specific to a particular matter" and "being given freely," the explicit consent was flawed, and a lawful personal data processing activity under Article 5 of the DP Law was not carried out. On the other hand, it was concluded that the transfer of personal data abroad using third-party cookies, which are in the mandatory cookie category and provided by companies based abroad, was unlawful due to the lack of legal grounds for data transfer abroad. In conclusion, the Board decided to impose an administrative fine of TRY 750,000 on the data controller.

8. Employment Relationship and Recruitment Process-Related Decisions on Personal Data Processing Activities

8.1. Board Decision dated 21 April 2022, numbered 2022/386, regarding the sharing of the termination of the employment contract of an employee on the data controller's social media account

The data subject requested the data controller to delete a post on the data controller's social media account, which contained the content: "... We apologize for the inconvenience caused to you by the DISMISSAL of ... due to irregularities he committed..." The data controller explained that the post was made to prevent harm to their customers by informing them about the activities of the data subject that could damage the commercial reputation of their companies. The Board, considering that the announcement, including allegations about the data subject's name, was published on the company's corporate social media account, accessible to everyone, and that there was no reasonable balance between the intended purpose of data processing under Article 4 of the DP Law and the action taken, concluded that it violated the principle of proportionality. Consequently, an administrative fine of TRY 30,000 was imposed due to the unlawful data processing activity taking place.

8.2. Board Decision dated 4 August 2022, numbered 2022/798, regarding the sharing of information about the content of a job interview, where the data subject had an interview with a company, by the company conducting the interview with the current workplace

The data subject, who was already working in one company, undertook a job interview with another company. The data controller company conducting the interview shared expressions arising from the interview that could harm the reputation of the data subject's employer company with the data subject's employer company, and, as a result, the data subject was placed on unpaid leave. Therefore, the data subject filed a complaint with the Board. The Board stated that the sharing activity by the data controller, which revealed information about the data subject's job interviews and his expressions about his current workplace during the job interview, violated the obligation to take all necessary technical and administrative measures to ensure an appropriate level of security to prevent the unlawful processing of personal data. Consequently, an administrative fine of TRY 100,000 was imposed.

8.3. Board Decision dated 2 June 2022, numbered 2022/896, regarding sharing legal correspondence containing the personal data of the data subject with their sibling by the former employer, the data controller

The data subject claimed that there had been a valid employment relationship with the data controller until the termination of the employment relationship for just cause. In this regard, certain personal data was processed without providing a privacy notice or obtaining explicit consent. Furthermore, the data subject alleged that legal correspondence information containing their name from a criminal investigation file, which had no relevance, was transmitted to the email address of the data subject's sibling without any connection. The data controller stated that the personal data of the data subject was processed within the scope of the employment relationship. The data controller argued that the data subject had violated obligations such as to safeguard trade secrets, not to share company software with third parties, and not to act contrary to confidentiality agreements. The Board determined that there was no basis for taking any action against the data

MOROĞLU ARSEVEN

controller within the scope of the DP Law regarding the processing of personal data within the employment contract. However, the Board found that the transmission of the prosecutor's complaint letter, which contained personal data of the data subject and other data subjects that was unrelated to the incident, to the sibling of the data subject via email was contrary to the obligation of the data controller to take necessary measures to prevent the unlawful processing of personal data. Consequently, an administrative fine of TRY 150,000 was imposed.

8.4. Board Decision dated 20 October 2022, numbered 2022/1147, on the continued processing of the personal data of a data subject by an employer after the termination of the employment contract

The data subject filed a complaint alleging that their former employer continued to use their image in the company's advertisements and that, after the termination of the employment relationship, the data controller had used the data subject's mobile phone number in the transportation processes of shipments. The data controller argued that the data subject's presentation of their profession in line with the terms of the employment contract was a necessary part of the position they were hired for, and it fell within the scope of their duties. According to the signed privacy notice, the data controller claimed that the data subject would be considered to have given consent for the processing of their personal data for marketing purposes, including appearing in company advertisements. The Board determined that the presence of the data subject's images in the archives of the data controller was lawful. However, the continued processing of these data by sharing them after the termination of the employment contract did not meet a valid processing condition within the scope of the DP Law. Additionally, it was found that the personal data of the data subject, registered with courier companies, was processed in violation of the DP Law. Consequently, an administrative fine of TRY 250,000 was imposed.

8.5. Board Decision dated 10 August 2023, numbered 2023/1356, regarding the presentation of images of the data subject's worship in a mosque in a reinstatement lawsuit by an employer

The data subject filed a complaint alleging that images of their worship in a place of worship, which qualified as sensitive personal data, were recorded by their former employer without their consent. They claimed that, shortly before the termination of the employment contract, they were asked to sign documents related to the retrospective processing of personal data, and the recorded images were submitted by the company to a court file in a dispute with the company. The data controller stated that the termination of the employment contract was due to the data subject's disruption of their duties within the scope of their job, absenteeism, and orchestration of false reports against the company and its officials, which had led to a criminal complaint about the reports. The data controller also argued that the video footage was processed as "physical space security" data to monitor any incidents within the mosque where the data subject performed their prayers. Therefore, they asserted that explicit consent was not required to be sought from the data subject for the processing of this non-recorded data. The Board concluded that the explicit consent for the personal data processing activity was not given freely, as the data subject had been compelled to sign without their consent due to the fear of termination.

It was determined that the data processing activity was carried out without relying on any legal basis and, even if explicit consent were obtained, the processing would still violate general principles. As a result, the Board decided to impose an administrative fine of TRY 300,000 on the data controller, instructing the cessation and destruction of the data processing and providing guidance to the data controller on compliance.

9. Decisions Regarding Other Sectors

9.1.Board Decision dated 11 April 2023, numbered 2023/570, regarding an excessive request for personal data for an increase in membership level by a crypto asset service provider

The data subject alleged that the data controller, a crypto asset service provider, processed personal data excessively and disproportionately by requesting the front and back photos of their identity card along with their own photo for the purpose of increasing their membership level on the platform. The data controller, a crypto asset service provider, stated that the data processing activity took place due to their obligations relating to the prevention of money laundering and the financing of terrorism according to the Regulation on Measures Regarding the Prevention of Laundering Proceeds of Crime and Financing of Terrorism ("**Measures Regulation**"). Moreover, the data controller stated that, if there was no cryptocurrency withdrawal transaction, there would be no need to share this data. The Board emphasized that there are detailed regulations on customer identification under the Measures Regulation and in the Crypto Asset Service Providers Guide published by MASAK, and it was highlighted that "identity verification" is the most crucial measure within the obligation of customer recognition.

The Board also noted that users could benefit from the services provided by the data controller by opening an account, and during the account opening process, various identity data were requested from users. It was understood that within these opened accounts, users were free to perform transactions up to a certain limit. Additionally, the Board stated that, for users to elevate their membership level and to perform transactions above a certain limit, it was necessary to share a photo of their Turkish ID card with the front and back sides, along with a photo of themselves holding a paper with a specific expression and the date written on it. The Board justified this requirement by considering that there was a public interest in identifying the user's identity, as there was a possibility of engaging in money laundering activities within the data controller's field of operation. As a result, the Board decided that the data controller had an obligation arising from the relevant legislation, such as Law on the Prevention of Money Laundering numbered 5549, and the processing of personal data was based on the legal ground of being "clearly stipulated in the laws" under Article 5/2(a) of the DP Law, and, therefore, no action needed to be taken within the scope of the DP Law.

9.2. Board Decision dated 20 July 2023, numbered 2023/1234, regarding the processing of personal data by a car rental company through requesting a Findeks report from the data subject

The data subject filed a complaint stating that the car rental company requested a Findeks report from them and made providing explicit consent for the processing of the data in the report a condition for being able to benefit from the car rental service. Allegedly, the vehicle was not delivered to the individual due to this reason.

The data controller stated that they had not requested a Findeks report, and that the reason for the individual not benefiting from the service was their refusal to provide a deposit. The data controller emphasized that the data was processed by the platform managing the vehicle, and, therefore, any complaints and requests should be directed to the platform selling travel tickets to users. The car rental company only interacted with the customer during the delivery of the vehicle. The platform processed the reservation and customer data, and a confidentiality agreement was in place between the platform and the car rental company, ensuring the necessary technical measures for data transfer were taken. The platform asserted its role as an "intermediary service provider," explaining that the contractual relationship involved notifying service providers when services were sold through the platform and purchased by users. The platform stated that it was not responsible for any illegal situations arising from the service or product and that the commission was collected from users through the platform, with a corresponding commission invoice issued, and the commission amount was separately paid to the platform by the car rental company. The Board considered that the processing of personal data through an inquiry of Findeks report information can only be carried out with explicit consent under Article 5/1 of the DP Law, and in this regard, tying explicit consent to the service condition by the data controller was a violation of their obligations under the DP Law. Therefore, an administrative fine of TRY 100,000 was imposed on the data controller. Additionally, the data controller was reminded to appropriately conclude any future applications and to ensure the destruction of the data.

9.3. Board Decision dated 3 August 2023, regarding the unlawful sharing of personal data of the data subject with third parties by an airline company

The data subject reported that, when entering their Passenger Name Record ("PNR") and surname to perform a check-in process with an airline company, the details of four unfamiliar individuals, including "name, surname, gender, date of birth, nationality, document type, issuing country of the document, document number, last validity date, visa information," were displayed. This situation raised concerns as it allowed the data subject to make changes to the tickets of individuals they did not know. To obtain detailed information about this process and potential access to their data by others, the data subject invoked their rights under Article 11 of the DP Law and submitted a complaint to the data controller. However, the data subject claimed that the data controller provided incomplete information about the process, leading them to appeal to the Board. The data controller asserted that it had taken the necessary technical and administrative measures to protect data privacy on the system, emphasizing the obligation of the travel agency creating the record not to combine different individuals with the same surname into a single Group PNR. They also claimed to have implemented the required security measures to prevent unauthorized access to personal data. The data controller stated that the data subject's PNR content was updated to ensure that they could only view their family members within the PNR and that a reminder was sent to travel agencies instructing them to separate the PNRs of passengers with the same surname but different family members.

Contrary to the data controller's claims, the Board, based on the screenshots provided by the data subject, observed that, even when the entry process was performed with the combination of PNR + SURNAME, individuals with different surnames could still be viewed under the same PNR. The Board concluded that this demonstrated the data controller's failure to take the necessary technical and administrative measures to prevent unauthorized access and to ensure the protection of personal data in line with the DP Law. Given the potential impact on numerous individuals and the data breach, the Board decided to impose an administrative fine of TRY 300,000 TL on the data controller.

9.4. Board Decision dated 3 August 2023, regarding the sharing with third parties of the personal data of the data subject by a hotel employee

The data subject filed a complaint alleging that a document containing information about the period they stayed at a hotel owned by the data controller was sent to them by a third party through a social media application and that this document was shared with third parties by a hotel employee. The data controller explained that luxury hotels, as per their standards, address guests by their last names to create a personal and exclusive atmosphere. Additionally, they mentioned that in case of emergency, floor service personnel need to ensure the well-being of guests. The data controller asserted that the document was stored in locked cabinets with a limited number of keyholders in a physical archive, and, during the relevant period, it was periodically destroyed. The Board determined that including the names and last names of customers in the document was an excessive data processing activity. It concluded that the personal data in the document shared with third parties was created within the data controller's structure and that the data controller had failed to take necessary administrative and technical measures, leading to the violation of the obligation to prevent unauthorized access to personal data and to ensure its protection. Therefore, an administrative fine of TRY 500,000 was imposed on the data controller. Additionally, the data controller was instructed to comply with the obligation to ensure an appropriate level of security to prevent unauthorized access to personal data, to provide information to the Board about the outcome of the measures to be taken, and to implement a separate explicit consent mechanism in the information text for processing for marketing purposes in accordance with the provisions of the DP Law.

9.5. Board Decision dated 17 August 2023, numbered 2023/1414, regarding the transmission of special category personal data of the data subject by a lawyer to the court

The data subject stated that a company with which they agreed to conduct a DNA test had sent encrypted DNA reports to the data subject's email address in confidentiality. The data subject accused the data controller, who was the opposing lawyer in a debt lawsuit, of unlawfully accessing the personal data of the data subject and their children through this encrypted email address and using it against the data subject in the debt case. The data controller explained that the DNA test reports of the data subject were submitted to the court file on a request for use in a lawsuit concerning the determination of family ties against family members. The data controller asserted that they processed this information by working on behalf of the data subject's ex-spouse and children within the scope of legal representation. They argued that this data processing activity, falling within the scope of legal representation, was based on the explicit consent obtained from the data subject's children and that there was no legal impediment since the data subject was a party to the lawsuits.

The Board evaluated the situation within the scope of Article 6/3 of the DP Law with reference to the objectives of the Law on Lawyers numbered 1136, which regulates the duties and authorities of lawyers, and its Article 35 emphasizing the duties and authorities of lawyers, and concluded that the data processing was compliant with the DP Law. Additionally, the Board referred to the evidence rules in the Law on Civil Procedure numbered 6100 and indicated that the processing of genetic data by the data controller and its transfer to the relevant courts were also in line with Article 8 of the DP Law. Furthermore, the Board emphasized that there was no evidence proving the lawyer's unauthorized access to the data, and the DNA test report, which contained information not only about the data subject but also about their children, was considered shared personal data with the children. Given the circumstances of the case, the Board concluded that there was no adverse consequence for the data subject's data security due to the submission of this document to the court. Therefore, the Board decided that there was no violation of the DP Law in relation to the complaint.

9.6. Board Decision dated 24 August 2023, numbered 2023/1461, regarding recording audio and video by an educational institution through cameras

The complainant stated that there had been a meeting between the data controller and one of the data subjects due to a rental dispute, and during this meeting, voice and image recordings of the data subjects were obtained, as declared in a warning letter sent by the data controller. The data controller asserted that the video and audio recordings were made in public areas, and that the video and audio recording during the rental payment with the landlord was for security and evidential purposes. It was emphasized that this did not constitute a violation of Article 133 of the Turkish Penal Code numbered 5237, and, as there were not 50 employees, there was no obligation to register with VERBIS. The data controller also raised the defense that they did not process personal data related to the other person, with whom they had no legal relationship, and had no obligation to respond to requests. Additionally, it was stated that the obtained video and audio recordings would be used by judicial authorities, and it was emphasized that this did not violate the DP Law. The Board acknowledged that the video recording was a legitimate, appropriate, and proportionate measure for security purposes. However, it pointed out that the audio recording did not share the same legitimacy. The Board emphasized that the audio recording constituted a significant interference with the fundamental rights and freedoms of the data subjects and lacked a legitimate interest. In this regard, it was evaluated that the audio recording was an unlawful data processing activity, and an administrative fine of TRY 200,000 was imposed on the data controller for acting contrary to Article 12 of the DP Law. Furthermore, it was determined that, although the video recording was based on a legal basis, the obligation to inform was not fulfilled. Therefore, an additional fine of TRY 30,000 was imposed.

C. EXPECTED DEVELOPMENTS

I. Amendment on the DP Law

Within the scope of the Human Rights Action Plan ("Plan") published by the Ministry of Justice in April 2021, it was foreseen that the DP Law would be brought into compliance with European Union ("EU") standards within one year. Furthermore, in the 11th Development Report, it was stipulated that the DP Law would be harmonized with EU legislation. In adherence to these provisions, a dedicated working group was established in September 2022 under the auspices of the Ministry of Justice, effectively coordinating efforts. The culmination of these endeavors pertaining to legislative modifications was announced last year following their completion, as articulated during the Authority's Wednesday Seminars. The Minister of Justice formally communicated this development. As per the official announcement, emphasis was placed on forthcoming changes primarily concerning the processing of sensitive personal data and the international transfer of data. However, it is noteworthy that, as of the end of 2023, no legislative amendments have been enacted; nevertheless, declarations affirming the intent to initiate such changes persist. Within the context of the Medium-Term Program (2024-2026), it has been explicitly stated that the harmonization process of the DP Law with the EU acquis, particularly aligning with the GDPR and conforming to EU digital economy regulations, is slated for completion by the fourth quarter of 2024. Furthermore, the program underscores an expedited consideration of regulations addressing urgent matters related to direct investments.

II. Regulating Data on Electronic Platforms

On 7 July 2022, Law numbered 7416 amending the Law on the Regulation of Electronic Commerce was published in the Official Gazette numbered 31889. Subsequently, on 29 December 2022, the Regulation on Electronic Commerce Intermediary Service Providers and Electronic Commerce Service Providers was issued, as published in the Official Gazette numbered 32058. However, on 10 May 2023, the execution of many provisions included in the aforementioned legislative amendment was suspended by the 10th Chamber of the Council of State. With the Constitutional Court Decision dated 13 July 2023, numbered 2022/109 E., 2023/125, it was decided by majority vote that the provisions related to the Constitutional Court's decision are not in violation of the Constitution, and the decision to suspend the execution of these provisions was lifted. In line with this, certain obligations regarding the portability of data obtained by electronic commerce service providers from sales conducted by electronic commerce intermediary service providers above a certain volume were introduced into the Law on the Regulation of Electronic Commerce ("ECL") numbered 6563. Similarly, it is anticipated that the Authority will publish a guide regarding the data ownership of personal data obtained through sales in the electronic commerce environment.

III. Regulations on Data Portability

On 14 October 2022, a draft amendment to the Law on the Protection of Competition numbered 4054 ("Competition Law") was shared with relevant parties for feedback, particularly aimed at safeguarding competition in digital economies. During this period, the Competition Board imposed administrative fines on Facebook in 2022 for hindering the activities of competitors in the markets of social networking services for personal purposes and online video advertising, due to the integration of data collected from Facebook, Instagram, and WhatsApp services, referred to as "core services". The Competition Board concluded that such actions disrupted competition and created barriers to market entry, constituting a violation of the Competition Law.

Although anticipated changes to the Competition Law did not materialize in 2023, the Competition Board continued to impose administrative fines on digital platforms for disrupting the competition environment due to data usage and for violating the relevant provisions of the Competition Law. In this regard, a fine of TRY 61,342,847 was imposed on DSM Grup Danışmanlık İletişim ve Satış Tic. (as known as, Trendyol) by the Competition Board for unlawfully gaining an unfair advantage in its retail activities by manipulating algorithms and utilizing data from third-party sellers on its marketplace. Additionally, Sahibinden Bilgi Teknolojileri Pazarlama ve Ticaret AŞ received a fine of TRY 40,100,000 for abusing its dominant position in the second-hand digital market. Given the increasing impact of data usage on the competitive landscape, especially considering the market position of digital platforms, it is expected that the draft version of the Competition Law will be finalized and enforced in 2024.

Furthermore, similar changes related to data portability and access have been made under the ECL for the same purpose (see Section C.II.). Specifically, electronic commerce intermediary service providers with a net transaction volume exceeding ten billion Turkish Liras in a calendar year are required to enable the free portability of data obtained from the sales of electronic commerce service providers and to provide free and effective access to processed data. As of May 2023, the execution of the provision on data portability in the ECL has been suspended by the 10th Chamber of the Council of State and reinstated as of July 2023 by the Constitutional Court decision. Violations of data portability regulations may result in fines of not less than TRY 100,000, calculated as five-thousandths of the net sales amount for the calendar year preceding the date of the violation.

Issues related to data portability in competition and e-commerce sectors are actively shaping the agenda, and legislative implications are evident. Additionally, under the legislative change mentioned in Section C.I., during the harmonization process of the DP Law with the ECL, it is possible that Article 20 of the ECL related to data portability may be brought within the scope of the DP Law. Therefore, given the ongoing regulatory developments, especially in areas where personal data, including data portability, can be utilized as a significant competitive input, further guidance or legislative changes within the DP Law are anticipated.

MOROĞLU ARSEVEN

IV. Regulations Regarding the Personal Data of Children

As mentioned in Section A.II.3, the Regulation Amending the Regulation on Pre-School Education and Primary Education Institutions of the Ministry of National Education has been published. It stipulates that photos of students taken during educational activities, social and cultural events, as well as during trips and observation activities both inside and outside the school, cannot be shared on social media platforms and communication groups under any name without obtaining written consent from the parent and supervision by the guidance counselor. In recent times, it has been observed that children's data is used extensively, especially due to online games and social media usage.

The Board has been conducting various awareness campaigns since 2019 regarding the protection of the personal data of children. However, as of yet, no guide or public announcement has been issued on this matter. Changes encompassing stricter protection of the personal data of children, especially on online platforms (e.g. social media and online gaming platforms), and the publication of guidelines by the Board regarding considerations for processing the personal data of children are expected in 2024.

V. Financial Data Access

The European Commission published the Payment Service Directive 3 (PSD3), Payment Service Regulation 1 (PSR1), and Financial Data Access Regulation under the Financial Data Access and Payments Package on 28 June 2023. With this release, a significant step has been taken to make substantial changes to the legislation regulating the financial sector, including payment systems, within the EU. The aim is to enhance the synchronization of the payment and finance sectors in the digital age, to improve competition in electronic payments, and to provide access to financial products and services that securely share consumer data. In this regard, assessments related to the Regulation on Financial Data Access under the scope of the General Data Protection Regulation (GDPR) have been publicly disclosed as of 22 August 2023, through Opinion 38/2023 issued by the European Data Protection Authority.

In Turkiye, however, despite the Board having previously issued the Banking Sector Good Practice Guide on the Protection of Personal Data and providing detailed explanations regarding the protection of personal data within the banking sector, no publication has yet been shared that encompasses the financial and payment sectors. In the context of Turkish legislation, strict regulations are in place for the protection of primary system data in the financial and payment sectors, including finance and factoring companies. Alongside the protection of primary system data outlined in the relevant legislation, it is anticipated that the Board will issue a guide regarding the compliance of personal data included in a primary system with the regulations of the DP Law.

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 to 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 (VERBİS) 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

Our Team

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

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

CEYLAN NECİPOĞLU, PH.D, LL.M.
Lawyer
cnecipoglu@morogluarseven.com
D: +90 (212) 377 47 35
T: +90 (212) 377 47 00

MOROĞLU ARSEVEN

www.morogluarseven.com

Abdi İpekçi Caddesi 19-1
Nişantaşı, İstanbul, 34367

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