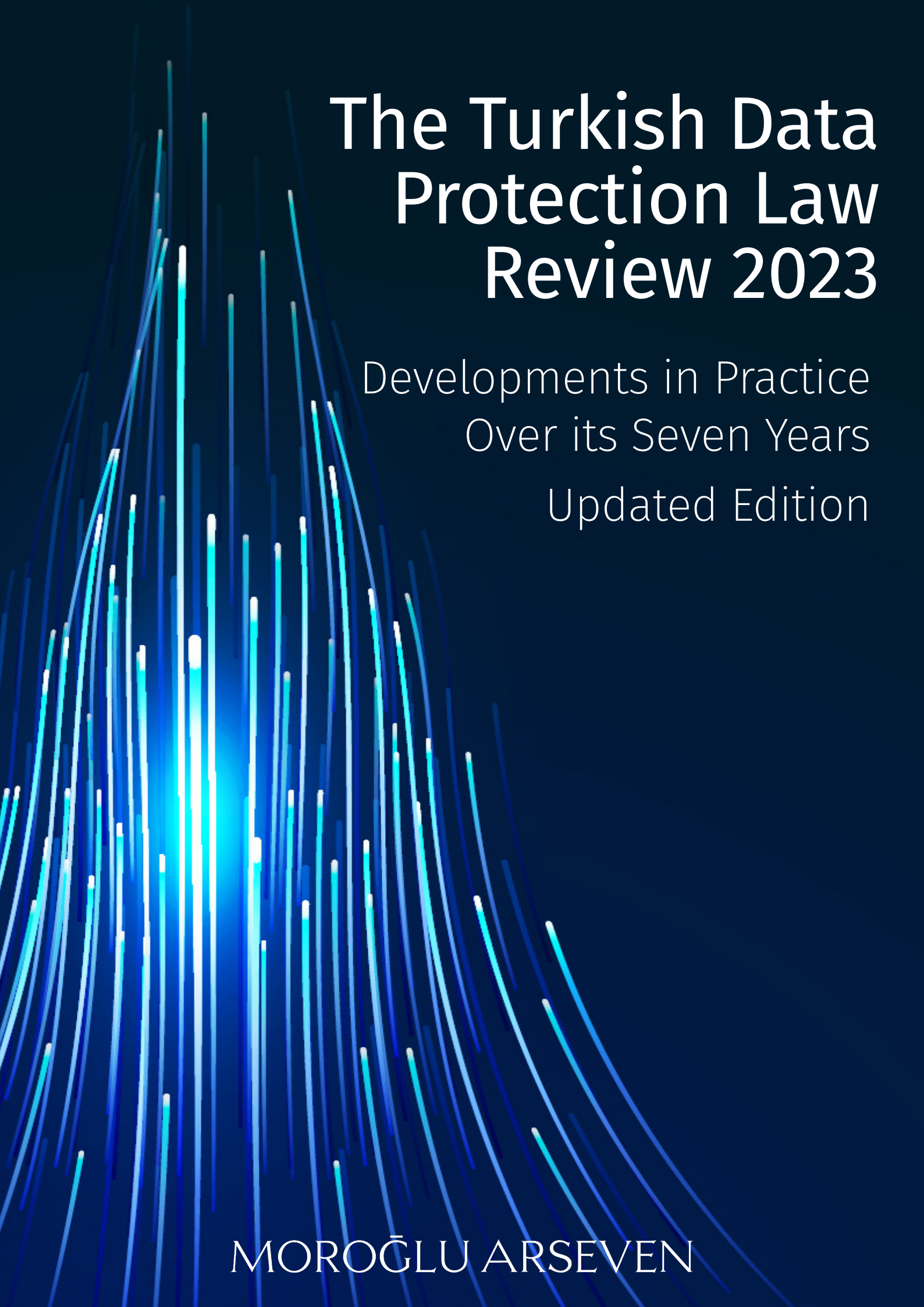
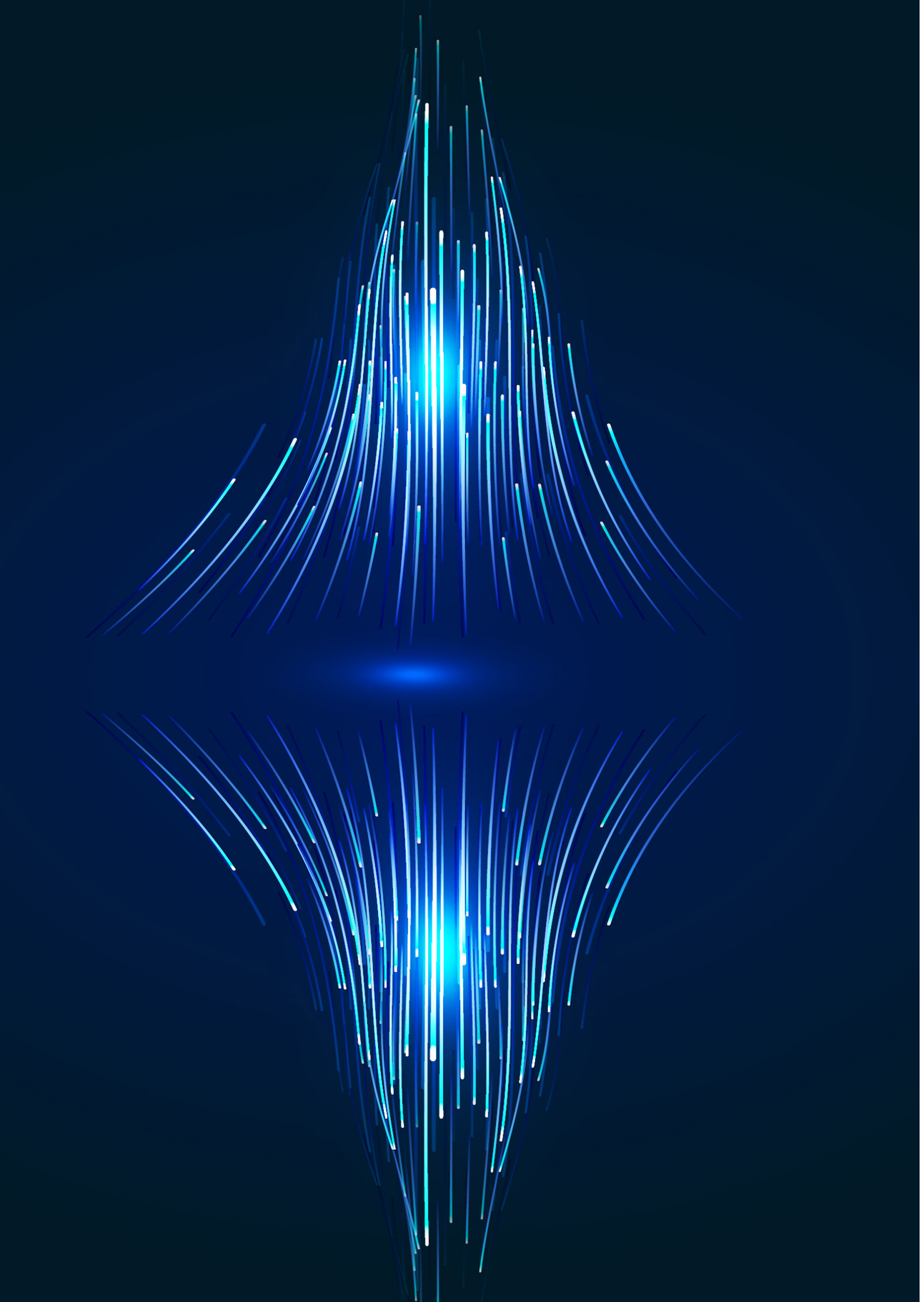


The Turkish Data Protection Law Review 2023

Developments in Practice Over its Seven Years

Updated Edition

MOROĞLU ARSEVEN



Preface

This guidelines, which we have published since the fifth year of the Law of Protection of Personal Data No 6698, we are glad to be presenting our third guideline, in relation to compliance processes under the Law of Protection of Personal Data, amended practices and the Board of Personal Data Protection's most recent approach to these issues in the Law of Protection of Personal Data No 6698's seventh year in practice between 28 January 2022 and 28 January 2023.

This guideline has been prepared based on the data included in the Board of Personal Data Protection's 2021 activity report dated 28 January 2023 and the decisions posted on the Board of Personal Data Protection's official website as of the date of guideline. It has been updated to your attention after the publication of the 2022 activity report on 12 April 2023.

Contents

MOROĞLU ARSEVEN

A. MAJOR DEVELOPMENTS IN LEGISLATION AND PRACTICE

The Turkish Data Protection Law in 2023 | Developments in Practice Over its Seven Years

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

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

The Board of Personal Data Protection ("Board") was established under the DP Law as a part of the Personal Data Protection Authority ("Authority") as a financially and administratively autonomous public legal entity with regulatory and supervisory authority.

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.

- 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

A number of regulations were introduced in 2022, one of which is a direct sub-legislation of the DP Law, while the others are set out in other laws and secondary legislation. The main legislative amendments in relation to personal data protection are set out below.

The regulations are listed in the form of laws, regulations, communiqués and circulars.

1. Law No. 6563 on the Regulation of Electronic Commerce

Law No 7416 Amending Law No 6563 on the Regulation of Electronic Commerce ("Amending Law") was published in the Official Gazette dated 7 July 2022, No 31889.

The Amending Law has introduced definitions of:

- "Electronic commerce service provider" (service providers who provide goods or services in electronic commerce marketplaces or their own electronic commerce environment).

- "Electronic commerce intermediary service provider" (service providers who act as an intermediary for the conclusion of contracts for the delivery of goods or services in electronic commerce marketplaces or their own electronic commerce environment).

The Amending Law also introduces new definitions of "electronic commerce marketplace", "net transaction volume" and "economic integrity". The Amending Law aims to prevent unfair competition and monopolization in e-commerce and to facilitate the entry of new actors into the market, as well as the balanced and healthy growth of the market.

The Turkish Data Protection Law in 2023 | Developments in Practice Over its Seven Years

In relation to data protection under the Amending Law:

• Electronic commerce intermediary service providers and electronic commerce service providers must keep specific information, documents, books and electronic records of their business and transactions for a period of 10 years from the date of the business or transaction.

• The Ministry of Commerce can obtain the subscriber information of real or legal persons who send commercial electronic messages via voice calls and text messages from the Information and Communication Technologies Authority.

In addition, an important obligation to protect data obtained through sales has been included for electronic commerce intermediary service providers whose net transaction volume in a calendar year is over 10 billion Turkish Liras. Such electronic commerce intermediary service providers must provide electronic commerce service providers with the technical means to maintain data obtained due to the intermediary's sales free of charge, and provide free and effective access to this data and obtained processed data.

Most of the amendments will enter into force on 1 January 2023, while subparagraph (b) and paragraph 10 of paragraph 2 of Annex-2 and paragraph 6 of Annex-4 will enter into force on 1 January 2024.

2. Regulation on Collection, Storage and Sharing of Insurance Data

The Regulation on Collection, Storage and Sharing of Insurance Data ("Insurance Regulation") was published in the Official Gazette dated 18 October 2022, No 31987. This regulates the procedures and principles for the collection, storage and use of insurance data and the sharing of such data with insurance, reinsurance and pension companies engaged in insurance activities, as well as other persons and institutions as determined by the Insurance and Private Pension Regulation and Supervision Authority ("IPPRSA"). The Insurance Regulation has now entered into force.

"Insurance data" is defined as:

• Data relating to insurance contracts, insurers and insurance companies who are parties to the insurance contract, the insured, beneficiaries and other third parties who directly or indirectly benefit from the insurance contract.

• All data based on risk assessment, including false insurance practices.

In this context, data that is not defined as "personal data" under the DP Law is also included within the scope of insurance data.

MOROĞLU ARSEVEN

MOROĞLU ARSEVEN

Insurance data will be collected and kept in the general database of the Insurance Information and Surveillance Centre ("ISC Centre") and institutions and organizations will be obliged to provide the data requested by the ISC.

In light of these developments, the important details of the Insurance Regulation are as follows:

• The ISC Centre will determine the authorized users who are granted access to the data in the general database and the content of the data they can access. Access to the system by authorized users who violate the rules for access will be restricted, with the approval of the IPPRSA and based on a decision by the ISC Centre.

• The ISC Centre can make policy and claim data that is related to insurance contracts available to data subject, where deemed appropriate by the IPPRSA, provided the necessary authentication or ownership is shown.

• Data subjects can request information from the ISC Centre about their own data in the general database, except for data on insurance malpractices.

• Insurance data can be used for the purposes of contributing to public supervision and control and economic security in the insurance sector, and for planning the financing of health services, monitoring insurance practices, ensuring unity of practice in insurance branches, monitoring compulsory insurance, contributing to the prevention of incorrect insurance practices, conducting studies to increase insurance rates, ensuring the production of reliable statistics on the insurance sector, and the calculation of insurance scores.

• Relevant institutions and organizations will be obliged to submit data requested by the ISC Centre accurately, consistently, completely and without delay, and must create the necessary infrastructure to share this data.

• Where the explicit consent or approval of the data subject must be sought regarding the data contained and shared in the general database, the institutions and organizations exchanging the data are responsible for obtaining explicit consent or approval from the data subject and for the fulfilment of the obligation to inform.

• The ISC Centre can only publish obtained data after anonymizing it.

The ISC Centre will use the data in the general database to:

• Associate current production, damage and compensation data received from relevant institutions and organizations with the data in the general database for the purpose of monitoring and determining compulsory insurances, in cooperation with the relevant institutions and organizations within the scope of the relevant legislation. This will include data on motorized vehicle operators and drivers.

• Create a database where information on accident investigation reports is kept.

• Keep data on third-party liability insurance agreements for foreign-registered vehicles entering the country and for motorized vehicles registered in Turkey leaving the country.

• Share past data regarding health and diseases with relevant institutions and organizations in order to preserve economic security in insurance risk assessment processes and to facilitate the planning of health services' financing, establishing an offsetting platform for the mutual recourse receivables.

3. Circular No 2022/1 on Sharing Secret Information under Banking Regulation

The Banking Regulation and Supervision Agency ("**BRSA**") has published Additional Explanations Regarding the Implementation of the Regulation on Sharing Secret Information under Banking Regulation , dated 11 August 2022, No 10295 ("**Circular**"), in order to eliminate certain practical difficulties in relation to banking secrecy.

The Circular sets out concepts, procedures and principles regarding the sharing of customer and bank confidential information. It imposes an obligation to report to the BRSA when information is shared by banks with a parent company, clarifies the scope of legitimate information sharing by banks, and addresses issues such as data being transferred abroad.

Under Article 73/3 of the Banking Law No 5411 ("**Banking Law**"), a "customer secrecy" consists of data specific to banking activities generated after the establishment of a customer relationship with the bank. However, even if no customer relationship has been established, obtaining, and learning confidential customer information held by another bank is also within the scope of the confidentiality obligation. In addition, such data relating to legal entities (which is not defined as "**personal data**" under the DP Law) will also be a customer secret.

Secret information regarding the bank's activities and management principles is considered to be a "bank secret" and cannot be disclosed to anyone other than the parties authorized by law, except for in the exceptional circumstances listed in the Regulation.

For the sharing of bank and customer confidences not to constitute a breach of the confidentiality obligation, either (i) a confidentiality agreement must be concluded between the parties or (ii) the sharing of such confidential information must be limited only to that necessary for specified purposes. Such disclosures are expected to comply with the principle of proportionality.

Being a joint customer (which is mandatory condition for the open disclosure of confidential customer information between banks) is not required for disclosures made under Articles 5/2(b) and 5/3 of the Regulation in the following cases:

• Disclosures that require sharing broad data on a large number of customers, such as loan provision calculations and internal capital adequacy calculations, provided the BRSA's consent has been obtained before disclosure.

• Disclosures to be made for counterparty compliance risk purposes, provided the BRSA's consent is obtained before the disclosure.

• Disclosures to be made for consolidated risk management purposes that include data on a natural or legal person or a risk group to which a loan of 10% or more of the bank's main capital has been granted. There is no requirement to obtain the BRSA's consent before such disclosures.

The Circular also sets out other exceptions to the obligation to keep secrets, including the following:

• Information that is not a customer secret and that only contains information belonging to the bank can be shared with third parties under the responsibility of the bank and with a decision of its board of directors.

• Customer secret information provided by the customer to a public institution or organization for the execution of any transaction can be shared by banks, Risk Centre or companies established by at least five banks or financial institutions, for confirmation regarding the accuracy of this information, provided the customer's request or instruction to do this has been received.

• Where it is necessary to prove claims or defences in disputes to which the bank is a party, information regarding relevant customer secrets or bank secrets can be shared with authorized institutions and persons.

Secret customer information cannot be shared with domestic and foreign third parties without a specific request or instruction from the customer, even if the customer's explicit general consent is obtained. The customer's explicit consent or request or instruction to share information cannot be made a precondition for the services to be provided by the bank. However, the exceptional circumstances are considered to be exceptions to this.

4. Circular No 2022/18 Regarding the State Organization Central Registration System

Circular No 2022/18 ("SOCRS Circular") regarding the State Organization Central Registration System ("SOCRS" also known as DETSİS in Turkish) was published in the Official Gazette dated 3 December 2022, No 32032. The SOCRS Circular transformed the previous State Organization Database for the centralized and electronic recording of data on the organizational structures of public institutions and organizations into the SOCRS.

Under the SOCRS Circular, public institutions and agencies must register all units in their structure in the SOCRS and ensure their registration is up to date. Institutions and agencies must update the SOCRS with changes in their structure within five working days.

MOROĞLU ARSEVEN

III. Guidelines Published by the Board in 2022

Guidelines published by the Board in 2022 are listed below in chronological order.

1. Guidelines for Good Practice for the Banking Sector Regarding Protection of Personal Data

The Guidelines for Good Practice for the Banking Sector Regarding Protection of Personal Data ("Banking Guidelines") were published on the Institution's website on 5 August 2022. The Banking Guidelines create good practice examples for banks that process personal data. This includes comprehensive good practice examples and explanations regarding relations between data controllers and data processors in the banking sector, personal data processing conditions that are specific to the banking sector, the transfer of personal data, general principles, and data controllers' obligations. The Banking Guidelines also set out guidance for banks that are data controllers to ensure their activities are in compliance with the DP law and the secondary legislation created by the Board. In addition, the Banking Guidelines give indications as to the Board's approach when evaluating a complaint or an alleged violation.

Under the Banking Guidelines, banks will generally be either data controllers or data processors in relation to their personal data processing activities, and banks will be data controllers in relation to their banking activities under Article 4 of the Banking Law No 5411. However, the characteristics of the specific case must be examined when evaluating whether a bank is data controller or a data processor in relation to certain other activities such as being an insurance agent or intermediary, or the provision of services such as individual retirement investment products or fast international money transfers. The Banking Guidelines provide for joint data responsibility, and the contract between the parties is important when determining the obligations among joint data controllers.

According to the Banking Guidelines, data processing activities that do not require explicit consent include the following:

• The transfer of the bank's customers' personal data to the BRSA.

• Providing authorized institutions with information.

• Processing personal data and transferring information within the scope of the legislation on money laundering.

• Searching criminal records in accordance with the Check Legislation.

The Banking Guidelines set out explanations in relation to the following:

• Ensuring transaction safety and taking the necessary precautions when unusual banking transactions and behaviours are detected.

• Evaluating customer data to determine the level of service to which the customer is subject and to understand the customers relationship with the bank and the usage of its products and channels by customers.

• Fulfilling the customer's needs correctly and providing the customer with appropriate products and services to ensure customer satisfaction with the efficient use of the bank's financial resources.

• The execution of strategy investigations.

• Customer satisfaction being evaluated within the scope of legitimate interests and the requirement for explicit consent.

There are also important assessments in relation to the transfer of data. Based on Article 73 of the Banking Law, the Banking Guidelines state that data can be transferred to the bank's main partner/subsidiaries, prospective buyers, banks and financial institutions, the Risk Centre, Interbank Card Centre and Credit Registration Bureau, their affiliates and valuation, rating and support service institutions within the limits set out in Article 73.

Finally, there are explanations regarding the obligations of the data controller and the fulfilment of these obligations.

2. Guideline on Cookies

On 20 June 2022, the Guideline on Cookies ("Cookie Guideline") was published on the Authority's website. For the purpose of creating a guidance document, the Authority had previously published a draft guide on 11 January 2022 in the form of recommendations to data controllers processing personal data via cookies. The Cookie Guideline was published on 20 June 2022 in line with the opinions received.

The Cookie Guideline covers data processing via cookies. Cookies that are not used for the processing of personal data are outside its scope. There is no guidance regarding similar technologies such as pixels, user fingerprints, local storage or beacons. The Cookie Guideline is also applicable to desktop and mobile websites or web applications.

The Cookie Guideline provides guidance on the following:

- The definition of cookies and the different types of cookies.

- The relationship between the Regulation of Electronic Communication and the DP Law.

- Important rules regarding cookies, including scenarios of cookie usage within other processing conditions other than explicit consent, and scenarios of cookie usage with the requirement of explicit consent (see below).

- The elements of explicit consent that must be lawfully obtained.

- Transfers of personal data abroad.

- Appropriate methods of informing data subjects.

- The Board's explanations regarding its decision dated 27 February 2020, No 2020/173.

Explicit consent is generally required for the application of cookies, including those that are not used for data processing within the scope of Article 5 of the DP Law. In addition, the application of cookies must always comply with the principles in Article 4 of the DP Law. Nevertheless, certain cookies with a user input do not require explicit consent. The Cookie Guide gives the following as examples of these:

- Cookies for creating a user shopping basket.

- Authentication cookies that are used to identify the user when they log onto a website.

- User-centric security cookies that are used to increase security within a service that is expressly requested by the user.

- Multimedia player session cookies that are used to store technical data needed for video playback or audio content.

- Load-balancing cookies that allow for the distribution of the web server requests over a pool of machines rather than a single machine.

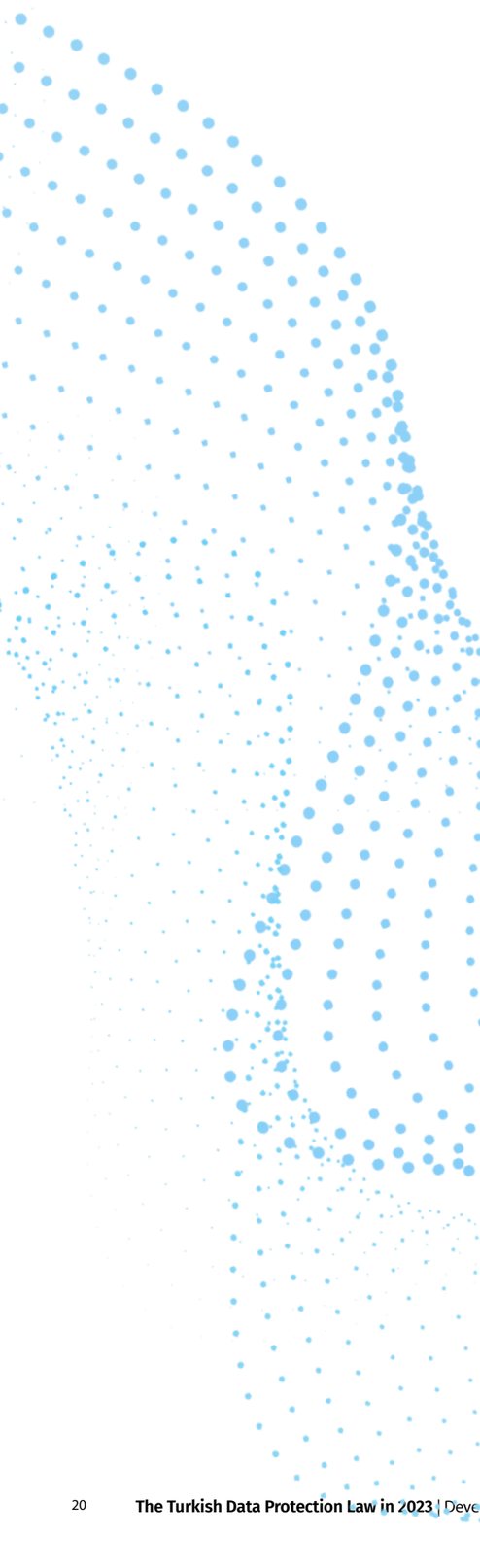
- User interface customization cookies and social plug-in content sharing ("like, share, comment") cookies that are used to store the user's preferences for a service on web pages.

- Cookies that are used for the explicit consent management platform.

- First-party analytics cookies.

- Cookies used for the security of the website.

However, social plug-in tracking cookies and online behavioural advertising cookies, which can be used to track members/non-members with the help of third-party cookies for additional purposes such as behavioural advertising, analytics or market research are types of cookies that require explicit consent.



3. Misconceptions About the DP Law Guideline 2

The Board published the Misconceptions About the DP Law Guideline 2 (Second Guideline) on its official website on 3 January 2022.

Certain matters regarding the first guideline and the legislation are explained in the Second Guideline and there are also significant changes in relation the Board's stance and ideas.

According to Question 14, the processing of data such as voice recordings, images and photographs cannot be directly qualified as biometric data processing. However, such personal data is regarded as biometric data when it is processed in a specific technical way that allows for the unique identification or verification of the person. Therefore, for data to be biometric data, that data must have the ability to identify or verify that person.

According to Question 17, the use of pseudonyms is not a method that anonymizes personal data and terminates the status of data as personal data. However, it is a method that helps to minimize data security risks related to personal data. Since the personal data related to the use of pseudonyms is not anonymized, it has the properties of personal data and is subject to the DP Law.

According to Question 19, where there is reliance on processing conditions other than explicit consent or a letter of undertaking approved by the Board, a transfer of data abroad must take place to a country that is approved by the Board as offering sufficient protection in relation to the personal data.

According to Question 22, keeping personal data on a cloud data service will be regarded as a transfer activity, even if the cloud service provider cannot access the data.

4. Procedures and Principles Regarding Certificates of Participation

The Procedures and Principles Regarding Certificates of Participation ("PPCP") were determined by the Board of Personal Data Protection's decision dated 23 December 2021, No 2021/1296, and were published on the Board's website on 11 February 2022. The PPCP have been in force since publication.

The PPCP set out the procedures and principles for issuing a certificate of participation under the Communiqué on Procedures and Principles Regarding Personnel Certification Mechanisms.

The scope of the PPCP includes regulations on basic training, the obligations of educational institutions, basic training principles, examining and documentation, and exceptions.

IV. Draft Guidelines

1.Draft Guideline on the Investigation of Loyalty Programmes under the Personal Data Protection Legislation

The Authority made the Draft Guideline for the Investigation of Loyalty Programmes under the Protection of Personal Data Legislation ("**Loyalty Programmes Guideline**") available to the public on 16 June 2022. The Loyalty Programmes Guideline sets out pseudonymous examples of loyalty programmes implemented in Turkey, and examples and explanations of the relevant practices regarding the processing of personal data.

The Loyalty Programmes Guideline applies to all data controllers, data processors, data subjects, processed personal data, processing conditions and data processing activities falling within the scope of loyalty programmes. The Loyalty Programmes Guideline gives guidance in relation to legal compliance, the requirement for explicit consent, the evaluation of data processing activities in terms of general principles, the obligation to inform, and issues related to data security.

Loyalty programmes under The Loyalty Programmes Guideline are defined as strategies that when applied by the companies unilaterally or via a partnership programme, provide benefits to customers while also improving the company's sales and profits. These may include providing the customer with points/gifts/advantages for shopping in return for processing customer's personal data in a way that enables the customer to be identifiable, the following of the customers shopping habits, or providing customized products or service offers through the processing of personal data.

According to The Loyalty Programmes Guideline , explicit consent is not required for personal data (for example, name and contact information) processing that pertains to the establishment and execution of a contract, including for instance when a loyalty programme is offered under a contract. However, this does not apply to a company processing data by profiling customers who take part in a loyalty programme, since the profiling of customers does not directly correlate with the establishment or execution of the contract, and therefore forms a new data processing process.

On a sale, a request from the data controller for explicit consent from the consumer for data processing in order to participate in a loyalty programme will not be evaluated as making the provision of the specific product/service subject to consent to data processing, and is therefore lawful. If explicit consent is not given to data processing, the specific product/service can still be provided, but must be offered without the additional benefit to the consumer of the loyalty programme.

Where explicit consent is given to the processing of personal data and becoming a member of the loyalty programme, the product/service can be supplied along with the provision to the customer of the additional benefits. However, to ensure that the explicit consent to data processing under loyalty programme is not offered as a condition of service, the discount or advantage under the programme must not create so significant a disadvantage to other customers as to affect the customers' free choice.

The Loyalty Programmes Guideline also includes the following recommendations:

• Correctly determining the legitimate legal purpose of the processing of personal data under loyalty programmes (for example, processing of phone numbers for the purpose of making the person identifiable, and processing for the purpose of sending commercial electronic messages, require different reasons to be legally compliant).

• Providing the data subject with the privacy notice and obtaining an explicit consent.

• Not obtaining general consents for processes that require explicit consent.

• Not seeking additional explicit consent where personal data is processed within the scope of the reasons for legal compliance set out in paragraph 2 of Article 5 of the DP Law.

• Not placing explicit consent declarations and clarification texts within the provisions of the contract.

• Ensuring information is clear and understandable, and making clear and unambiguous explanations regarding the transfer of personal data.

• Acting in accordance with the principle of proportionality and the general principles of the DP Law, especially for the purpose of processing.

• Ensuring that the advantage provided by the loyalty programme is reasonable and that the customer would not otherwise suffer a significant disadvantage, so that explicit consent is not a condition of the provision of goods/services offered within the scope of the loyalty programme.

• Obtaining separately and individually the necessary permissions/approvals/consents to send commercial electronic messages to the data subject within the scope of the loyalty programme.

• Fulfilment of data security obligations in relation to personal data processed within the scope of loyalty programmes.

MOROĞLU ARSEVEN

2. Draft Guideline on the Matters to Be Considered Regarding the Processing of Genetic Data

On 24 August 2022 the Draft Guideline on Matters to be Considered Regarding the Processing of Genetic Data ("**Genetic Data Draft Guideline**") aims to regulate the analysis of genetic data for medical diagnosis and treatment, the treatment of prenatal or postnatal diseases, and the analysis of parental and descendant lineage. This data may be processed by hospitals and medical laboratories, or for commercial purposes, such as in the determination of paternity or to execute other legal processes. In addition to cases of medical necessity, genetic data processing may also be carried out for purposes such as in relation to nutrition or genetic predisposition to sports or other talents, depending on the request of data subject.

Article 6/3 of the DP Law stipulates that personal data other than that relating to health and sexual life can be processed without seeking the explicit consent of the data subject in certain circumstances stipulated by the law. Therefore, genetic data can also be processed in these cases without requiring explicit consent. However, data processors must comply with the general principles listed in Article 4 of the DP Law when processing these kinds of data (see below). Therefore, Article 4 of the DP Law applies regardless of whether personal data processing is based on the explicit consent of the data subjects or is based on the legally stipulated personal data processing conditions. In addition, various measures must be taken in relation to the transfer of genetic data abroad, in consideration of the fundamental rights and freedoms of individuals.

The procedures and principles regarding the licensing, opening, operation and inspection of Genetic Diseases Evaluation Centres, which are used for the purpose of diagnosis and treatment of genetic diseases, are also regulated. All organizations operating in this field are subject to the regulations, including real or legal persons (including Ministry, university, private law legal entities, and so on) who are data controllers by virtue of determining the purposes and means of the processing personal data and being connected to and responsible for its establishment and management. Data processors are natural or legal persons who process personal data on behalf of a data controller under the data controller's authority. Therefore, operators of cloud systems where genetic data is kept can also be considered to be data processors.

A "data subject" is defined as a natural person whose personal data is processed. "Personal data" is defined as any information relating to an identified or identifiable real person. Therefore, certain genetic data processing processes may process the data of the data subject as well as that of their genetic relatives.

A data controller can only process genetic data in accordance with the general principles set out in Article 4 of the DP Law and the conditions stipulated in Article 6. These principles are:

• Not breaching the essence of fundamental rights and freedoms.

• For the data processing activity to be appropriate for the purpose of data processing.

• For the genetic data processing method to be necessary for the purpose.

• For the goal and the means to achieve the goal to be proportional.

• Keeping the processed genetic data for the required period of time only.

• Destroying the data without delay in accordance with the personal data retention and destruction policy after the necessity disappears.

There are specific criteria to be complied with where genetic data is processed for scientific purposes under the scope of Article 28 f/1-c of the DP Law. For example, in cumulative variant frequency systems, collective studies must be carried out without making individuals identifiable. Although it is possible to use genetic data for scientific purposes (except in specific cases stipulated in the law) this should be a last resort only used in cases where it is necessary to reach the result. To ensure that the right to protection of personal data under the Turkish Constitution is not breached, the data processor must provide the necessary security measures and act in accordance with the principles of the data being connected, limited and proportional to the purpose for which it is processed. For completed scientific research, if it is not necessary to retain the data, the data must be destroyed accordance with the personal data retention and destruction policy.

The primary technical measure that must be taken to ensure the security of genetic data is to not keep the genetic data in cloud systems. However, where it is necessary to connect the data to an analysis program server for processing, a detailed record of the genetic data stored in the cloud should be kept, backups should be stored outside the cloud, and two-stage authentication should be applied for remote access to the genetic data in the cloud. The processed and stored genetic data must be encrypted in accordance with the current technology, with cryptographic methods that provide adequate security. Applications, devices, and systems that use the algorithms included in the standardized and secure cryptographic algorithm suite must be used. Industry standards and best practices for standardized and secure cryptographic algorithms must be considered. If it is necessary to use cryptographic algorithms that are not included in the standardized cryptographic algorithm suite, an analysis and evaluation of whether they provide adequate security must be carried out by an authorized crypto analysis laboratory before use. The encryption and key management policies must be clearly defined. Access to cryptographic keys must be restricted to authorized personnel with clearance (in the form of a crypto security certificate). Where possible, individual encryption keys should be used specifically for each cloud service solution.

If devices are delivered to other companies for repair or similar purposes, the data on them should be erased, and a written undertaking should be obtained stating that there is no data in the device.

The Genetic Data Draft Guideline also regulates the administrative measures that must be taken by data controllers processing genetic data. These include the following:

• Establishment and management of data processing mechanisms on the basis of "Privacy Based Design".

• Implementation of a "Data Protection Impact Assessment" regarding the quality of data and possible risks that data processing may pose for the data subject.

• Storing genetic data in a way that is inaccessible to anyone other than authorized, trained and confidential personnel.

• Preparing a personal data processing inventory and notifying the Data Controllers Registry Information System (VERBİS).

• Creating separate processing policies, emergency procedures and reporting mechanisms regarding genetic data processing processes.

MOROĞLU ARSEVEN

• Regularly backing up genetic data in the electronic environment.

• Informing the persons whose data will be processed in accordance with the DP Law.

• Obtaining consent and using the data only in accordance with the consent given.

• Having internal random and periodic audits and risk analyses regarding genetic data processing activities.

• The data controller constantly measuring their readiness for a possible data breach.

• Necessary security measures being included in service contracts with data processors.

• Audits to be carried out periodically on whether the necessary technical and administrative measures are provided by the data processor.

The processing of genetic data is sensitive and may imply national strategic issues that affect society. Therefore, it is necessary to bind the processing of genetic data to certain rules and procedures, as well as to raise awareness in society, as the processing of the genetic data of the data subject might affect not only themselves, but also their relatives, future generations and even the national security and economy. This can be seen, for example, in the emerging economic sector known as "biotechnology" or "bioeconomics", which has received government support in many countries as a developing strategic sector. Increasing efficiency in economic output, especially in fields such as health, agriculture and bioenergy, through the use of genetic data as an economic input is regarded as a high priority economic and national security issue. It is therefore necessary to prepare against data breach risks that a sector with high innovation capacity and R&D studies involving other genetic data processing activities may be exposed to, and it is essential to take some national security measures in this regard.

In this regard, in Turkey, the Presidency's Digital Transformation Office published the Information and Communication Security Guide in July 2020 within the framework of national and international standards and information security criteria, in order to ensure the security of critical data that could lead to disruption of the public order. In addition, the Presidential Circular No 2019/12 on Information and Communication Security Measures published in the Official Gazette dated 6 July 2019, No 30823 states that "Critical data such as population, health and communication record information, genetic and biometric data will be stored safely in the country".

Similarly, the National Cyber Security Strategy and Action Plan (2020-2023) published in the Official Gazette on 29 December 2020, No 31349 and the Presidency Circular No 2020/15 have also entered into force, and set out measures to be taken nationally by the Board, including the following:

• Further consideration of the procedures and rules relating to the purposes of processing genetic data. For example, paragraph (2), Article 25 entitled "Transport of Samples" of the Regulation on Genetic Diseases Evaluation grants the relevant licensed Genetic Diseases Evaluation Centre the authority to send samples abroad for examination purposes, while biological samples of human origin must be recorded in the Ministry's tracking system for the purpose of examination. It is currently unclear as to whether the data processing of a sample in the Ministry's tracking system falls under Article 9 of the DP Law (and is a data processing activity subject to the requirement of being proportionate or necessary within the framework of the general data processing principles and Article 4 of the DP Law), or whether it falls under the scope of a scientific activity.

• Where it is necessary to conduct tests or research on genetic data abroad (under the International Declaration on Human Genetic Data of the UNESCO General Conference dated 16 October 2003), ensuring the privacy of genetic data processed for scientific research or investigation purposes, and taking necessary measures to prevent its use for purposes other than the reason for which it was collected.

• Supporting national laboratories to supply necessary domestically produced medical devices and strengthening specialized human resources to prevent as much as possible genetic data tests from being sent abroad.

• Supporting local, national and accredited informatics infrastructure by making the necessary administrative arrangements so that it is possible to store genetic data domestically.

• Encouraging the establishment of genetic data storage centres to be used for scientific purposes, by developing national genetic data banking.

• Promoting the development of transparency, openness and accountability practices and thereby ensuring that society is informed about the reasons and consequences of genetic data processing performed by Authoritys carrying out research and studies in this field.

• Organizations that carry out research or testing activities that require the processing of genetic data are to have a "Patient Rights Unit" including personnel who have received the necessary training in the field of personal data protection. This will act to inform the relevant people about where and how obtained personal data will be used and will answer the relevant queries.

• Informing the data subjects about the consequences of sending their genetic data abroad, increasing social awareness through methods such as public service announcements and meetings (thereby reducing the number of people sending their genetic data abroad), and conducting awareness-raising activities for health care professionals in order to adequately inform the relevant people and prevent tests that can already be performed domestically from being carried out abroad.

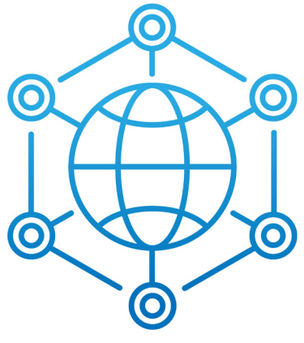
V. Public Announcements Made by the Board in 2022

In 2022, the Board published 4 public announcements on security measures, data transfers abroad and the obligation to notify VERBİS. Although these public announcements are not legally binding, they are important in terms of showing the Board's legal assessment, evaluation and approach regarding these issues.

The published public announcements are listed below in chronological order.

1.Data Transfer Abroad via Undertaking

According to a public announcement published on 18 January 2021, the Turkish Football Federation has been evaluated by the Board under subparagraph (b) of paragraph 2 of Article 9 of the DP Law in relation to an application by the data controller to transfer personal data abroad with an undertaking, which the Board has approved.



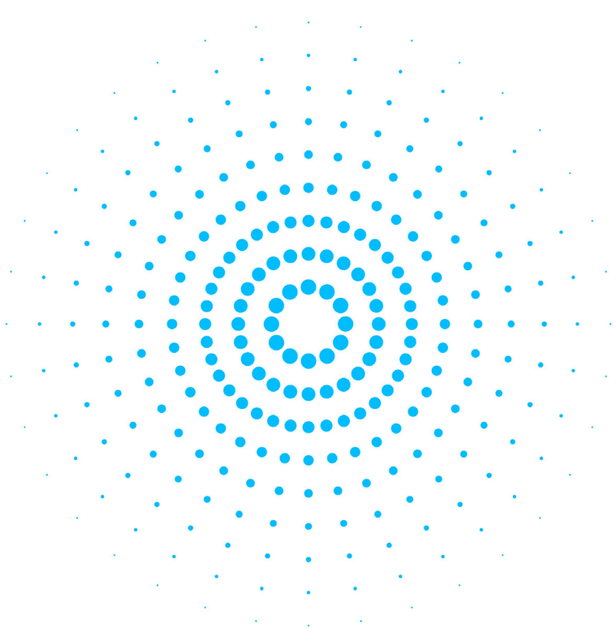
2. Obligation to Notify VERBİS

On 4 January 2022, a public announcement was published on the official website of the Board on issues that were deemed necessary to re-state in relation to the obligation to register with VERBİS. These included the following:

• Simply entering the VERBİS registration application form into the system or sending it to the VERBİS by mail, cargo, courier, REM (Registered Electronic Mail) or hand-delivery does not mean that the registration and notification obligation has been fulfilled. For the registration and notification obligation to be fulfilled, the VERBİS registration application must be sent to the Authority by mail, courier, courier, REM or by hand delivery and be approved by the Authority. It is then further necessary to log into the Data Controller Login page in the VERBİS system ("VERBIS") with the username and password sent to the e-mail address specified in the application form, and then appoint a "contact person". The appointed contact person must also then log in via the "Register to the Registry" button on the VERBİS main page, and a "notification" must be issued for the relevant data controller. The notification must then be approved on the system.

• VERBİS is open to access for application and statement arrangements, and it is currently possible to submit applications and issue statements through the system. Therefore, it is important to complete missing applications and notifications as soon as possible. In addition, as "Data controllers notify the Authority via VERBİS, in case of a change in the information registered in the Registry, within seven days from the date of the change", it is possible to make a "statement update" by logging in via VERBİS.

• The obligation to register with VERBİS is in addition to the further obligations that data controllers must comply with under the DP Law and secondary legislation.



3. Public Announcement on Technical and Administrative Measures Recommended to be Taken by Data Controllers Regarding User Security

The Board published the Public Announcement on Technical and Administrative Measures Recommended to be Taken by Data Controllers Regarding User Security ("Security Announcement") on its official website on 15 February 2022.

The Security Announcement evaluates breaches of personal data statements that have recently been submitted to the Board. It observes that user account information (username and passwords) used to log in to the websites of data controllers operating in various sectors such as finance, e-commerce, social media and gaming have been publicly published on some websites. It also observes that third parties have actively accessed the websites of data controllers who have obtained user accounts, without the knowledge of the users, and viewed the data of the relevant persons.

In addition, it observes that personal data obtained from the systems of data controllers or by using security vulnerabilities in end-user computers have been illegally shared and offered for sale for an economic value. The data belonging to the relevant persons may be circulated, archived by malicious people, and re-marketed as larger data sets.

Considering these issues, the Security Announcement recommends that data controllers take the following security measures:

• Establishing two-factor authentication systems and providing them to users as an alternative security measure from the membership application stage.

• In cases of logins from devices other than devices that provide frequent access to the users' accounts, the login information must be sent via e-mail/SMS to the relevant person's contact accounts.

• Protecting applications with HTTPS (Hypertext Transfer Protocol Secure) or in a way that provides the same level of security.

• Using secure and up-to-date hashing algorithms to protect user passwords against cyber-attack methods.

• Limiting the number of unsuccessful logins attempts from an IP (Internet Protocol Address) address.

• Ensuring that the relevant persons can view information about at least the last five successful and unsuccessful login attempts.

• Reminding the relevant persons that the same password should not be used on more than one platform.

• Establishing a password policy by data controllers, ensuring that users' passwords are changed periodically and reminding the relevant persons to change their password.

• Preventing newly created passwords from being the same as old passwords (at least the last three passwords), using technologies such as security codes (CAPTCHA, four processes, and so on) that distinguish between computer and human behaviour when logging into user accounts.

• Limiting the IP addresses that are allowed to access the relevant account.

• Ensuring that passwords are strong by making sure they are at least 10 characters in length, and requiring at least one upper case, one lower case, one number and one specialized character.

• If third-party software or services are used to log into the systems of data controllers, ensuring that there are regular security updates of these software services.

• Performing necessary security checks.

4. VERBİS Registration Obligation

On 21 April 2022, a public announcement regarding the VERBİS registration obligation was published on the official website of the Board. The announcement states that administrative sanctions can be imposed by the Board on data controllers that fail to fulfil their obligation to properly register with and notify the VERBİS. Article 18/1 of the DP Law imposes an administrative fine from 20,000 Turkish Lira to 1 million Turkish Lira for violations of the obligation to register and notify stipulated in Article 16. If these actions are committed within public Authoritys and organizations and professional organizations in the nature of public Authoritys, on notification by the Board, disciplinary action will be taken against the relevant individual civil servants, public officials or workers in professional organizations in the nature of public Authoritys. The result of these actions must be reported to the Board.

In this context, administrative sanctions have begun to be imposed on data controllers who are found to have not fulfilled their VERBİS registration and notification obligations, in accordance with Article 18 of the DP Law.

VI. Constitutional Court Decision of 2022

The Constitutional Court has decided that an applicant's right to protection of personal data was violated due to the failure by the state to conduct an investigation regarding the unlawful recording of a non-public conversation in accordance with the state's positive obligations.

In the incident subject to the decision, the applicant's voice recordings regarding a debt relationship were obtained in a non-public environment and the voice recording was placed as evidence in a criminal file in which the applicant was a suspect. The applicant filed a complaint with the Chief Public Prosecutor's Office against the person who had made the audio recording. The Chief Public Prosecutor's Office concluded that the person who had made the audio recording did not intend to commit a crime, but acted with the motive of providing evidence of crimes allegedly committed by the applicant.

The Constitutional Court found that "the recording of the applicant's conversations with other people in a non-public environment based on his justified expectation that his privacy would be protected and the use of the audio content in question, against his consent, constitutes an attack on his personal data within the scope of his private life and that the effects of the attack on the aforementioned legal values are severe". According to the Constitutional Court, as no proportionality assessment was made, no effort was made to balance the conflicting interests in a fair manner, the applicant's requests to determine whether there were any cuts or additions in the audio recording were not met, and information from other persons mentioned in the allegation to the effect that the audio recording was made in a planned manner was not applied, showed that the applicant did not adequately benefit from procedural guarantees. With this decision, the Constitutional Court has shown that the recording of non-public conversations for the purpose of using them as evidence cannot be accepted as lawful in every case, and that a conclusion must be reached by observing the principle of proportionality and fairly balancing the conflicting interests.

MOROĞLU ARSEVEN

B. STRUCTURE AND SUPERVISORY ACTIVITIES OF THE BOARD AND AUTHORITY

The Turkish Data Protection Law in 2023 | Developments in Practice Over its Seven Years

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 eight members of the Board and seven presidential units, apart from the President of the Authority, the Vice President of the Board, and the President of the Board.

Following the election held at the 3rd Meeting of the General Assembly on 5 October 2022, İsmail Aydın and Recep Keskin were elected for the two vacant seats on the Board.

The Current Structure	
Head of Authority	Prof. Dr. Faruk BİLİR
Board Member	Hasan AYDIN
Board Member	İsmail 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

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 announced on its official website that it held a total of 188 seminars, workshops, training, and events in 2022, including Wednesday Seminars. These include the:

- 44th Global Privacy Assembly Conference
- 28 January Personal Data Protection Day Event
- Metaverse in the Digital World
- Relation between Online Behavioural Advertising and Personal Data Protection Law
- Personal Data Protection Law: A View from Today to the Future
- Workshop on Personal Data and Audit Practices in the Digital World
- Workshop on Evaluation of the Implementation of Guidelines for Good Practice for the Banking Sector Regarding Protection of Personal Data
- 5th E-Safe Personal Data Protection Summit
- Data Science Summit
- 2nd Personal Data Protection Conference

The Board published an annual report for the first time in 2018 and continued this practice for 2019, 2020 and 2021. The Board published its annual report on the activities carried out in 2022 as of 12 April 2022, and the statistical data included in the activity report under II below have been updated as per the year 2022. In this regard, a total of 60 data breach notifications and 9,059 complaint applications were carried out; 75 commitments were submitted, of which 30 are still under review, 5 were undertaking approval and 40 were not undertaking approval. Within the guideline, the publications on the official website of the Board in 2022, were considered a total of 118 published summary decision.

II. Overview of the Board's Supervisory Activities Shared with the Public in 2022'

1. Data Breach Notifications and the Board's approach

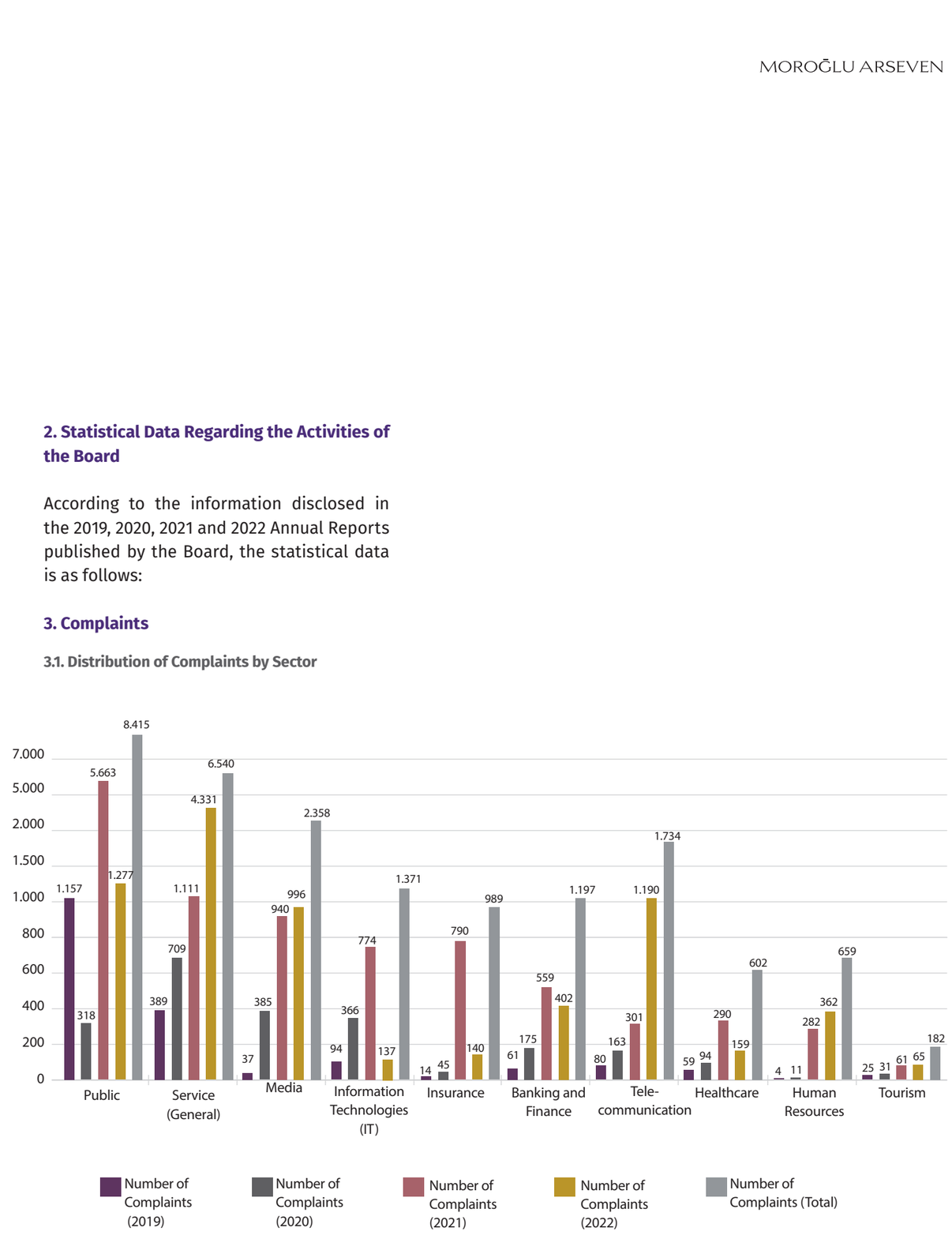
In 2022, a total number of 260 data breach notifications were submitted to the Authority; while 104 of these were concluded and 54 were published on its official website by the Authority.

2. Statistical Data Regarding the Activities of the Board

According to the information disclosed in the 2019, 2020, 2021 and 2022 Annual Reports published by the Board, the statistical data is as follows:

3. Complaints

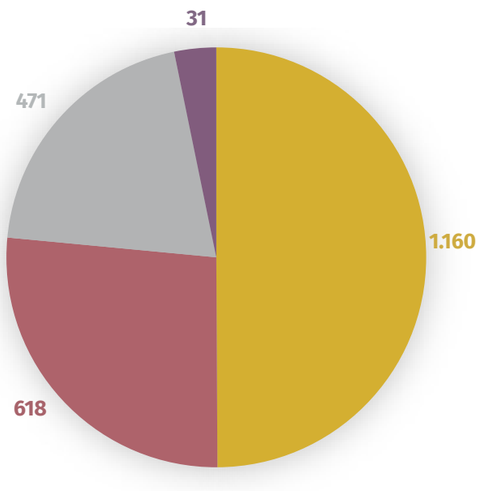
3.1. Distribution of Complaints by Sector



[1] Details regarding the summaries of the decisions, data breach notifications and public announcements published by the Authority on its official website in 2022 will be included in our fourth issue, and this third updated issue contains only statistical data on complaints, notifications, and administrative sanctions for the year of 2022.

3.2. Distribution of Complaints by Subject

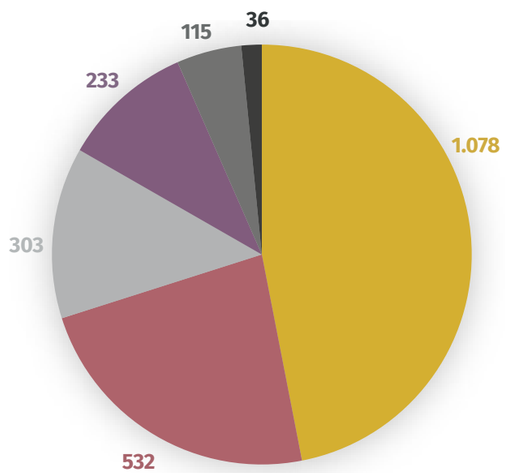
Distribution of Complaints in 2019[2]



SUM : 2280

- Complaints of citizens living abroad about sharing of their personal data with the authorities of the country they live in.
- Unlawful sharing of personal data with third parties by the data controller.
- Unlawful processing of personal data by the data controller.
- Failure of the data controller to fulfil the requests of the data subject.

Distribution of Complaints in 2020[3]

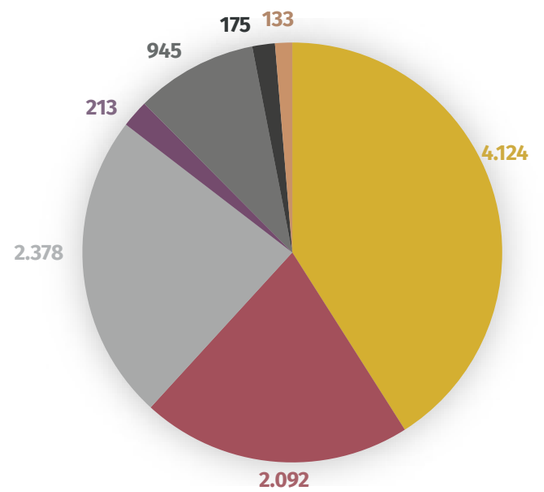


SUM : 2297

- Unlawful sharing of personal data with third parties by the data controller.
- Unlawful processing of personal data by the data controller.
- Deletion, destruction and anonymization of data by the data controller.
- SMS/Call without permission.
- Failure of the data controller to fulfil the requests of the data subject.
- Failure to fulfil the obligation to inform.

[2]Taken from the annual report published by the Board.
[3] Taken from the annual report published by the Board.

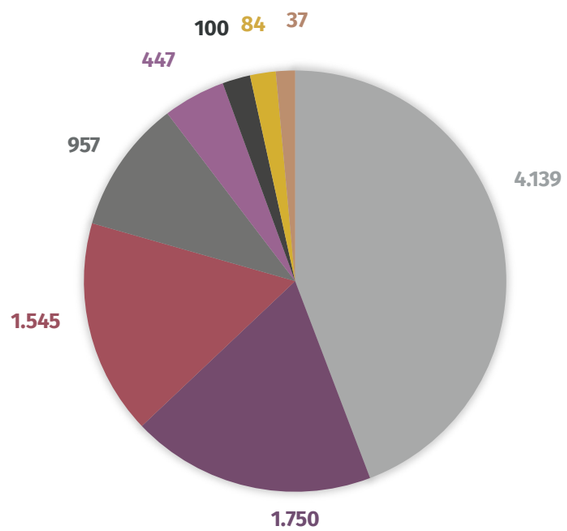
Distribution of Complaints in 2021[4]



SUM : 10,060

- Requests for not to transfer personal data abroad.
- Unlawful sharing of personal data with third parties by the data controller.
- Unlawful processing of personal data by the data controller.
- Deletion, destruction and anonymization of data by the data controller.
- Failure of the data controller to fulfil the requests of the data subject.
- Claims under the right to be forgotten.
- Failure to fulfil the obligation to inform.

Distribution of Complaints in 2022 [5]

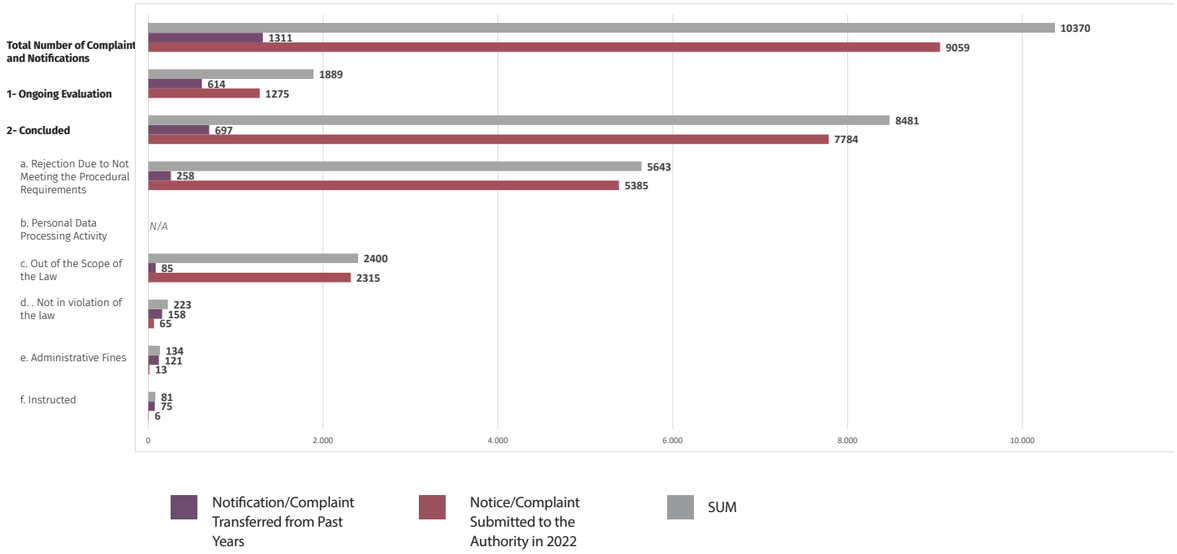


SUM: 9,059

- Requests for not to transfer personal data abroad.
- Unlawful sharing of personal data with third parties by the data controller.
- Unlawful processing of personal data by the data controller.
- Unauthorised SMS/Call
- Failure of the data controller to fulfil the requests of the data subject.
- Claims under the right to be forgotten.
- Deletion, destruction and anonymization of data by the data controller.
- Failure to fulfil the obligation to inform.

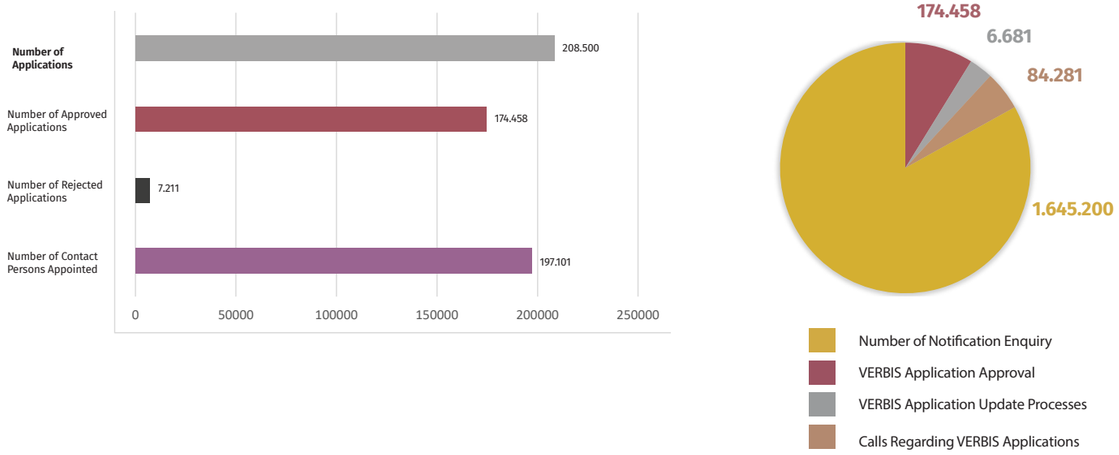
[4] Taken from the annual report published by the Board.
[5] Taken from the annual report published by the Board.

3.3. Number of Complaints and Notifications[6]



3.4. Number of Registrations and Applications to VERBIS and Numerical Status of Activities Realised through VERBIS [7]

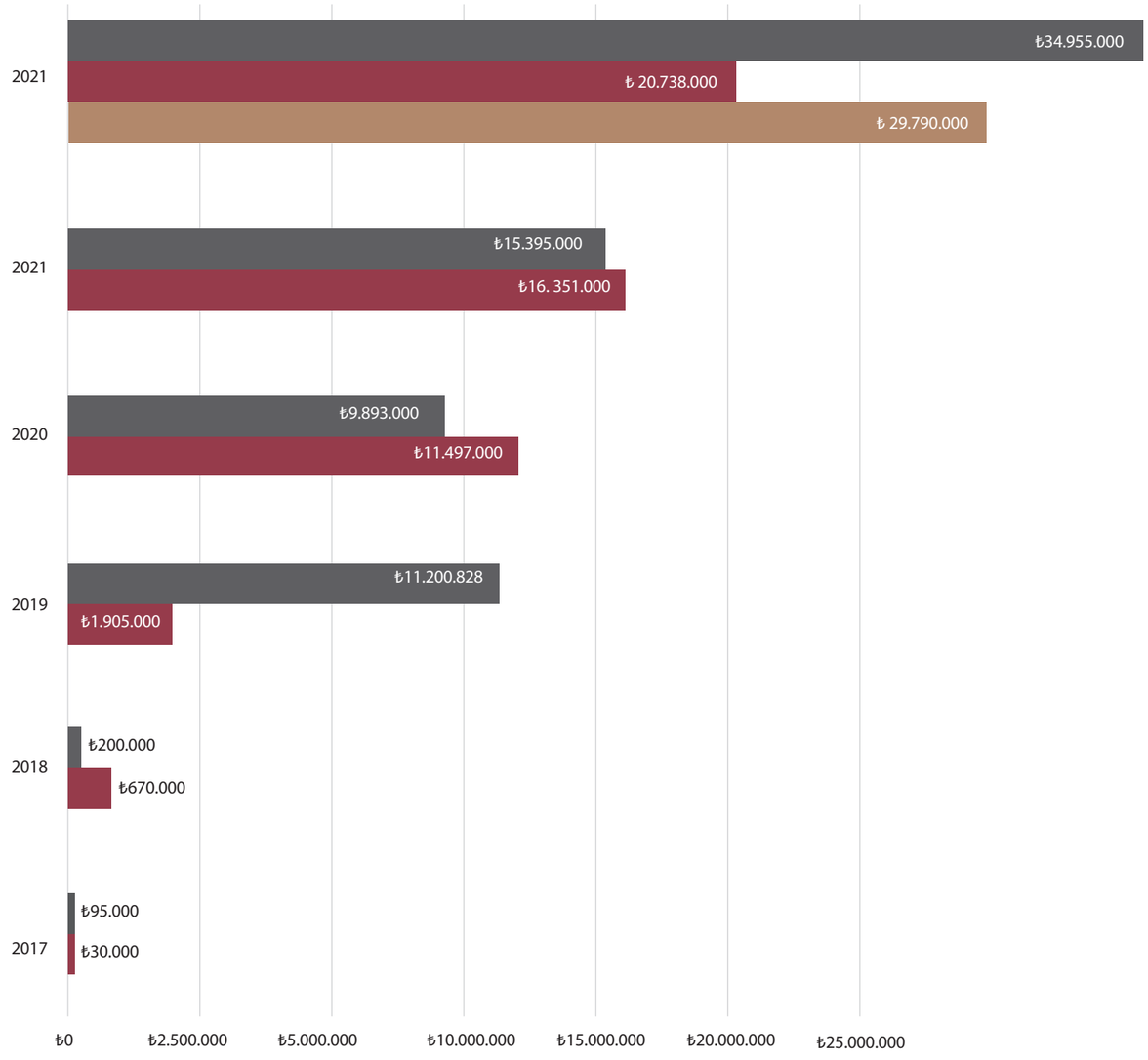
As of 31 December 2022, statistical data on the number of registrations and applications to VERBIS are as follows:



[6] Taken from the annual report published by the Board.
[7] Taken from the annual report published by the Board.

4. Sanctions

4.1. Administrative Sanctions



[8] The deadline for VERBIS registration and notification obligation is 31 December 2021, and with the announcement of the Authority dated 21 April 2022, it was stated that administrative sanctions will be imposed due to violation of the VERBIS registration and notification obligation. Therefore, there are no administrative fines imposed in the 2017-2021.

4.2. Review of Sanctions

- **36 Million Turkish Lira in Administrative Fines Between 2017-2022**

The highest penalty issued was 1,950,000 Turkish Lira to WhatsApp This penalty is the highest fine imposed in a single case and the highest since the Board started its activities.

- **32 Summary/Short Decisions Published in 2022**

- 20 administrative fines for not taking the necessary technical and administrative measures to prevent the unlawful processing of personal data.

- 1 administrative fine for not notifying the Board and data owners within a reasonable time that personal data is being processed unlawfully.

- 0 administrative fines for non-compliance with installation instructions and rectification orders.

- 4 administrative fines for not complying with general data protection principles.

- 0 administrative fines due to non-compliance with Article 11 regulating the rights of the data subjects.

- **Decisions Published by Sectors**

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

- 6 decisions about Banking and Finance
- 5 decisions about Retail and E-Commerce
- 4 decisions about Informatics, Telecommunication and Electronic Commerce
- 2 decisions about Health Care
- 2 decisions about Education
- 2 decisions about Human Resources
- 1 decision about Insurance
- 1 decision about Law
- There was no mention of sectors in 7 decisions

4.3. Decisions Published According to Relevant Law Articles

The distribution of the decisions published on the website of the Authority in 2022 according to the relevant law is as follows:

ADMINISTRATIVE SANCTIONS UNDER ARTICLE 18	Number
Administrative Fine for Violation of the Obligation to Inform – Article 18/1 (a)	0
Administrative Fine for Non-Compliance with Data Security Rules - Article 18/1 (b)	19
Administrative Fine for not complying with the Board Decisions - Article 18/1 (c)	0
Administrative Fine for not complying with Registration Obligations - Article 18/1 (d)	0
Disciplinary provisions for public Authoritys and public authorities - Article 18/3	2
SUM	**21**

5. Highest Administrative Fines

The table below lists the top 20 fines that have been issued by the Board since 2018, of the decisions that have been made public. Examining the table, the IT and Media sector comes first as the sector that receives the most penalties, when looked at the first five decisions with the highest administrative fines. When the relevant decisions are analysed, in four of these five decisions, data breaches were caused by malfunctions in information systems rather than administrative malfunctions (along with not notifying the Board in a timely manner).

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	Facebook	Information Technologies and Media	Article 12/1 Article 12/5	TRY 1,650,000	11 March 2019
4	Facebook	Information Technologies and Media	Article 12/1 Article 12/5	TRY 1,550,000	18 September 2019
5	Factoring Companies	Banking and Finance	Article 12/1 Article 12/5	TRY 1,500,000	03 March 2020
6	Marriott International	Tourism	Article 12/1 Article 12/5	TRY 1,450,000	16 May 2019
7	Amazon	e-Commerce	Article 18/1 Article 12/1	TRY 1,200,000	27 February 2020
8	Unspecified	Gaming	Article 12/1 Article 12/5	TRY 1,100,000	16 April 2020
9	Unspecified	Banking and Finance	Article 12/1	TRY 1,000,000	05 May 2020
10	Unspecified	Automotive	Article 12/1	TRY 900,000	22 July 2020
11	Unspecified	Healthcare	Article 12/1 Article 12/5	TRY 800,000	27 April 2021
12	Unspecified	e-Commerce	Article 12/1	TRY 800,000	10 March 2022
13	Dubsmash Inc.	Information Technologies and Media	Article 12/1 Article 12/5	TRY 730,000	17 July 2019
14	Unspecified	e-Commerce	Article 12/1 Article 12/5	TRY 600,000	20 April 2021
15	Clickbus Travel Services Inc.	Transportation	Article 12/1 Article 12/5	TRY 550,000	16 May 2019
16	Cathay Pasific Airway Limited	Transportation	Article 12/1 Article 12/5	TRY 550.000	16 May 2019
17	Unspecified	Tourism	Article 12/1 Article 12/3 Article 12/5	TRY 500.000	27 August 2019
18	Unspecified	Paper	Article 12/1	TRY 500.000	4 August 2022
19	Unspecified	Banking and Finance	Article 12/1 Article 12/5	TRY 450.000	N / A
20	Unspecified	IT	Article 12/1	TRY 450.000	N / A

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 shown in the table above, 80 percent of the sanctions applied in the decisions published by the Board are based on Article 18/1 (b), which sets out the administrative fine for not complying with the data security rules set out in Article 12. The reason for this is that the DP Law only stipulates sanctions for violations of Articles 10, 12, 15 and 16, and the DP Law does not stipulate any sanctions for violations of Articles 4, 5, and 6.

III. The Board's Principal Decisions

1.Blacklisting in the Car Rental Industry

The Board published in the Official Gazette its principal decision No 2021/1303 on blacklisting in the car rental sector on 23 December 2021.

Reports referred to by the Board stated that "blacklisting" software, application and programs were being used in the car rental industry. According to these investigations, car rental software developers sold car rental software that included a "blacklist" feature to car rental companies (or individuals working in the rental car industry). The personal data of the individual customers renting the car were then processed by the car rental companies using the software. The processed data included "blacklist" information such as adverse information on events during the customers' use of the vehicles or comments by the car rental company. This information was then processed by the car rental companies for use when deciding on further rentals. In addition, the software allowed the different car rental companies to access the data that one of them had entered, creating a system with data flow and transfer, allowing the relevant persons' personal data to be processed by multiple car rental companies.

Taking these matters into account, the Board decided that:

• The software companies and car rental companies that had control over the data were both data controllers where personal data was processed within the scope of blacklist practices in the car rental sector, and were in violation of the general principles in Article 4, the processing conditions in Article 5 and the provisions on transfers in Article 8 of the DP Law.

• Such unlawful practices would be terminated, and data controllers were to take the necessary technical and administrative measures set out in Article 12 of the DP Law to ensure that personal data processing processes in the car rental sector complied with the legislation.

• The public would be informed that Article 18 of the DP Law applied to data controllers using blacklist software in the car rental sector without taking the appropriate measures and in violation of the legalisation.

• The decision would be published on the Official Gazette and Board's website under Article 15/6 of the DP Law.

2. Payment and Debt Inquiry Services of Municipalities

The Board published in the Official Gazette its principal decision No 2021/1304 on municipalities' payment and debt inquiry services on 21 April 2022.

Various reports submitted to the Board stated that accessing municipal real estate tax payment/fast payment and debt inquiry services from the web by entering a person's TC identity number posed a problem in terms of the protection of personal data, and it was requested to examine this issue with respect to the DP Law. After investigation, the Board unanimously decided that:

• Municipalities should take the necessary technical and administrative measures within the scope of Article 12 of the DP Law by using membership and password or double-factor authentication in real estate tax payment/ fast payment and debt inquiry services.

• The public would be informed that action would be taken against the relevant municipalities under Article 18 of the DP Law in accordance with complaints/notifications about municipalities that do not take such measures.

• The decision would be published according to Article 15/6 of the DP Law on the Official Gazette and on the website of the Board regarding the necessity of using "membership and password" or "double factor authentication" within the scope of Article 12 of DP Law in municipalities' real estate tax payment/fast payment and debt inquiry services.

MOROĞLU ARSEVEN

IV.Summary of Important Decisions

1. Decision Regarding Special Category of Personal Data

1.1. Decision of the Board of Personal Data Protection on the processing of "hand geometry" information in order to enter the service building of an enterprise without obtaining explicit consent	Date : 07/07/2022 No : 2022/662

The data subject stated that when subscribing to a business, palm and fingerprint information were scanned by the relevant company authorities in order to allow entry into a service area, and that this data was processed in the company records. On the data controller not responding to queries, the data subject filed a complaint with the Board, claiming that the palm and fingerprint were scanned without a legally valid explicit consent. The legal issue addressed by the Board was whether hand geometry data was a special category of personal data.

Biometric data is special category of personal data according to Article 6 of the DP Law and these kinds of data can only be used and processed if the person that owns the data has given explicit consent or in the justified cases stipulated by the law.

The Council of State has stated in a decision that hand geometry recognition is a biometric measurement method. The EU's General Data Protection Regulation defines biometric data as physical features that can uniquely identify an individual. In other words, hand geometry is biological data used to identify or confirm that person. The Constitutional Court, with a similar point of view, considered biometric data to be special category of personal data that enables a person to be distinguished from others and to be identified.

The Board concluded that hand geometry data is a special category of personal data, since the device that recognized the hand geometry produced a three-dimensional picture of the hand that was almost impossible to mistake, and this data was used to authenticate individuals. Therefore, the processing of such data will only be possible in cases where explicit consent has been given or in the justified cases stipulated by the law.

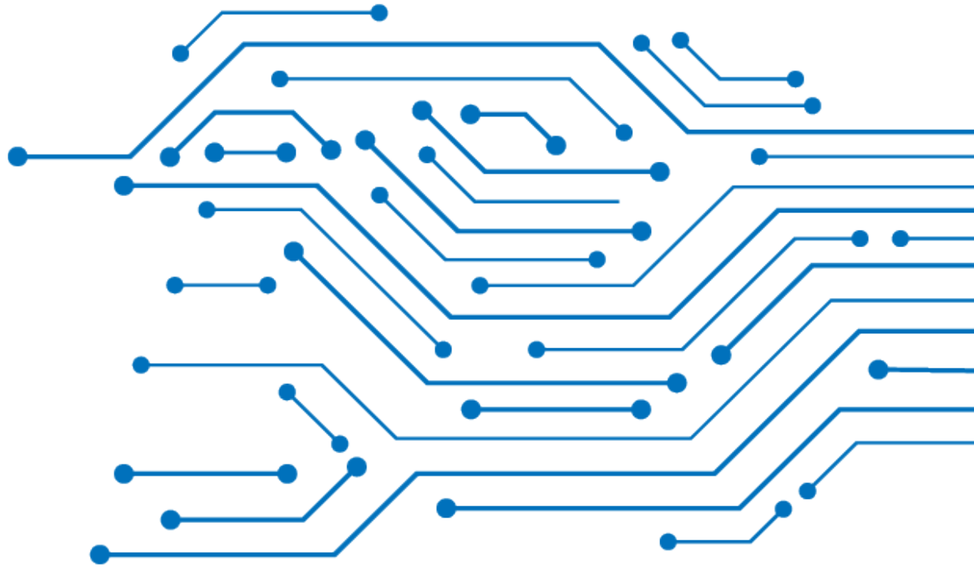
Customers whose hand geometry data was stored were not sufficiently informed about the stored personal data. Therefore, the Board requested the data supervisor to erase this data in accordance with Article 12 of the DP Law to prevent unlawful processing of the personal data and to ensure its security. The data supervisor was also subject to an administrative fine of 100,000 Turkish Lira.

2. Decision Regarding Loyalty Programmes

2.1 Decision of the Board of Personal Data Protection on the processing of personal data within the scope of a loyalty programme	Date : 05/07/2019 No : 2019/198

A special discount was applied to some products sold by the data controller under a loyalty card programme. The special discounts were conditional on participation in the loyalty programme. The customer's personal data was requested for membership in the loyalty programme and for the supply of the card, and explicit consent was imposed as a condition for membership in the loyalty programme. The Authority was notified about the data controller.

The Board found that, on examination of the products or services offered by the data controller under the loyalty programme, explicit consent to data processing was not required as a condition for the provision of the product or service (as opposed to the discount). The Board therefore decided that there was no action to be taken under the DP Law regarding the complaint.



3. Decisions Regarding Sending Commercial Electronic Messages

3.1 Decision of the Board of Personal Data Protection on the processing of personal data by sending an SMS with advertising content by a data controller selling medical products	Date : 11/11/2021 No : 2021/1153

The complaint submitted to the Board stated that:

• A commercial electronic message with advertising content selling medical products was sent from a data controller to the complainant's mobile phone number, which was regarded as personal data.

• The complainant had not given explicit consent for the processing of his personal data, and had requested the data controller for the deletion of his personal data, and had also asked for information about how his personal data was obtained.

• In response to the application, the data controller stated that they did not have any data other than the phone number of the data subject. The mobile phone number in question was the contact information of another patient registered with the data controller who had consented to receive advertising and promotional messages, and that it was believed that that person had accidently given the complainant's phone number to the data controller.

The complainant considered the answer given by the data controller to be insufficient and the data controller to be negligent since the approval mechanism was carried out without verification. The complainant requested the necessary action to be taken about the data controller.

The Board decided that:

• The mobile phone number in question was not associated with the relevant person in the records of the data controller and that the incident subject to the complaint occurred as a result of the wrong number being inadvertently reported by a customer. Therefore, there was no necessary action to be taken under the DP Law.

• The data controller would be instructed to delete the complainant's personal data in accordance with Article 7 of the DP Law and the Regulation on the Deletion, Destruction or Anonymization of Personal Data.

3.2 Decision of the Board of Personal Data Protection on the processing of mobile phone number personal data by calling and sending marketing SMS messages	Date : 02/12/2021 No : 2021/1210

The complainant stated that they had received multiple calls about Digitürk campaigns to their mobile phone number from a Digitürk dealer and that an SMS was sent to the complainant for the purpose of advertising and marketing Digitürk services. However, the complainant had given no explicit consent for the processing of the contact information through sending commercial electronic messages. Therefore, personal data was processed unlawfully without relying on any processing conditions. The complainant made an application to Digitürk. In response, Digitürk stated that the complainant's personal data was not contained in its systems because the person did not have a subscription record with the company, the commercial messages in question were not sent by Digitürk (but by the dealer and/or the dealer's subcontractors) and that the originating phone numbers specified in the compliant did not belong to Digitürk. The complainant requested an investigation.

The Board made the following evaluations:

• When an evaluation was made regarding the relationship between Digitürk and the dealer, Digitürk was the data controller since it had the authority to make decisions and give instructions regarding the processing of personal data of the data subject. The dealer was data processor when acting within the instructions given to it.

• MD was an individual subcontractor of the dealer. MD was authorized to use the telephone line registered with the dealer under the subcontracting agreement. The responsibility for the use of the line was left to MD, and the agreement did not contain provisions indicating that MD was operating within the framework of the dealer's instructions. Therefore, the dealer did not qualify as a data controller regarding the incident in the complaint. Instead, MD was one of the data controllers in the personal data processing activity in the complaint. Since the communication channels used for sending commercial electronic messages were personal data, the message sending process also had to comply with the data protection legislation. As the data was obtained by number derivation, no processing condition had been met in the processing of the phone number.

• MA, a further individual subcontractor of the dealer, was found to be the other data controller in the incident subject to the complaint. An application form was submitted in evidence that included the mobile phone number of the complainant. The date of the form was written in MA's handwriting, and the "I give consent" box was ticked, including MA's name and phone number. When an evaluation was made in terms of personal data processing activity, the validity of the form, which was allegedly filled in by the complainant over a website, had to be questioned, because the relevant form was not submitted to the Board in the form shown on the website or in a log record or similar format. Since the document was signed by MA himself, it was not sufficient to believe that the form was filled by the complainant, as MA claimed, and the form could not be accepted as a lawful explicit consent declaration.

The Board decided that:

• Since it could not be determined that Digitürk and the dealer acted as data controllers in the present case, there was no action to be taken against the companies.

• Administrative sanctions would be issued against the data controller MD for the phone number personal data of the data subject processing not being based on any processing conditions.

• MA was a data controller. The form submitted by MA to the Board could not be accepted as explicit consent and there were no stipulated processing conditions in accordance with the law. Administrative sanctions would therefore be issued against MA.

• MD and MA would be instructed to destroy the relevant phone number data and to inform the Board of the result.

• Digitürk would be instructed to direct/inform its dealers to show maximum care and attention regarding compliance with the DP Law in the process of acquiring new customers, and to include clear provisions regarding who is the data controller and data processor when concluding contracts with dealers.

3.3. Decision of the Board of Personal Data Protection on the processing of the personal data without the explicit consent of a data subject for the purpose of sending commercial electronic messages by the data controller operating in the health sector	Date : 18/01/2022
	No : 2022/31

The complaint stated that a commercial message was sent to the data subject's e-mail address by the data controller operating in health sector, without either the explicit consent of the data subject or the special conditions stipulated for the processing of personal data under the DP Law.

The Board made the following evaluations:

• Processing the contact information of the data subject or his companions during the opening of a patient registration did not constitute a violation of the DP Law or other legislation. However, in the present case, the contact information of the data subject had been used for a marketing activity. The content of the e-mail sent to the data subject was for informational and commercial purposes, and was not used for the transmission of any medical information to him or his relatives.

• Clause (ç) of Article 4/2 of the DP Law states that personal data can only be processed in a limited, connected and measured way for the purpose for which it is processed. Although it is lawful for the data controller to receive contact information from the relevant person when opening a patient record, in the case in question, the personal data was processed for the purpose of sending a commercial email, which was an unrelated purpose to the purpose of acquisition of the data.

• Although it was lawful for the data controller to acquire the personal data of the data subject, the data processing activity complained of was unlawful because the personal data in question was not used for the purposes for which it was obtained, without a justification. An administrative fine of 100.000 Turkish Lira would therefore be imposed.

4. Decisions Regarding Liaison Offices

4.1 Regarding an employee not being informed by a data controller residing abroad about the personal data processing activities carried out about the data subject, and the unlawful processing of the personal data by the data controller	Date : 02/12/2021 No : 2021/1218

The complaint stated that the data subject had been working for a data controller that was resident abroad at its Istanbul liaison office when his contract was terminated. It stated that the Istanbul liaison office of the data controller had not fulfilled its obligations arising from the DP Law regarding the employee as data subject during the employment and on termination. Clear and accurate information had not been supplied to the employee in response to a letter prepared by the employee as data subject based on Article 13 of the DP Law and addressed to the Istanbul liaison office. The employee had not been properly informed of the relevant data processing issues, including the purpose and scope of the processing of his personal data and special category of personal data, and his explicit consent had not been properly obtained.

Although the employee filed a complaint against the Istanbul liaison office of the data controller, the liaison offices of foreign companies in Turkey did not have legal personality. Under Article 2, the DP Law was only applicable to real persons and legal persons. Instead, an investigation was initiated against the data controller residing abroad based on the claims of the data subject.

The Board decided that:

• The data subject had been informed within the scope of the obligations of the EU's General Data Protection Regulation (GDPR). However, the data controller was reminded to fulfil the obligation of disclosure in accordance with Article 10 of the DP Law in relation to personal data processed in Turkey.

• The relevant person had to take action before the judicial authorities to resolve the disputes arising from the business relationship between the data subject and the data controller.

• The data controller had to respond to the applications made by the data subject in accordance with Articles 11 and 13 of the DP Law and Article 5 of the Communiqué on the Procedures and Principles of Application to the Data Controller, and in accordance with principles of the law and honesty under Article 13 of the DP Law and Article 6 of the Communiqué on the Procedures and Principles of Application to the Data Controller.

4.2. Regarding a foreign data controller requesting personal data from candidates during a recruitment process at a liaison office in Turkey	Date : 24/02/2022 No : 2022/172

The complaint stated from the data subject who was an employee at the liaison office and requested for his criminal record, health report, lung film report, blood group certificate, photocopy of driver's licence, photocopy of marriage certificate and the identity cards of family members. These documents were provided by the data subject and the liaison office had not obtained explicit consent from the data subject for the processing of these special categories of personal information. The complaint stated that requesting identity card information of family members contradicted the general principles in Article 4 of the DP Law, because the data controller was resident abroad, and the personal data of the data subject could be transferred abroad. In addition, the data controller had not responded to an application by the data subject within the 30-day legal period.

The Board decided that:

• The company resident abroad was data controller, not the liaison office.

• Since the liaison office manager was also the employer's and the data controller's representative, the application made by the data subject to the liaison office was legally binding and valid.

• The data controller did not respond to the data subject's application within the required legal period, violating the provisions of the DP Law and the Communiqué.

• In the present case, it was not illegal to transfer data abroad. The personal data of the data subject was obtained through the contract concluded by the data controller residing abroad within the scope of the business relationship, in accordance with the law of the resident country. However, the relevant provisions of the legislation abroad had not been thoroughly explained to the data subject or the Board.

• Since it was necessary for the personal data of the data subject to be processed abroad for the execution of the employment contract, the only way to accomplish this was to obtain their explicit consent. The express consent obtained from the data subject had been obtained lawfully.

• A supporting document stating that the personal data of the data subject had been destroyed at both the company headquarters and the liaison office had not been submitted to the Board.

The data controller was instructed to:

• Pay the utmost care and attention to applications by data subjects.

• Submit the document showing that the personal data of the employee has been destroyed at the company headquarters and the liaison office to the Board.

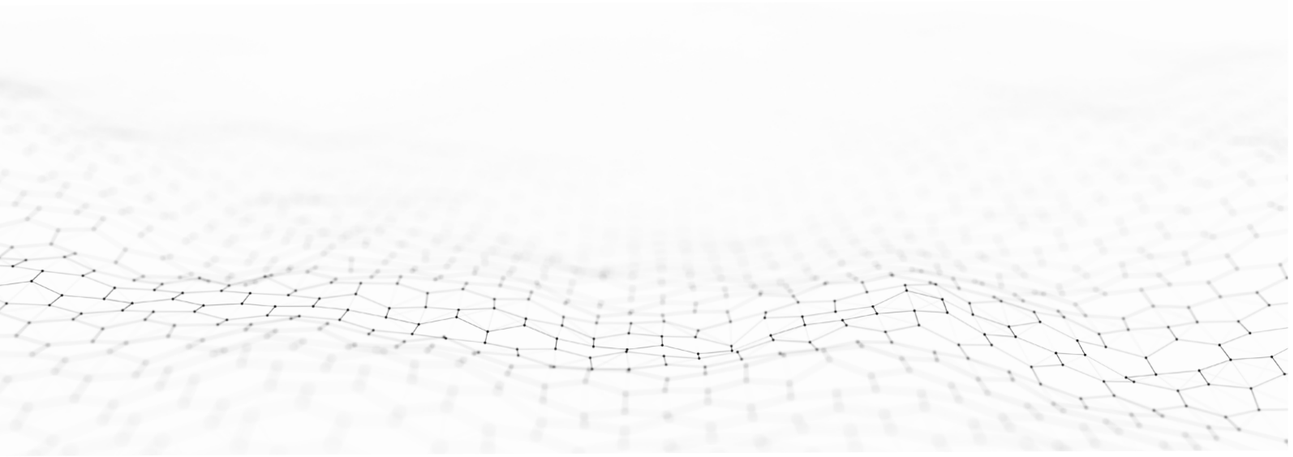
5. Decisions Regarding Commercial Companies

5.1 The unlawful sharing on the internet of company registry information personal data	Date : 06/01/2022
	No : 2022/6

The name and surname of a former partner of a company was shared on the website of the company without permission. The data subject applied verbally and in writing to the Chamber of Commerce for the deletion of this data because he had no administrative or legal role in the company, but the Chamber of Commerce rejected his request.

Under the DP Law, personal data must be deleted, destroyed or anonymized at the request of the person if the reasons for the data processing have lapsed. The Board concluded that the purpose of presenting the information in the Trade Registry Gazette on the page of the Chamber of Commerce was to provide easier access to information on trade registry transactions. As stipulated in the Union of Chambers and Commodity Exchanges of Turkey and the Law on Chambers and Commodity Exchanges, the responsibilities of these Authorities were to facilitate the acquisition of information concerning trade and industry, and to provide all kinds of information that their members might need while performing their professions.

The Board decided that it was the duty of the Chamber of Commerce to store this data and that therefore the processing of the personal data was legitimate under the DP Law. As the reason for the retention of the data in accordance with the DP Law had not yet lapsed, the Board rejected the request of the data subject and decided that there was no action to be taken against the data controller under the DP Law.



5.2 Sharing the content of a file regarding enforcement proceedings initiated against a company in which the name of the data subject was mentioned in the title	Date : 10/02/2022
	No : 2022/103

A legal enforcement proceeding was initiated by the data controller. The data subject's name was mentioned in the title of the enforcement proceeding. The enforcement file was shared with third parties in an open social media group. The data subject filed a complaint to the Board, stating that his personal information had been disclosed in the enforcement file and that his personal rights were violated.

The Board decided that the data shared did not meet the definition of personal data in the DP Law. Although the name and surname of the relevant company official were used, the sharing and the comments made under the post were aimed at the company, and the company's title or debt information, address and tax identification number did not have an effect on the rights and interests of a real person. Therefore, the data shared was not personal data but "data belonging to a legal person". The complaint was rejected by the Board and no action was taken against the data controller under the DP Law.

6. Decisions Regarding Personal Data Processing Activities in Business Relationships and Recruitment Processes

6.1 An employment job search and recruitment platform engaging in practices contrary to the DP Law	Date : 14/10/2021 No : 2021/1051

The complaint submitted to the Board stated that the data controller, an employment platform that carried out job search and recruitment processes, had engaged in practices contrary to the DP Law regarding the confidentiality and processing of personal data. The data subject had requested a digital copy of all the information and documents submitted to employers regarding his job applications and interviews. This was not fulfilled by the data controller. In addition, the reply letter sent in response to this application stated that the data would be deleted without the consent of the data subject.

The data subject had filed a complaint to the Board before making the request for access to his personal data to the data controller. The data subject had not submitted evidence to the Board contrary to the data controller's statement that the data subject's personal data had been or would be deleted. There was therefore no action to be taken under the DP Law regarding the complaint for not being able to access the personal data.

As the data subject continued to apply for jobs on the platform after the date of the complaint and request for deletion of his data, no fault could be given to the data controller. No action could be taken under the DP Law in relation to the data subject complaints as to the notification that the personal data would be deleted/destroyed by the data controller without the data subject's request.

The data subject had not submitted any substantiating evidence regarding the claim that personal data regarding job applications and job interviews had been transferred to other employers without the knowledge and consent of the data subject. The data controller stated that employers could only see information uploaded to the platform by employee candidates, and there was no practice of transferring employers' notes and impressions about employee candidates to other employers. The Board therefore determined that there was no action to be taken under the DP Law.

6.2 A data controller employer accessing the corporate e-mail account of a former employee	Date : 25/11/2021 No : 2021/1187

The data subject was a former employee of the data controller. The complaint stated that the data subject's private data had been accessed by the data controller through their former company e-mail account. This included private conversations, personal bank account statements and expenditure records. No explanation or notification had been made by the data controller stating that the e-mail accounts given to the company employees should be used only for business purposes. The complaint stated that personal data belonging to the data subject had been processed and transferred to third parties by the data controller in violation of the processing conditions stipulated in the DP Law, including in the period after the data subject had unilaterally terminated the employment contract. No clarification had been made to the data subject and a clear clarification text had not been presented that employee information was being kept. The platform on which the relevant personal data was kept was a cloud service provider with servers located abroad. Although it was not clear who had access to the data subject's company e-mail account, from the content of the reply letter submitted by the data controller, it was understood that the data was accessible to the company shareholders and company officials and some other workplace employees.

The Board made the following determinations:

• The company e-mail account had been allocated to the data subject by the data controller within their business relationship, to be used in corporate activities and for the purposes of work. However, the data controller had not properly informed the data subject under Article 10 of the DP Law and Article 4 of the Communiqué on the Procedures and Principles to be Complied with in Fulfilling the Obligation to Inform ("Communiqué") as to how and when the emails could be examined.

• The examination of the data subject's e-mails by the data controller was not based on any processing condition, as the data subject had not been informed under the DP Law and the Communiqué.

• Where the data subject requested the deletion of unlawfully processed personal data, to the extent that that data had been presented to the court as evidence in an ongoing lawsuit, there was no action to be taken under the DP law, as it was not possible to examine matters subject to the court's jurisdiction.

• In the present case, the data subject undertaking his correspondence via his company e-mail did not mean that he wished to disclose his data to the public, so the personal data had not been made public.

• As the examination of the e-mails of the data subject by the data controller was not based on any processing conditions, and due to the fact that no disclosure was made to the data subject within the scope of the provisions of the DP Law and the Communiqué, an administrative fine of 250,000 Turkish Lira would be issued to the data controller.

• The application sent to the data controller by the data subject did not include the claim that his data had been made accessible to unauthorized third parties. It was necessary to remind the data subject that the relevant person should first convey such claims to the data controller under Article 14 of the DP Law.

• An investigation would be initiated into whether the personal data processing in question had to be carried out in accordance with Article 9 of the DP Law because the cloud service provider company was located abroad.

6.3 Decision of the Board of Personal Data Protection on the processing of an e-mail address regarded as personal data by a human resources firm in order to send e-mails for advertising and marketing	Date : 09/12/2021
	No : 2021/1243

The complaint submitted to the Board stated that:

• Commercial promotional e-mails had been sent to the data subject by a human resources firm that was responsible for the data.

• The data subject had not had any previous legal relationship with the data controller, so had no knowledge of where and how his personal data was obtained.

• The data subject had not given explicit consent for the processing of his personal data.

• The data subject had applied to the data controller in this regard and had requested the deletion of his personal data, but had not been informed about where his personal data had been obtained or for what purpose it has been processed.

The data subject requested the necessary action to be taken against the data controller.

The Board decided that:

• Since the e-mail address was the personal data of the data subject and it was processed by sending a commercial e-mail to the data subject, and none of the conditions for the processing of personal data were present, the data controller was subject to Article 12 of the DP Law. An administrative fine of 50,000 Turkish Lira would be imposed on the data controller in accordance with paragraph (1) of Article 18 of the DP Law.

• The data controller would be instructed to delete the personal data of the person and to forward the log records of the destruction process to the Board.

6.4 The unlawful processing of the personal data of a data subject whose employment contract had been terminated by the data controller company	Date : 16/12/2021
	No : 2021/1258

The complaint stated that the data controller company did not have an application form allowing data subject employees to apply to the company for the deletion of their personal data. In addition, it stated that the data controller's obligation to properly inform the data subject had not been properly fulfilled. Special category of personal data was processed without explicit consent. Log-ins into the data controller company were through a fingerprint and face scanning system, and the group company had branches abroad so that the data subject's personal data was transferred abroad without his explicit consent during foreign branch visits. Adequate technical and administrative security measures were not taken for his personal data, and there was no privacy policy on the website of the data controller company.

As a result of the investigation, the Board made the following determinations:

• The wording of the employment contract did not fulfil the obligations to inform and receive explicit consent, and the clarification text did not contain the minimum elements that were required.

• The explicit consent text included in the employment contract (in which the data controller company claimed legal reasons for processing the biometric data) was not signed voluntarily because the data subject did not have a chance to start work without signing the employment contract, and the possibility of not accepting the explicit consent text was not explained to the relevant person.

• The purpose of the biometric data scanning on entrance and exiting the workplace could be achieved by other means, and the processing of biometric data based on the explicit consent requirement was disproportionate and unlawful.

The Board decided to:

• Instruct the data controller company to destroy the illegally processed biometric data and inform the Board of having done so.

• Issue an administrative fine of 125,000 Turkish Lira on the data controller company for violating its obligation to take the necessary technical and administrative measures regarding the protection of personal data.

MOROĞLU ARSEVEN

7. Decisions Regarding the Technology and Media Sectors

7.1 The allegation that an untrue and dishonourable television report was made about the relevant person by using her photograph and that of her child	Date : 02/12/2021 No : 2021/1217

The complaint to the Board stated that a media company, as data controller and service provider, had broadcast an untrue, dishonourable and degrading television news item about the data subject using photographs of her and her child taken from her Facebook page. In addition, despite an application made to the media company, the illegality had not been resolved within the legal period of 30 days and the applicants had not been properly informed in response.

The Board made the following evaluations:

• The name and surname of the data subject, and a photograph of her and her child was personal data, since they made the individual specific or identifiable. The media company was therefore a data controller of that data.

• The fact that the photograph was blurred on publication did not remove its nature as personal data, since it was possible to identify the relevant persons in the photograph and other information such as their names was combined and matched with it. It was also possible to access the unblurred version of the photo through an internet search of the name of the data subject.

• The fact that the photograph had been on Facebook did not allow its use for any other purpose. The processing of the photograph had to be based on the personal data processing conditions regulated in the DP Law. "Publicizing" under the DP Law had a narrower meaning than the presentation of personal data to the public and was closely related to the will of the data subject and the purpose of making it public.

• In determining whether news is of public interest and benefit, it is necessary to evaluate whether the news serves the public's sense of unnecessary curiosity or the protection of high moral and legal values. There was no public interest and/or benefit in the sharing of the information that constituted the basis of the news item in the complaint. However, considering that such news was frequently featured in the press, whether the news in question had "public interest and benefit" was controversial.

• In settled judicial decisions on news reporting it was accepted that it was possible for the press not to be held responsible for news made in accordance with apparent reality even if that was different from actual reality.

• While the wider facts on which the news item was based were real, when viewed as a whole the news item was not true because the name and photograph used were of a person unrelated to the incident. The media company therefore did not pay attention to the accuracy of the elements in the news content before publishing.

• There was no legal reason for the personal data processing activities carried out by the data controller as to the data subject, making the data processing activities illegal.

The Board issued an administrative fine of 300,000 Turkish Lira on the data controller and informed the data subject that further action could be taken before the judicial authorities for material and/or moral compensation claims.

7.2 Yemek Sepeti Elektronik İletişim Perakende Gıda Lojistik AŞ about data breach notification	Date : 23/12/2021
	No : 2021/1324

The data controller notified a data breach to the Board. As a result of examining the notification the Board's determined that:

• The data controller's server had been accessed by third parties installing an application and running a command, due to a vulnerability on a web application server belonging to the data controller.

• 21,504,083 users were affected by the breach.

• Affected personal data included usernames, addresses, phone numbers, e-mail addresses, passwords and IP information.

• Considering the large number of people affected by the breach and the fact that almost the entire customer database was leaked, the breach was very large.

• Considering the extent of the breach, the size of the leaked data and the nature of the leaked personal data, the breach posed significant risks for the relevant persons, such as loss of control over personal data.

• The person or persons that entered the system had collected information by accessing other systems with malicious software and tools and had installed malicious software on the system that ran for eight days. The data controller was at fault because it was responsible for checking which software and services were running on the information networks and determining whether there was a problem.

• Alarms from security software products monitored by third party companies were turned off before the data controller's security team were notified and before the necessary actions were taken. As the breach was noticed a week later as a result of the examination of an alarm sent by the data controller's security team, this indicated that the data controller did not have an effective control mechanism over the third-party companies that it received services from, and that there were deficiencies in the follow-up of security software and the use of security procedures.

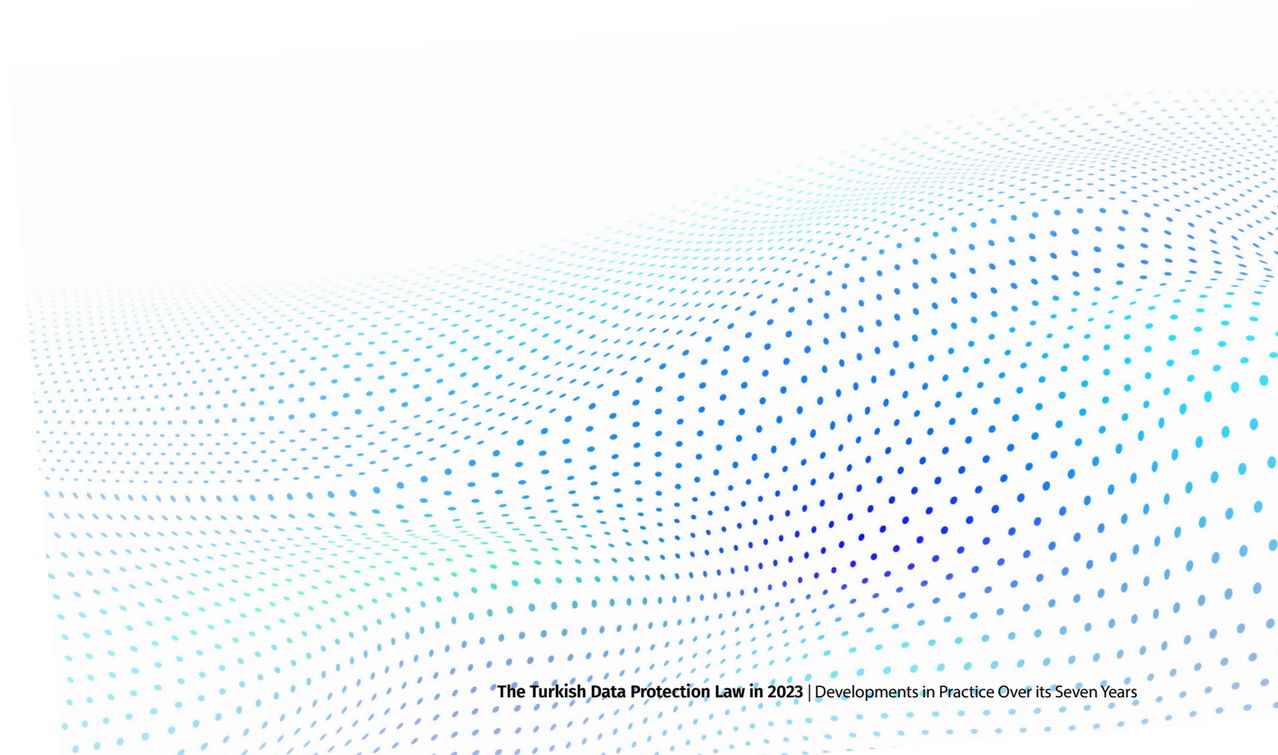
MOROĞLU ARSEVEN

• The attackers forwarded the data they obtained from the data controller to an IP address/server location in France. The fact that 28.2 GB of data leaving the system/outgoing traffic was not noticed by the data controller even though there were traces on the firewall was an indication that security controls and data security monitoring were not carried out properly by the data controller.

• As it was stated that the server has passed penetration tests, the penetration tests were not properly conducted.

• A data controller who processes a large amount of personal data experiencing such a violation and being late in intervening was an indication that the data controller did not properly assess the existing risks and threats.

The Board issued an administrative fine of 1,900,000 Turkish Lira on the data controller for failure to take the necessary technical and administrative measures to ensure data security, taking into account the extent of the violation, the seriousness of the effects, the fault of the data controller and the economic situation.



7.3 The creation of a blacklist program processing personal data and the sharing of this data among the car rental companies by the software developers and dealers of car rental programs	Date : 23/12/2021
	No : 2021/1303

The notice submitted to the Board stated that car rental companies had recorded data about their customers through software provided by car rental software manufacturers or vendors, who were data controllers processing personal data. Other rental companies using the same software could see the personal data of the relevant customers through a "blacklist" without the data subject's consent, and therefore the personal data was shared with other users using the software.

The Board made the following evaluations:

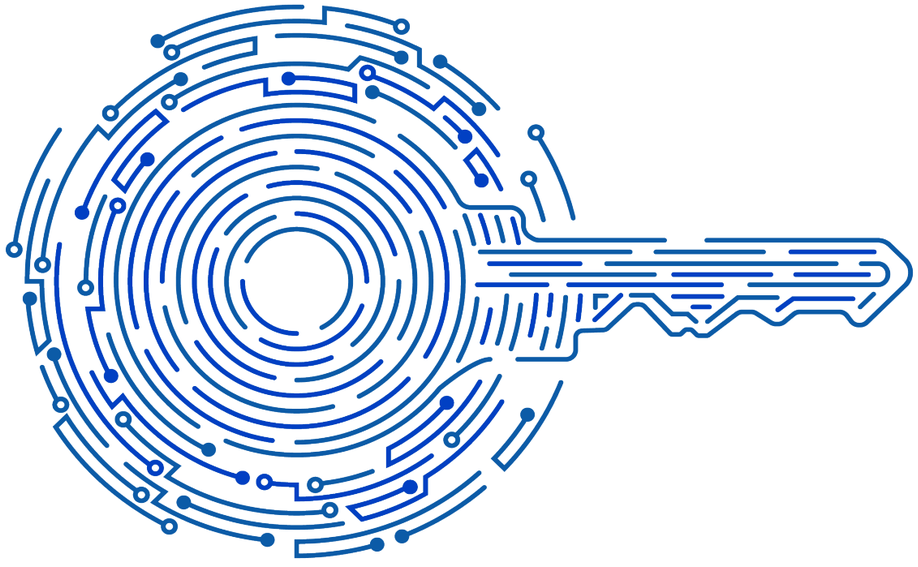
• The personal data of the customers had been processed in breach of the DP Law.

• The software company was a joint data controller with the car rental company, as the software company made the processed data available to other customers.

• Car rental companies notifying law enforcement agencies of the car rental process and collecting necessary data under the rental contract was in accordance with the data processing conditions under the DP Law.

• The blacklist database harmed the fundamental rights and freedoms of individuals, and was contrary to the general principles of the DP Law such as being in compliance with the law and honesty, having specific and legitimate purposes, being connected with a legitimate purpose, and being limited and proportional.

• An administrative fine would be issued unless all processes, necessary administrative and technical measures were carried out in accordance with the legislation



7.4. Unlawful processing of personal data by a data controller company operating in the e-commerce sector, through cookies used on the website/mobile applications	Date : 10/03/2022
	No : 2022/229

The complaint submitted to the Board stated that the cookie policy implemented by a data controller company operating in the e-commerce sector was intrusive to the fundamental rights and freedoms of individuals and the privacy of private life. In addition, as the company's website policy statement on the use of cookies contained incomprehensible and unspecified information, the obligation to inform about cookies had not been fulfilled. It was not legally possible to claim mandatory legitimate interests as a processing condition for the use of cookies, and the processing activity was not carried out by the data controller based on explicit consent. Furthermore, it was not stated which data subjectgroup the complainant was included in, and the processing purposes of the data types, data categories and data types processed in relation to the member customer and the guest customer were not fully explained and their scope was not understood.

The Board made the following evaluations:

• While there was no need for the explicit consent of the relevant persons regarding mandatory cookies for a website to function properly, the use of cookies for advertising, marketing and performance purposes was subject to the users' explicit consent.

• "Strictly necessary cookies" are cookies that are necessary for the website to work properly. Such personal data processing can be carried out based on one of the processing conditions in the DP Law without the explicit consent of the relevant person.

• If personal data processing is carried out with cookies that are not "strictly necessary cookies" and one of the processing conditions in the DP Law is not met, the explicit consent of the relevant person is required.

• Although it is understood that the data controller evaluates the user preferences of the data subjects within the scope of strictly necessary cookies, and that these cookies are used for the purpose of providing functionality, where it is not clear that the data subject clearly requests the information society service, explicit consent is required.

• Explicit consent according to the DP Law, is defined as "consent on a specific subject, based on information and expressed with free will" and it is accepted as a principle that explicit consent will be given through an "active action". If the data controller uses cookies that are not strictly necessary, and there is no explicit consent mechanism for this processing activity, personal data processing cannot be carried out without relying on one of the personal data processing conditions in the DP Law.

• The data controller's cookie policy did not clearly state which personal data was associated with which processing purpose and the legal reason for processing, or which personal data was obtained by which method, as required by the Communiqué on the Procedures and Principles to be Complied with in Fulfilling the Obligation to Inform.

As the data controller carried out personal data processing activities through cookies other than those that were "absolutely necessary", and personal data was transferred without relying on any of legitimate transfer methods, the Board issued an administrative fine of 800,000 Turkish Lira on the data controller, who had not fulfilled the obligation to take the necessary technical and administrative measures to ensure data security.

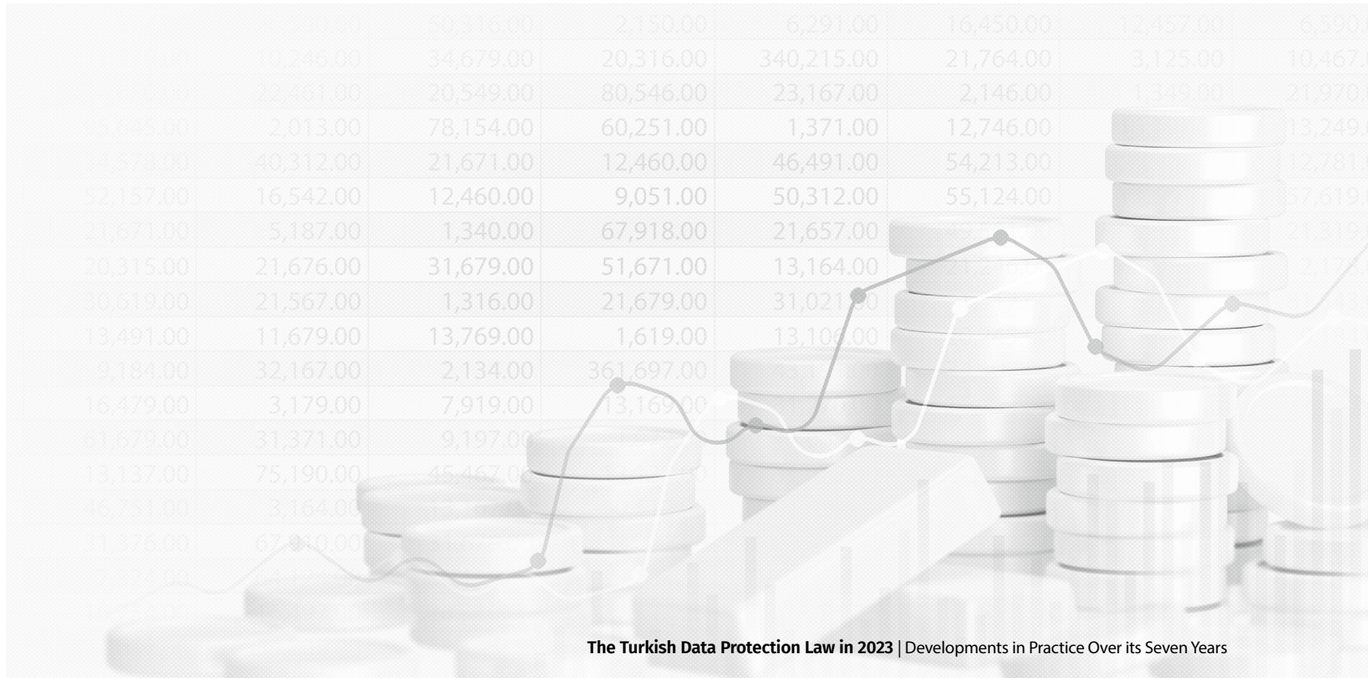
8. Decisions regarding the Banking, Finance and Insurance Sectors

8.1 Regarding the unlawful processing of personal data by a bank by sending an SMS to the mobile phone number of the relevant person	Date : 02/11/2021 No : 2021/1104

The complaint submitted to the Board stated that the data subject had requested a bank to delete telephone number information given to the bank when he was customer. The bank replied stating that the necessary actions had been taken and that the personal data would not be processed other than for the purpose of storage. However, the bank continued to send messages via SMS and e-mail. The messages were informational and related to COVID-19 epidemic measures. The Regulation on Commercial Communication and Commercial Electronic Messages was used as a justification when the complainant applied to the bank.
The Board made the following determinations:
• Article 42 of the Banking Law required banks to retain relevant documents for 10 years, within the framework of its procedures. A period of 10 years had not passed since the account was closed. Therefore, the reasons for processing of the personal data for the purpose of storage had not lapsed. It was not unlawful for the data controller to retain the data. However, the processing of the personal data by sending an SMS served a different processing purpose.

• The Bank's processing of the personal data of the data subject by sending an SMS for information purposes was not based on any pre-mentioned processing conditions. Therefore, an administrative fee of 50,000 Turkish Lira would be issued to the data controller.

• As the 10-year period had not passed since the last transaction date, the reasons requiring the processing of the personal data of the data subject had not yet disappeared. The request for the deletion of this data was not lawful for the data controller to fulfil, and there was no action to be taken under the DP Law regarding this.



MOROĞLU ARSEVEN

8.2 A bank not correcting the credit rating of the data subject, and sharing his personal data with third parties	Date : 02/11/2021
	No : 2021/1107

The complaint submitted to the Board stated that a bank, the data controller, had allowed unlawful transaction activities on the data subject's credit card account that affected his credit score. He complained that he had not made any credit card or credit applications with other financial institutions and that therefore his financial information had been non-accurately and unlawfully shared with third persons and his reputation had been unfairly damaged. In addition, his requests to the Bank had not been responded to.

The Board determined that the data controller had failed to fulfil its obligations since credit score information, as personal data, had been wrongly processed. The transfer of the misleading personal data to the Risk Centre violated the DP Law's general principles of "being accurate, up-to-date and used when necessary" and of preventing the unlawful processing of personal data. As a bank, the data controller had a great deal of power in the banking sectordata subject and had an active duty of care to ensure the accuracy of the personal data it processed, due to the creation of financially important consequences for the data subjects.

The Board issued an administrative fine of 150,000 Turkish Lira on the data controller. It also reminded the data controller that the applications of data subjects should be answered adequately and in accordance with the procedure determined in the Law and the Communiqué on the Procedures and Principles of Application to the Data Controller.

8.3 Regarding the sharing of personal data by a data controller bank by making a phone call to the family of the data subject	Date : 09/12/2021
	No : 2021/1239

The complaint submitted to the Board stated that the data subject had entered into a loan agreement with a bank, the data controller, which had shared his personal data making a phone call to his family. The data subject's parents' phones were persistently called, with the reason given that the bank was unable to reach the complainant. The data subject stated that he had been put in a difficult situation because of the calls.

The Board determined that:

• There was no action to be taken against the data controller under the DP Law. The data controller had called the phone number registered in its system. From the available information and documents, it was not possible to determine whether personal data had been shared by the data controller. The necessary action had been taken in a timely manner by the data controller on the request of the data subject.

• The data controller was to be reminded be more careful to protect personal data during phone calls and to inform its personnel about this issue.

8.4 Decision of the Board of Personal Data Protection on the processing of the data subject's banking information by an insurance company	Date :16/12/2021
	No : 2021/1262

The complaint submitted to the Board stated that a data subject had not shared his banking information with a data controller insurance company, and that his information had been processed unlawfully by the data controller. Through their attorneys, the data subject applied for information from the data controller and for his personal data to be deleted or destroyed, but his application was left unanswered. The data subject requested the necessary administrative sanctions under the DP Law.

The data controller insurance company requested a power of attorney with special authority from the data subject's attorneys in order to access the data subject's personal data for the purposes of his application.

The data controller claimed that it carried out its activities in cooperation with insurance agencies and had collected the data subject's personal data (account type, bank code, account type, branch code, foreign currency information, account number, purpose of use and IBAN number) in order to collect policy premiums and to fulfil its policy obligations. A decision of the Consumer Arbitration Committee had held that account information regarding an insurance payment made to a data subject must be kept for 10 years in accordance with the relevant legal obligations.

The Board determined that, although the application submitted by the data subject to the data controller through their representative was not answered because the data controller had not received a power of attorney, the personal data protection legislation did not require a special power of attorney for applications made by data controllers through their proxies. The Board stated that the condition of "special authorization" should not be sought. Based on these evaluations, the Board decided that there was no action to be taken against the data controller under the DP Law.

8.5 Sharing the phone number of a data subject with third parties by a bank's call centre	Date :10/03 /2021
	No : 2022/224

The complaint submitted to the Board stated that the data subject had found a bankcard at the bank's ATM. The bank's call centre officer suggested delivering the bankcard from the data subject to the cardholder by sharing the data subject's phone number with the cardholder. The data subject did not consent to this solution data subjectand instead handed over the bankcard to bank officials at the call centre officer's request. However, a message was sent by the cardholder to the data subject via their personal phone number. As personal data had been transferred to the cardholderdata subject, the data subject had not been informed of the processing of their name, surname and telephone number, and had not explicitly consented to the transfer of their data.

The Board decided that:

• The unlawful sharing of the name, surname and telephone number information of the data subject with a third party was a data breach. Administrative sanctions would be imposed on the data controller under Article 18 of the DP Law, as the data controller had not fulfilled its obligation to prevent the unlawful processing of personal data and had not been able to preserve the data properly according to Article 12 of the DP Law.

• When contacting the bank via the call centre, the DP Law clarification text had been presented to the data subject. Similarly, when the data subject had applied from the "Contact Us" section of the data controller's website, and in the documents sent by the data controller, the data subject had checked the box stating "I have read and understood the information regarding the DP Law". Therefore, there no action was to be taken under the DP Law in relation to the allegation that the obligation to inform had not been fulfilled.

C. EXPECTED DEVELOPMENTS

The Turkish Data Protection Law in 2023 | Developments in Practice Over its Seven Years

I. Amendment on the Law

The Human Rights Action Plan ("Plan") published by the Ministry of Justice in April 2021, foresees that the DP Law would be harmonized with EU standards within one year. In addition, it was stipulated in the 11th Development Report that DP Law would be harmonized with the EU legislation. Under these regulations, a working group was established in September 2022, accompanied by the Ministry of Justice, and work was completed on the legislative amendments expressed by the Board at the Wednesday Seminars last year. This matter has been announced by the Minister of Justice, who stated that changes will be made primarily in the processing of special category of personal data and data transfers abroad. The relevant changes are expected to come into effect gradually at the end of 2022 and the beginning of 2023.

II. Regulating Data on Electronic Platforms

As stated in Section A.II.2 above, certain amendments have been made to the Regulation of Electronic Commerce imposing obligations on electronic commerce intermediary service providers above a certain volume to ensure the portability of the data obtained due to sales made by electronic commerce service providers.

III. Regulations on Data Portability

Law No 4054 on the Protection of Competition is planned to be amended to protect competition, especially in digital economies. Similar amendments have been made to the Regulation of Electronic Commerce for the same purpose (see Section A.II.2). In this context, similar to the EU's Digital Markets Act, there are regulations in relation to gateway companies in particular. Within these regulations, various regulations are planned to be made in areas where personal data can be used as an important competitive input, particularly data portability. The amendment has been shared with sector representatives and is expected to be published in 2023.

ABBREVIATIONS

11. Development Plan	T.R. Presidential 11th Development Plan (2019-2023)
Contract No. 108	Agreement on the Protection of Individuals Against Automatic Processing of Personal Data
EU	European Union
Genetic Data Draft Guideline Regulation of Electronic Commerce	Guideline on Considerations in the Processing of Biometric Data Law No. 6363 on the Regulation of Electronic Commerce
Board	Board of Personal Data Protection
Authority	Personal Data Protection Authority
DP Law	Personal Data Protection Law No 6698
TGNA	Turkish Grand National Assembly
TCC	TTurkish Penal Code No. 5237
VERBİS AI Guideline	Data Controllers Registry Information System Recommendations on the Protection of Personal Data in the Field of Artificial Intelligence
Loyalty Programmes Guideline	Draft Guideline for the Investigation of Loyalty Programmes

APPENDIX 1 Fundamental Concepts

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 of Personal Data
is data about arealperson's race, ethnicity, politicalopinion,philosophicalbelief,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 of 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 of personal data with explicit consent as a 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,takingoverormakingavailableof 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.

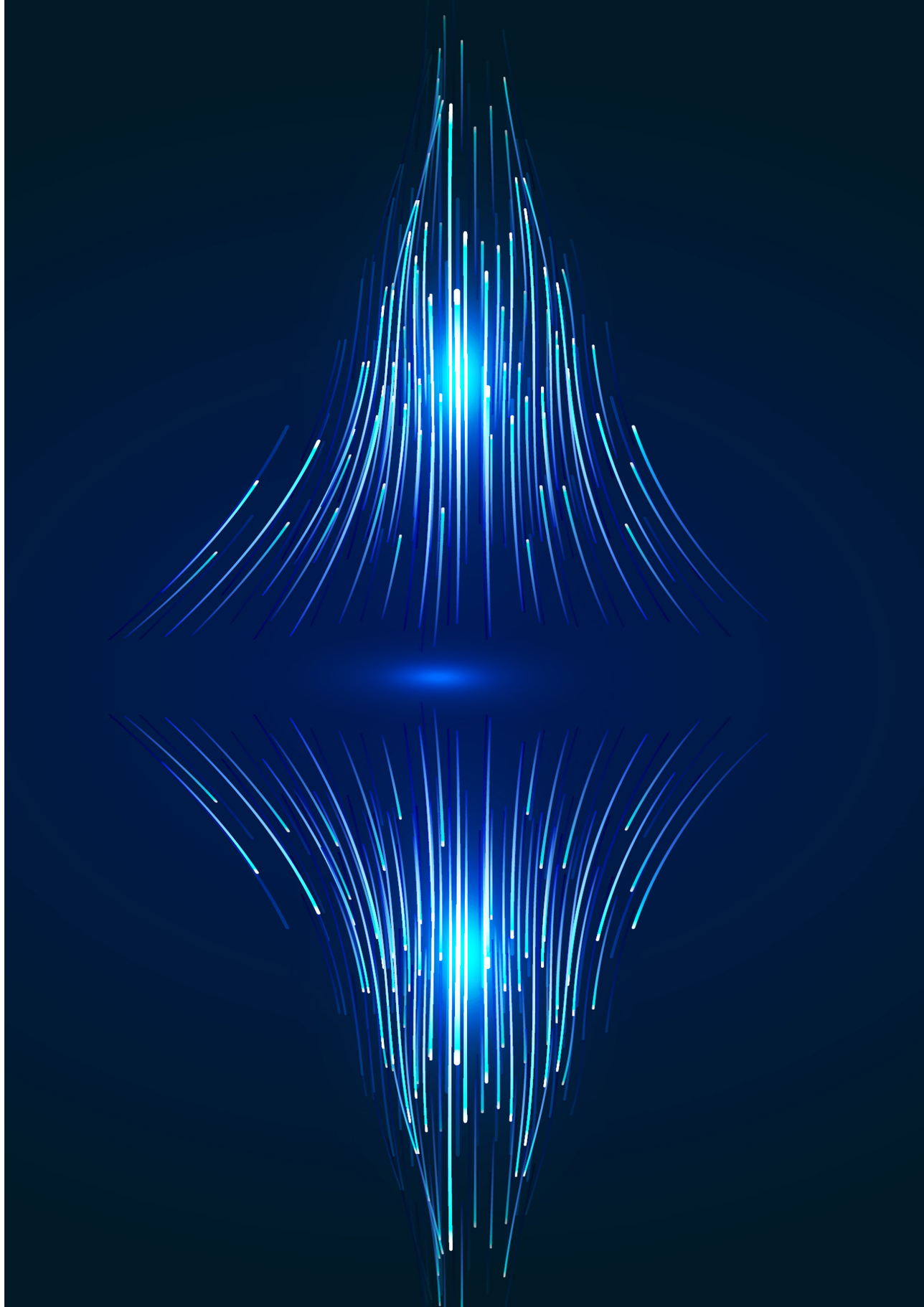
Data Controllers Registry Information System (VERBİS)
is the information system created and managed by the Presidency of the Personal Data Protection Agency, accessible over the internet, that data controllers must use in applications to the Data Controllers Registry and other related transactions.

Authors

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

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

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



MOROĞLU ARSEVEN

www.morogluarseven.com

Abdi Ipekçi Caddesi 19-1
Nişantaşı, İstanbul, 34367

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