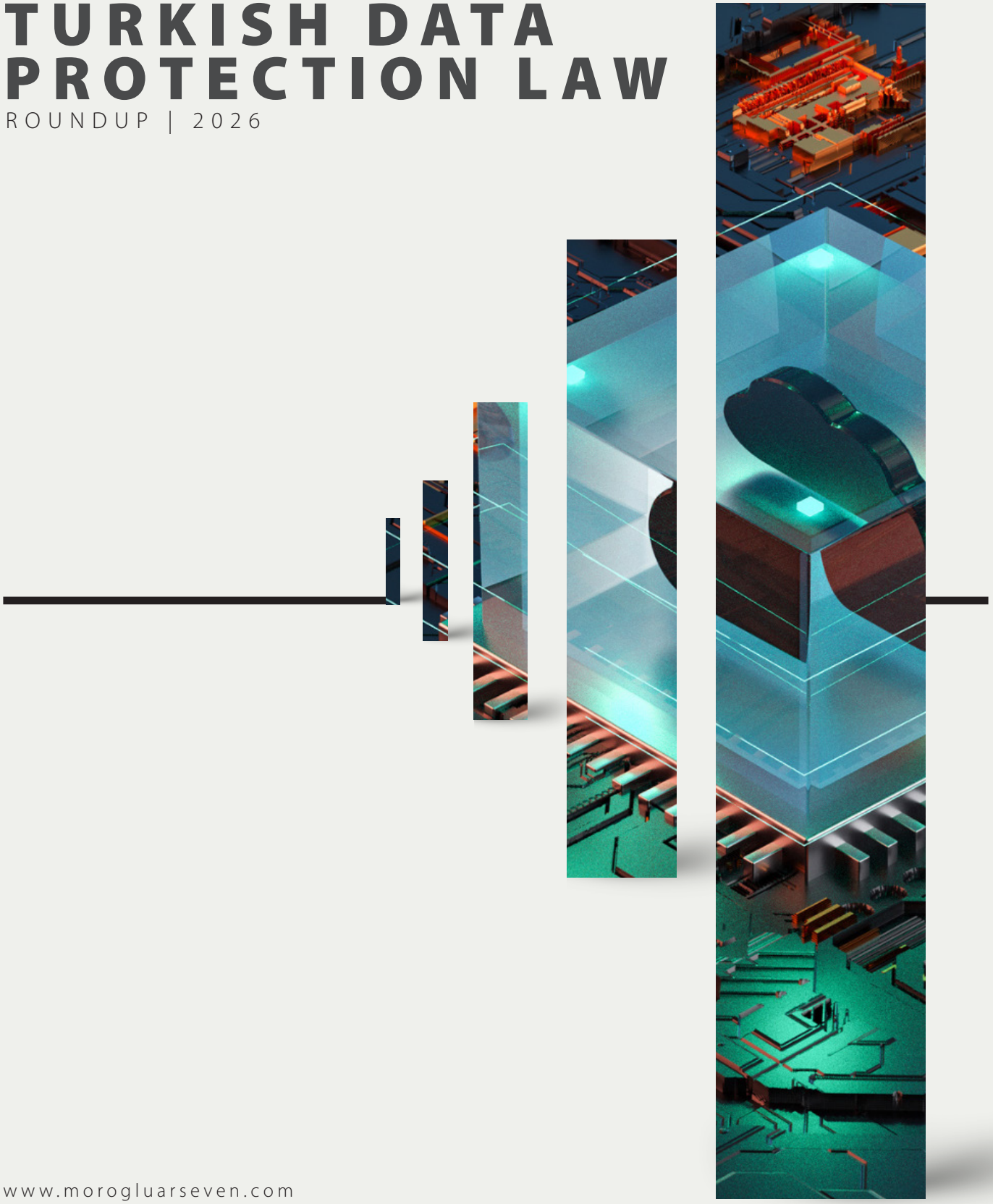
MOROĞLU ARSEVEN

TURKISH DATA PROTECTION LAW

ROUNDUP | 2026



www.morogluarseven.com

MOROĞLU ARSEVEN

Abdi İpekçi Caddesi 19-1 Nişantaşı İstanbul, 34367
www.morogluarseven.com | info@morogluarseven.com
T: +90 212 377 4700

Moroğlu Arseven is an independent, Turkish full-service law firm that combines the expertise, experience, and problem-solving capabilities of its team across all areas of economic law. Since our establishment in 2000, we have been delivering result-oriented, reliable, and practical legal solutions to our clients.

Our independence, along with the strong and trusted relationships we have established both nationally and internationally relationships that also offer flexible options enables us to closely monitor our clients' domestic and cross-border developments, and to design and implement the necessary support on a global scale.

INTRODUCTION

Since the entry into force of Law No. 6698 on the Protection of Personal Data, our study titled "Turkish Data Protection Law Roundup 2026", prepared by Moroğlu Arseven and shared with you this year, comprehensively addresses the matters that should be taken into consideration during the compliance process with the Law on the Protection of Personal Data, the legislative amendments, practices, and the approach of the Personal Data Protection Board throughout the period 1 January 2025 – 31 December 2025.

As the Personal Data Protection Authority's 2025 Annual Activity Report has not yet been published, this study has been prepared on the basis of (i) the data included in the Authority's 2024 Annual Activity Report with respect to official statistics concerning 2025, and (ii) the public announcements, studies, and Board decisions published on the Authority's official website as of the date of publication. Following the publication of the official data regarding 2025, the study will be updated and additionally shared.

Should you request further information or a detailed legal assessment regarding the matters addressed within the scope of this study, please contact us so that we may discuss in more detail.

TABLE OF CONTENTS

A. DEVELOPMENTS IN LEGISLATION AND PRACTICE

OVERVIEW OF LEGISLATION ON THE PROTECTION OF PERSONAL DATA

Personal data are afforded protection under Turkish law through various legal sources, primarily the Constitution of the Republic of Türkiye. However, the principal and comprehensive regulation governing the protection of personal data in line with the modern international regulatory approach was introduced through Law No. 6698 on the Protection of Personal Data ("**DP Law**"). With the entry into force of the DP Law, the rules governing the lawful processing of personal data were established, thereby providing clarity—both in terms of interpretation and implementation—to numerous legal regulations, most notably the provisions on the protection of personal data set forth under the Turkish Penal Code No. 5237 ("**TPC**").

Pursuant to the DP Law, the Personal Data Protection Authority ("**Authority**"), which enjoys administrative and financial autonomy and has legal personality under public law, was established with regulatory and supervisory administrative powers. The Authority carries out its activities through a structure consisting of its decision-making body, the Personal Data Protection Board ("**Board**"), and the Presidency.

Following the entry into force of the DP Law, secondary legislation has been enacted, including, in particular, the Regulation on the Data Controllers' Registry, the Regulation on the Deletion, Destruction or Anonymization of Personal Data, the Communiqué on the Procedures and Principles of Application to the Data Controller, the Communiqué on the Procedures and Principles to Be Followed in Fulfilling the Obligation to Inform, the Communiqué on the Procedures and Principles Regarding the Personnel Certification Mechanism, and the Regulation on the Procedures and Principles Regarding the Transfer of Personal Data Abroad. In addition, the Authority guides practice in the field of personal data protection law through its guidelines, public announcements, and decisions rendered within the scope of its supervisory activities.

2 LEGISLATION AND REGULATIONS ON DATA PROTECTION AND PRIVACY

In order to enhance alignment with the General Data Protection Regulation ("**GDPR**") applied within the European Union ("**EU**"), the long-anticipated comprehensive amendments to the DP Law entered into force on 1 June 2024.

Through these amendments, the legal grounds for the processing of special categories of personal data and the regulatory framework governing the transfer of personal data abroad were restructured; as a result, the applicable legal bases and compliance obligations for data controllers have undergone significant changes. Detailed information regarding the scope of these amendments and their potential implications in practice was extensively addressed in our fifth issue.[1]

1. Developments in the Field of Artificial Intelligence

1.1. Bill on Amendments to Certain Laws Introducing New Regulations on Artificial Intelligence Applications

In Türkiye, the regulatory process in the field of artificial intelligence has been shaped through the 2021–2025 National Artificial Intelligence Strategy, which set out the fundamental objectives and the governance framework, and the 2024–2025 Artificial Intelligence Action Plan, which planned the steps for the implementation of this framework.

Against this background, the first Draft Artificial Intelligence Law[2], published on 24 June 2024, set out, at draft level, the primary regulatory areas concerning artificial intelligence systems.

At the next stage of the process, the "Bill on Amendments to Certain Laws", dated 7 November 2025, which includes provisions on the use of artificial intelligence technologies (the "**Artificial Intelligence Bill**"), was submitted to the Grand National Assembly of Türkiye ("**GNAT**") and brought onto the legislative agenda with a view to enacting regulations on artificial intelligence.

Within this scope, the Artificial Intelligence Bill envisages amendments to the following principal laws:

- TPC
- DP Law
- Law No. 5651 on the Regulation of Publications Made on the Internet ("**Internet Law**")
- Electronic Communications Law No. 5809 ("**ECL**")
- Cybersecurity Law No. 7545 ("**Cybersecurity Law**")

The Artificial Intelligence Bill aims to clearly define, at the statutory level, the legal nature and scope of artificial intelligence systems, to establish effective and swift intervention mechanisms in relation to content generated by or reproduced through the use of artificial intelligence, and to support such mechanisms with an appropriate sanctions regime.

Within this framework, transparency obligations aimed at informing users are envisaged, particularly with respect to deepfake content; furthermore, it is rendered mandatory that the datasets used in artificial intelligence systems be created and utilized in compliance with the principles of data security, non-discrimination, and lawfulness.

In addition, it is intended to introduce differentiated technical and administrative obligations for service providers and artificial intelligence developers, depending on the nature of the risk involved; in high-risk use scenarios, the operation of human oversight, traceability, and accountability mechanisms is envisaged. The Bill further seeks to clarify the areas of liability arising from the use of artificial intelligence in terms of criminal law and electronic communications legislation, thereby aiming to establish a more predictable and practicable framework for the allocation of responsibilities among users, developers, and service providers.

[1] For further details, see, https://www.morogluarseven.com/wp-content/uploads/2025/01/Turkish-Data-Protection-Law-2024_Moroglu-Arseven.pdf
[2] For further details, see https://www.morogluarseven.com/wp-content/uploads/2025/01/Turkish-Data-Protection-Law-2024_Moroglu-Arseven.pdf

Nevertheless, the aforementioned regulations have not yet completed the legislative process and, accordingly, do not currently constitute binding norms in force.

1.2. Digital Copyright Bill

The Digital Copyright Bill, consisting of 13 articles and submitted to the GNAT on 11 December 2025, which also addresses the concept of artificial intelligence, aims to reassess copyright law applicable to content circulated through digital platforms in line with the new risks and needs arising from the platform economy and artificial intelligence–assisted production models. Within the Digital Copyright Bill, a comprehensive regulatory framework is proposed, particularly with a view to strengthening the legal position of copyright holders and journalists in the face of the reproduction and commercialization of news content in digital environments.

Within this framework, the Digital Copyright Bill subjects the use of news content by search engines and digital platforms to a contract-based licensing regime and envisages that a certain portion of the economic value arising from such licensing relationships be transferred directly to content producers. Furthermore, with respect to large-scale platforms exceeding a certain user threshold, the Bill introduces proactive technical measures aimed at preventing copyright infringements, institutional transparency obligations, and standardized notice-and-takedown procedures, while compliance obligations for smaller-scale service providers are addressed within a gradual and proportionate framework.

The Digital Copyright Bill also sets out the fundamental principles regarding authorship, copyright protection, and revenue sharing in the context of artificial intelligence–assisted content production, and envisages institutional structures for oversight and dispute resolution in this field. In this respect, the establishment of a Copyright Monitoring Authority and a Copyright Dispute Arbitration Commission is envisaged, together with the imposition of graduated administrative sanctions, calculated on the basis of Türkiye-sourced revenues, on intermediary service providers in cases of non-compliance with the prescribed obligations.

2. Legislative Developments in the Field of Cybersecurity[3]

Cybersecurity Law entered into force upon its publication in the Official Gazette on 19 March 2025. By defining, at the statutory level, the duties, powers, and responsibilities of the Cybersecurity Presidency ("**Presidency**"), which was established pursuant to Presidential Decree No. 177 dated 8 January 2025, the Cybersecurity Law establishes a centralized and binding administrative structure in the field of cybersecurity.

The fundamental approach of the regulation is to address cybersecurity not merely as a field limited to technical measures, but as a public policy matter directly linked to public order, national security, and the continuity of critical services. Within this scope, the Law envisages nationwide coordination, early warning and response mechanisms aimed at preventing and mitigating cyber threats, as well as minimum information security standards and regular audit processes.

Cybersecurity Law also introduces obligations for natural and legal persons conducting activities through information systems. Accordingly, the prompt notification of cyber incidents and vulnerabilities, acting in cooperation with the Presidency, and subjecting certain activities to certification or authorization processes are established as core requirements. In addition, the supervisory and audit powers applicable to companies operating in the field of cybersecurity, as well as to the products and services offered by such companies, have been expanded. Where the prescribed obligations are breached, a multi-layered sanctions regime is introduced, including high administrative fines and custodial sentences, depending on the nature of the violation. In this respect, the Cybersecurity Law constitutes a framework law governing cybersecurity in Türkiye, as it jointly regulates administrative, technical, and criminal enforcement mechanisms.

Pursuant to Presidential Decree No. 192 dated 25 December 2025, the scope of the duties and powers of the Presidency was restructured so as to encompass, in addition to cybersecurity, digital government policies, public information technology infrastructures, data governance, and artificial intelligence applications in the public sector. Within this scope, the duties of the Presidency were also defined to include the conduct of legislative activities in the fields of digital government and cybersecurity; the preparation of national policies, strategies, and action plans; the coordination and monitoring of implementation; the alignment of national legislation with international regulations; and the determination of administrative, financial, and technical principles and standards regarding information technology products, services, and systems to be used by public institutions. Furthermore, the development and operation of the e-Government Gateway and shared digital products and services, the determination of project management standards for public information technology projects, and the provision of opinions to the Presidency of Strategy and Budget with respect to financial and technical aspects were also brought within the scope of the Presidency's authority.

By establishing centralized governance and standard-setting authority in the field of artificial intelligence within the public sector, the following duties have been vested in the Presidency:

- conducting legislative and policy activities relating to artificial intelligence;
- determining data governance principles and standards covering the entire data lifecycle, from creation to disposal;
- establishing and operating a common data space infrastructure; and
- granting compliance approval with data quality standards to be applied in public-sector artificial intelligence applications.

The organizational structure of the Presidency has been restructured to consist of a President, three Vice Presidents, and service units; it is further envisaged that up to seven domestic representative offices may be established, that an overseas organization may be formed, and that companies may be incorporated domestically or abroad within the scope of its mandate. In this context, the following units have been established: (i) the Directorate General for Public Artificial Intelligence, (ii) the Directorate General for Digital Government, (iii) the Directorate General for Administrative Services, and (iv) the Department of Strategy Development.

Secondary legislation regarding cybersecurity is expected to be enacted during 2026.

[3] For further details, see https://www.morogluarseven.com/news-and-publications/cybersecurity-law-has-been-published/

3. Regulations Concerning Health Data

3.1. Regulation on Private Healthcare Institutions Providing Outpatient Diagnosis and Treatment

The Regulation on Private Healthcare Institutions Providing Outpatient Diagnosis and Treatment, published on 19 April 2025, regulates the obligations regarding the processing of personal health data applicable to private medical practices, medical centers, and polyclinics, within an implementation-oriented framework aligned with the DP Law.

In this respect,

- It has been rendered mandatory that patient data be stored electronically solely through health information management systems registered with the Ministry of Health; furthermore, the transfer of personal health data to the central health data system, as well as record-keeping and notification obligations, have been regulated.
- Obligations relating to the confidentiality, integrity, and access security of medical records have been detailed; processes concerning the confirmation of the official document status of electronically signed records, as well as backup, archiving, and authorization, have been restructured within the framework of the DP Law.
- protection of the confidentiality and integrity of forensic case and report records has been regulated; in this respect, it is stipulated that reports may not be altered after approval, that access be limited to the responsible manager or persons authorized thereby, and that certified copies be shared only in response to official requests.

3.2. Regulation Amending the Regulation on Private Health Insurance[4]

The Regulation Amending the Regulation on Private Health Insurance, published in the Official Gazette dated 20 October 2025, restructures the framework governing the processing of personal data in private health insurance practices so as to ensure alignment with the DP Law.

Pursuant to these amendments, the following changes have been introduced:

- In the process of concluding and assessing private health insurance contracts, insurance companies are enabled to obtain data from treatment providers, the Insurance Information and Monitoring Center, and public institutions; accordingly, the requirement to obtain the insured's written consent has been abolished.
- Restrictions on access to the insured's medical history have been limited solely to cases of legal or technical impossibility.
- The individual-based retention of health information and insurance records has been rendered independent of any written consent requirement.
- The requirement to obtain explicit consent for data transfers to third parties has been abolished, and compliance with the DP Law and secondary legislation has been adopted as the governing principle.
- A retention period of ten (10) years has been stipulated for personal data held by the Insurance Information and Monitoring Center, starting from the termination of the insurance relationship.
- It has been stipulated that the duty of confidentiality shall continue even after the termination of the status of being an insurer.

The amendments entered into force on 1 January 2026.

3.3. Regulation Amending the Regulation on Personal Health Data[5]

The Regulation Amending the Regulation on Personal Health Data, published in the Official Gazette dated 3 December 2025, revisited the existing framework governing the processing of and access to personal health data so as to ensure alignment with the amendments introduced as of March 2024 regarding the processing of special categories of personal data under the DP Law.

Under the amendments, the provision requiring the inclusion of explicit consent in a power of attorney for lawyers' access to their clients' health data has been abolished. Prior to this amendment, the 10th Chamber of the Council of State had rejected the request for annulment of the regulation requiring explicit consent in the power of attorney for lawyers' access to their clients' health data, holding that the regime governing the protection of personal health data should be assessed within the scope of special legislation, and accepting that the DP Law sets out the fundamental framework in this field.

In addition to the amendment concerning lawyers' access to health data: ***(i)*** it has been stipulated that the regime applicable to the processing of historical health data shall be based on the lawful processing conditions set forth under the DP Law; ***(ii)*** healthcare professionals' access to personal health data has been concretized through objective, proportionate, and identifiable criteria linked to the nature of the service and the scope of duty; and ***(iii)*** the implementation principles regarding access to children's health data, the security preferences determined via the e-Nabız system, and physicians' data access authorizations have been updated.

4. Amendment Regarding the Data Protection Personnel Certification and Authorization Regime

With its decision numbered 2025/2023, the 10th Chamber of the Council of State annulled the Communiqué on the Procedures and Principles Regarding the Personnel Certification Mechanism published by the Authority.

In its decision, the Court held that the regulation concerning the "Data Protection Officer Certification Program" established a status not envisaged under the DP Law; that no statutory authority had been granted to the Board with respect to the definition and certification of a data protection officer; and that the regulation did not fall within the scope of the Authority's statutory duties. Furthermore, it was assessed that the said program constituted an excess of authority insofar as it concerned activities that may be carried out exclusively by attorneys pursuant to Article 35 of the Attorneyship Law.

5.Regulation-Based Developments in National Education Practices

As of 1 December 2025, biometric identity verification and camera-assisted monitoring systems have been implemented in private special education and rehabilitation centers. As part of the implementation, the entry and exit movements of students and staff, as well as class attendance, have begun to be monitored through biometric verification; facial recognition data were registered in the system through Guidance and Research Centers by 1 September 2025. As part of the implementation, students, parents, and staff were duly informed, and explicit consent processes compliant with the DP Law were carried out. The system operates in an integrated manner with the information technology infrastructure of the Ministry of National Education; the data are stored both by the relevant institutions and within the Ministry of National Education, while camera recordings at entry and exit points are retained for a minimum period of ninety (90) days.

[4] For further details, see https://www.morogluarseven.com/news-and-publications/the-regulation-amending-the-private-health-insurance-regulation-has-been-published/
[5] For further details, see https://www.morogluarseven.com/news-and-publications/the-regulation-amending-the-regulation-on-personal-health-data-has-been-published/

6. Developments under the Internet Law

On 3 December 2025, the Bill on Amendments to the Law on the Regulation of Publications Made on the Internet and the Combating of Crimes Committed through Such Publications, which envisages amendments under the Internet Law, was submitted to the GNAT.

Under the Bill, it is rendered mandatory that all audio, written, and visual content generated through the use of artificial intelligence, or giving the impression of having been generated by artificial intelligence, be presented with an artificial intelligence label that enables users to clearly and unambiguously distinguish such content. In the event that this obligation is breached, particularly where deepfake content is published, it is envisaged that content producers may incur criminal liability pursuant to Article 217/A of the TPC.

In the rationale of the Bill, it is emphasized that artificial intelligence–generated fake content undermines individuals' reputations, has the potential to manipulate public perception, and poses serious risks to public order. While it is noted that the absence of an explicit obligation under the current legislation to label artificial intelligence–generated content creates a significant legal gap, the proposed regulation aims to enhance transparency and accountability within the digital content ecosystem.

7. Recent Developments in the Legislation on Family and Social Services

The Regulation on Data Sharing of the Ministry of Family and Social Services, which entered into force upon its publication in the Official Gazette dated 15 February 2025, sets out the procedures and principles governing the sharing of personal data held within the Ministry of Family and Social Services, within the framework of the DP Law. While regulating online and offline data-sharing methods, the regulation is based on the conduct of data processing and transfer activities in compliance with the principles of lawfulness, purpose limitation, and data security.

Under the regulation, a Data Sharing Board has been established within the Ministry of Family and Social Services to assess data sharing requests; furthermore, data security, confidentiality, and data destruction obligations applicable to recipient institutions and individuals benefiting from data sharing have been explicitly stipulated. With respect to acts contrary to the protection of personal data, the existing criminal liability regime has been preserved by reference to the DP Law and the relevant legislation.

8. Recent Developments in Road Traffic Legislation

With the Regulation Amending the Road Traffic Regulation, published in the Official Gazette dated 19 August 2025, new obligations concerning security and monitoring infrastructure have entered into force for certain categories of commercial vehicles.

As part of the implementation, it has become mandatory for commercial vehicles—such as taxis, shared taxis, urban buses, and school and personnel service vehicles—to be equipped with a vehicle tracking system, cameras and image recording devices, and an emergency button. While these obligations apply immediately to newly registered vehicles, a phased transition schedule based on the model year has been envisaged for vehicles already registered in traffic:

- for 2023–2025 model vehicles, the obligations shall apply at the first inspection conducted after 1 January 2026;
- for 2018–2022 model vehicles, at the first inspection conducted after 1 January 2027;
- for 2017 and earlier model vehicles, at the first inspection conducted after 1 January 2028; and
- for vehicles registered as school service vehicles between 18 February 2025 and 1 October 2025 and already equipped with camera and recording systems compliant with the previous regulation, the new obligations shall apply at the first inspection conducted after 31 December 2027.

3

DOCUMENTS PUBLISHED AND UPDATED BY THE AUTHORITY IN 2025

1. Updated Information Notes

No new information notes were published by the Authority during 2025.

Within the scope of the existing documents, the following materials were updated based on the 2024 amendments to the DP Law:

- Deepfake Information Note;
- Law No. 6698 on the Protection of Personal Data with Its Articles and Justifications (Information Note) and the Glossary of Terms on the Protection of Personal Data; and
- Information Note on the Personal Data Processing Condition of Being Prescribed by Law.

2. Bulletins

During 2025, the Authority published three DP Law Bulletins.

- **December 2024 – February 2025, Issue No. 7** – Published under the title "Convention No. 108 and Data Protection Day", this bulletin addresses international standards in the field of data protection within the framework of the Council of Europe Convention No. 108, current practices under Convention No. 108, and assessments concerning the institutionalization of the data protection culture.
- **March – May 2025, Issue No. 8** – The bulletin titled "An Overview of Artificial Intelligence" examines the risk areas posed by artificial intelligence technologies from the perspective of personal data protection law; algorithmic decision-making processes, automated processing, and their relationship with the principles of the DP Law are evaluated in general terms.
- **June – August 2025, Issue No. 9** – The issue themed "Protection of Personal Data on Social Media" aims to raise awareness regarding the protection of personal data in the context of data processing activities carried out on social media platforms, user behavior, visibility settings, and third-party access; the rights and obligations of individuals are explained through practical examples.

4

GUIDELINES

1. Guidelines on Generative Artificial Intelligence and the Protection of Personal Data[6]

The Guidelines on Generative Artificial Intelligence and the Protection of Personal Data, published by the Authority on 24 November 2025 (the "**GenAI Guidelines**"), assess the impacts of generative artificial intelligence ("**GenAI**") systems on personal data within the framework of the DP Law and set out fundamental principles for practice.

The main points highlighted under the GenAI Guidelines may be summarized as follows:

- Fundamental concepts relating to the GenAI ecosystem (including large language models, profiling, synthetic data, black box, and privacy-enhancing technologies, among others) are defined in light of international standards and regulatory approaches.
- GenAI systems are addressed as structures trained on large datasets and capable of generating text, images, audio, video, or code based on user inputs.
- It is emphasized that legal, ethical, and societal impacts should be jointly assessed throughout all stages of the GenAI lifecycle (design, training, deployment, and improvement).
- Risks specific to the use of GenAI are identified under headings such as inaccurate outputs, bias and discrimination, unintended data processing, intellectual property infringement, and manipulation.
- It is stated that personal data within the scope of GenAI should be processed only for specific, explicit, and legitimate purposes, and in a manner that is relevant, limited, and proportionate to such purposes.
- It is noted that the distinction between data controller and data processor should be determined based on actual control and the data lifecycle, irrespective of contractual designations.
- It is emphasized that a legal basis must be determined separately for each data processing activity within GenAI processes, and that reliance on legitimate interest is subject to a balancing test.
- It is stated that the processing of special categories of personal data within the scope of GenAI entails high risks, and that enhanced technical and administrative measures are mandatory to mitigate such risks.
- It is emphasized that cross-border transfers of personal data within GenAI systems must be carried out in compliance with Article 9 of the DP Law and the relevant secondary legislation.
- Transparency is underlined as a fundamental obligation, and it is stressed that users must be able to clearly understand when they are interacting with a GenAI system.
- It is stated that the data subject rights set out under Article 11 of the DP Law are equally applicable to GenAI systems, and that the possibility of human intervention must be ensured in automated decision-making processes.
- It is emphasized that data security should be addressed within the framework of privacy by design and by default, taking into account GenAI-specific attacks and vulnerabilities.
- Users are advised to avoid entering sensitive personal data into GenAI systems and to carefully manage privacy settings.
- It is emphasized that, in interactions between children and GenAI systems, age-appropriate content controls and parental guidance are required.

2. Guidelines on Good Practices Regarding the Protection of Personal Data in the Payment and Electronic Money Sector[7]

The Guidelines on Good Practices Regarding the Protection of Personal Data in the Payment and Electronic Money Sector (the "**Payment and Electronic Money Sector Guidelines**") were published by the Authority on 11 April 2025, in cooperation with the Turkish Payment and Electronic Money Institutions Association.

In this respect, the Guidelines aim to concretize the obligations of payment institutions and electronic money institutions operating pursuant to Law No. 6493 on Payment and Securities Settlement Systems, Payment Services and Electronic Money Institutions ("**Law No. 6493**") under the DP Law, by taking into account sector-specific business models and operational structures.

The main points highlighted in the Payment and Electronic Money Sector Guidelines are as follows:

- Role allocation, including the qualification of parties, is determined based on the nature of the payment service; it is acknowledged that the same actor may act as a data controller or a data processor depending on the specific service provided. The Guidelines emphasize that data processing relationships with operational support units,

[6] For further details, see https://www.morogluarseven.com/news-and-publications/13740/
[7] For further details, see https://www.morogluarseven.com/tr/news-and-publications/13475/

such as call centres, IT service providers and similar entities, must be governed by written data processing agreements

- The scope of data subjects is limited to users who are direct parties to the payment service; individuals whose data are processed indirectly during the payment process are classified as "silent parties", and it is stated that their data may be processed solely to the extent necessary for the performance of the transaction.
- Data categories are classified on a service-specific basis, primarily including identity data, contact details, financial information, transaction security data and customer transaction records. It is noted that a significant portion of these data categories arise from obligations under banking legislation and the regulations of the Financial Crimes Investigation Board ("**FCIB**").
- Legal grounds for processing are explained through sector-specific examples, and it is stated that data processing activities aimed at preventing fraud and ensuring transaction security may be carried out on the basis of legitimate interest.
- Data transfers are addressed by distinguishing between domestic transfers carried out vis-à-vis FCIB and the Central Bank of the Republic of Türkiye ("**CBRT**"), and cross-border transfers falling within the scope of Article 9 of the DP Law. In cross-border data transfers, compliance with the principle of proportionality and the requirement to maintain primary systems within Türkiye is expressly reiterated.
- Data security and audits are assessed together with the data security obligations under Article 12 of the DP Law and the domestic data localisation and long-term record-keeping obligations under Law No. 6493. The Guidelines underline that the protection of personal data constitutes a core audit focus in both CBRT supervisory activities and independent audit processes.

3. Guidelines on the Processing of Special Categories of Personal Data

The Guidelines on the Processing of Special Categories of Personal Data, published by the Authority on 26 February 2025 (the "**Special Categories Guidelines**"), were prepared with the aim of explaining the procedures, principles, and obligations set out under Article 6 of the DP Law, which was amended as of March 2024 and governs the conditions for the processing of special categories of personal data.

As stated in the rationale of the DP Law, the Special Categories Guidelines indicate that special categories of personal data are subject to a strict protection regime, given their nature, which may give rise to discrimination or victimization of the data subject if disclosed.

The Special Categories Guidelines emphasize that the scope of special categories of personal data is exhaustively defined under Article 6 of the DP Law and that this scope may not be expanded by way of analogy. In this respect, the following data are considered to fall within the scope of special categories of personal data: ***race and ethnic origin, political opinion, philosophical belief, religion, sect or other beliefs, dress and appearance, membership of associations, foundations, or trade unions, data relating to health and sexual life, data relating to criminal convictions and security measures, as well as biometric and genetic data.***

- The Special Categories Guidelines explain the categories of special categories of personal data through concrete and practice-oriented examples. In this respect, some of the prominent examples are as follows:

◊ Data relating to data subjects' political opinions

- Information concerning an individual's membership of a political party, being apolitical, or socio-political attitudes and behaviors is considered to fall within the scope of data relating to political opinions.
- With reference to the decision of the 12th Criminal Chamber of the Court of Cassation dated 15 May 2012, it is emphasized that, if such data become known among different segments of society, they may expose the data subject to a risk of discrimination.

◊ Health Data

- Health data are not limited solely to information relating to diagnosed illnesses; rather, they are interpreted broadly so as to cover the entire healthcare service process.
- Information such as *the hospital, clinic, or unit where an appointment is scheduled, preliminary diagnoses, requested medical tests and their results, final diagnoses, as well as prescribed medications or treatment methods* to be applied, are considered to constitute health data.
- It is explicitly stated that blood type information contained in old-type passports, driver's licenses, identity cards, or workplace identification cards also qualifies as health data and, due to its nature, constitutes special categories of personal data.

◊ Data relating to criminal convictions and security measures

- Finalized conviction judgments recorded in criminal records are considered data relating to criminal convictions and security measures and, as such, fall within the scope of special categories of personal data. However, where such data are processed by a data controller, the processing conditions set out under Article 6 of the DP Law must be complied with.

The Special Categories Guidelines place particular emphasis on the fact that, in determining when special categories of personal data may be processed lawfully, the concepts of "***necessary***" and "***mandatory***" set out in the wording of Article 6 of the DP Law are decisive.

- Necessity refers to the requirement that the processing activity be reasonable, proportionate, and objectively justifiable for the achievement of the intended purpose, and that there be a concrete link between the data processed and such purpose.
- Mandatory nature refers to situations where, in the absence of any alternative method, the processing of special categories of personal data becomes inevitable due to public or societal reasons.

Within the framework of this conceptual approach, the Special Categories Guidelines provide practical examples of data processing activities carried out within the scope of statutory obligations. Among these examples, particular reference is made to:

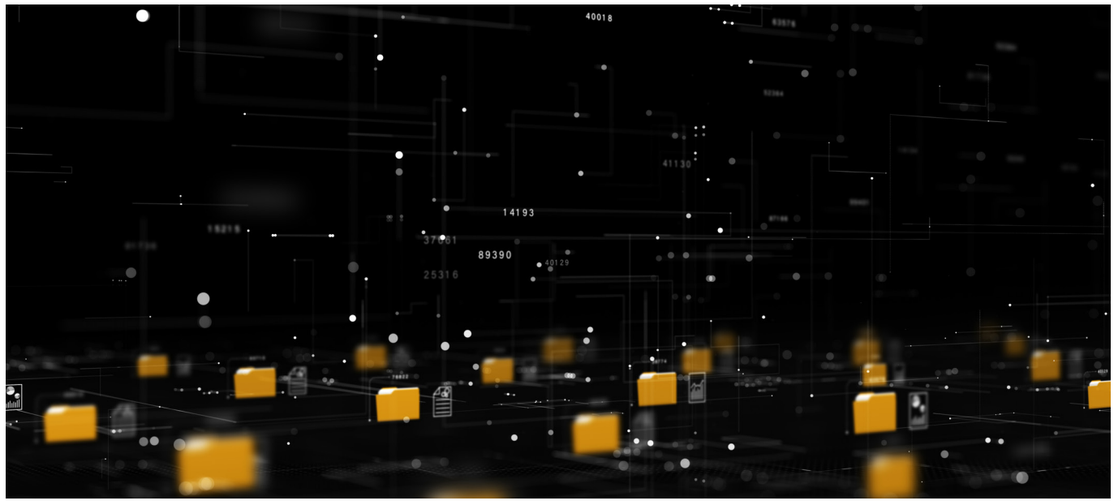
- the processing of certain health data within the scope of an employer's obligation to maintain personnel files pursuant to Labor Law No. 4857;
- the processing of data relating to criminal convictions and health data concerning drivers as required under the Road Traffic Legislation; and
- cases where individuals are subject to health examinations necessitated by the nature of the work within the framework of collective bargaining agreements.

Finally, the Special Categories Guidelines state that data controllers are required to carry out a comprehensive compliance exercise to align their personal data processing activities with the March 2024 amendments. In this regard, it is emphasized that data inventories, explicit consent mechanisms, privacy notices, retention and destruction processes, as well as the technical and administrative measures relating to special categories of personal data, should be reviewed and restructured accordingly.

4. Updated Guidelines

During 2025, the Authority updated and republished various guidelines, booklets, and practical documents. In this regard, the principal documents that were updated are as follows:

- Guide to Good Practices in the Banking Sector Regarding the Protection of Personal Data
- Guidelines on Matters to Be Considered in the Processing of Biometric Data
- Guidelines on the Fulfilment of the Obligation to Inform
- Practical Guidelines on the DP Law
- The DP Law in 100 Questions
- Recommendations on the Protection of Privacy in Mobile Applications
- Assessment of the Right to Be Forgotten with Respect to Search Engines
- Frequently Asked Questions on the DP Law
- Protection of Personal Data Through Examples
- Personal Data Security Guidelines
- Guidelines on the Deletion, Destruction, or Anonymization of Personal Data
- Guidelines on the Preparation of a Personal Data Processing Inventory
- Guidelines on Matters to Be Considered in the Processing of Genetic Data
- Guidelines on the Processing of Turkish Identity Numbers
- Booklet on the Principle Decisions of the Personal Data Protection Board
- Guidelines on Cookie Practices
- Booklet on the Fundamental Principles of Personal Data Processing
- Data Controllers' Registry Information System in Questions and the Data Controllers' Registry Information System User Guide



5

PUBLIC ANNOUNCEMENTS PUBLISHED BY THE AUTHORITY IN 2025

During 2025, the Authority published a total of five public announcements on its official website.

1. Public Announcement on the Fulfilment of the Obligation to Inform within the Scope of Mediation Activities[8]

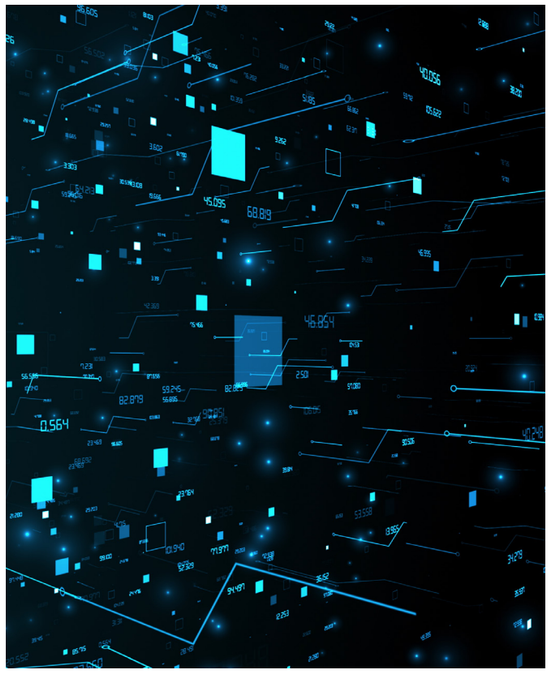
The Public Announcement on the Fulfilment of the Obligation to Inform within the Scope of Mediation Activities, published by the Authority on 13 January 2024, contains explanations regarding the processing of personal data in mediation activities carried out pursuant to Law No. 6325 on Mediation in Civil Disputes ("**Law No. 6325**") and the application of the DP Law in such processes. The announcement states that mediators act in the capacity of data controllers with respect to the personal data processed during mediation activities and, in this capacity, are subject to the obligations set out under the DP Law.

The Authority emphasizes that the mediator's obligation to inform the parties about the mediation process pursuant to Law No. 6325 differs in both scope and purpose from the obligation to inform regulated under Article 10 of the DP Law. Accordingly, it is stated that informing the parties at the outset of the mediation process does not in itself result in the fulfilment of the obligation to inform under the DP Law; rather, mediators are required to separately fulfil the obligation to inform with respect to the personal data processed within the scope of mediation activities.

2. Public Announcement on Matters to Be Considered in Standard Contracts to Be Used for the Cross-Border Transfer of Personal Data[9]

The Public Announcement on Matters to Be Considered in Standard Contracts to Be Used for the Cross-Border Transfer of Personal Data, published by the Authority on 5 February 2025, clarifies the implementation errors identified and the points requiring attention as a result of the reviews conducted by the Authority with respect to the Standard Contracts ("**SCs**") used for the transfer of personal data abroad pursuant to Article 9/5 of the DP Law. Through this announcement, the minimum formal and substantive criteria required for the legal validity of the SCs and for the proper submission of notifications to the Authority have been set out.

In this regard, the Authority emphasizes that the SCs must be signed by duly authorized persons, that the signatures must comply with the Turkish Code of Obligations ("**TCO**"), that signatures must be affixed on the Turkish-language text in contracts executed in a foreign language, and that documents evidencing signatory authority, together with their notarized Turkish translations, must be submitted to the Authority. It is further underlined that party and address information must be complete, and that notifications must be made within five (5) business days following the date of signature. In addition, it is explicitly stated that SCs must not include retroactive effect clauses, that amendments may be made only to optional provisions, and that foreign official documents must be submitted with an apostille or consular certification.



3. Public Announcement on the Use of the E-Notification System of the Revenue Administration of the Ministry of Treasury and Finance for the Service of Administrative Fines

The Public Announcement on the Use of the E-Notification System of the Revenue Administration of the Ministry of Treasury and Finance for the Service of Administrative Fines, published by the Authority on 10 June 2025, announces a change in practice regarding the method of service of administrative fines to be imposed pursuant to Article 18 of the DP Law. In this context, the protocol efforts carried out between the Authority and the Ministry of Treasury and Finance within the framework of Article 26 of the Misdemeanors Law have been completed, and the technical infrastructure enabling the electronic service of administrative sanctions has been established.

Pursuant to the announcement, notifications regarding administrative fines to be imposed under the DP Law will be served electronically on the relevant data controllers through the E-Notification System of the Revenue Administration of the Ministry of Treasury and Finance. However, it is stated that, with respect to data controllers who do not have an active taxpayer registration in the e-notification system or whose registration has been deleted, notification procedures will continue to be carried out through physical means in accordance with the provisions of Law No. 7201 on Notifications.

[8] For further details, see https://www.morogluarseven.com/news-and-publications/public-announcement-on-the-fulfillment-of-the-obligation-to-inform-in-the-scope-of-mediation-activities/

[9] For further details, see https://www.morogluarseven.com/news-and-publications/public-announcement-on-key-considerations-for-standard-contracts-in-cross-border-personal-data-transfers-issued/

4. Public Announcement on the Sharing of Debt Information by Creditors' Representatives through Access to the Telephone Numbers of Relatives of Debtor Data Subjects

On 20 August 2025, the Authority published the Public Announcement on the Sharing of Debt Information by Creditors' Representatives through Access to the Telephone Numbers of Relatives of Debtor Data Subjects.

In the said public announcement, it is summarized that:

- the sharing by creditors' representatives of personal data such as a debtor's name, surname, and debt-related information with the debtor's relatives via telephone calls or short message services (SMS) constitutes a personal data processing activity;
- the disclosure of a debtor's personal data to third parties without the explicit consent of the data subject or without reliance on a valid legal basis set out under Article 5 of the DP Law may constitute a violation of the DP Law;
- in addition to the sharing of data relating to the debtor, the processing of contact details of the debtor's relatives who are not related to the debt also constitutes a separate personal data processing activity and falls within the scope of the DP Law; and
- where such violations are identified, a breach of the data security obligations regulated under Article 12 of the DP Law may arise, and administrative fines may be imposed depending on the specific circumstances of the case.

5. Public Announcement on the Exemption Criterion Regarding the VERBİS Registration Obligation of Data Controllers Whose Main Activity Is the Processing of Special Categories of Personal Data

The Public Announcement on the Exemption Criterion Regarding the VERBİS Registration Obligation of Data Controllers Whose Main Activity Is the Processing of Special Categories of Personal Data, published by the Authority on 1 October 2025, announces that amendments have been introduced to the exemption criteria applicable to the VERBİS registration obligation of data controllers whose main activity consists of processing special categories of personal data.

Pursuant to the decision of the Board dated 4 September 2025 and numbered 2025/1572, it has been decided that data controllers whose main activity involves the processing of special categories of personal data, but who employ fewer than ten (10) employees annually and whose annual financial balance sheet total is below TRY 10 million, shall be exempt from the VERBİS registration and notification obligation.

For a detailed assessment of the relevant Board decision, please refer to B.III.1. The Board's Decision on the VERBIS Registration Obligation .

6. Public Announcement on the Implementation Principles of the Decision of the Board dated 4 September 2025 and numbered 2025/1572

Following the Decision of the Board dated 4 September 2025 and numbered 2025/1572, which was adopted to update the exemption applicable to data controllers whose main activity is the processing of special categories of personal data, the Authority published, on 12 January 2026, the Public Announcement on the Implementation Principles of the Decision of the Personal Data Protection Board dated 04.09.2025 and numbered 2025/1572, providing clarification on the application of the said exemption with respect to data controllers who do not keep books on a balance-sheet basis.

Accordingly:

i. with respect to **data controllers keeping books on a balance-sheet basis,** the criteria relating **to the number of employees and the annual financial balance sheet total shall be assessed cumulatively;** and
ii. with respect to **data controllers not keeping books on a balance sheet basis,** given the absence of data relating to the **annual financial balance sheet total, only the criterion relating to the number of employees** shall be taken into account.

6

OTHER ACTIVITIES OF THE AUTHORITY

1. Authority Publication Titled "The Personal Data Protection Authority in Its 8th Year"

On 29 December 2025, the Authority shared with the public a publication prepared under the title "The Personal Data Protection Authority in Its 8th Year" (**the "Publication"**). The Publication covers the eight-year period of activities of the Authority between 2017 and April 2025 and systematically compiles the entirety of the activities carried out by the Authority since its establishment. In this respect, the Publication provides a holistic overview of the Authority's institutional structure, legislative output, decision-making processes, and implementation-related activities.

The key statistics highlighted within the scope of the Publication are summarized below:

The Publication comprehensively addresses the regulatory framework established to date in the field of personal data protection. In this regard, **10** regulations, **4** communiqués, **8** principle decisions, **321** Board decisions, and **99** public announcements are examined in detail, and the role of these regulations and decisions in the development of the legal framework and their practical implications in the field of personal data protection are presented.

Statistics relating to a total of **49,420** notices, complaints, and applications submitted to the Authority between 2 January 2017, when the Board commenced its duties, and 30 April 2025 are included; the fact that **47,787** of these applications have been finalized enables a quantitative assessment of the functioning of the Authority's application mechanisms and its decision-making practice.[10]

The Publication examines **1,676** personal data breach notifications, and the processes relating to the public disclosure of **363** of these breaches are explained in detail. Accordingly, information is provided regarding the criteria applied in the assessment of data breach notifications, the public disclosure processes, and the procedures followed.

Data concerning administrative fines imposed as a result of examinations, amounting in total to TRY **1,052,298,513**[11] , are shared, thereby presenting a statistical overview of the Authority's sanctioning practices.

The Publication includes **59** guidelines and documents prepared for data controllers, data processors, and data subjects involved in personal data processing activities, and evaluates the information and guidance activities carried out through these documents.

Data relating to **863,250** calls handled through the ALO 198 Information and Consultation Center are also included, quantitatively demonstrating the scope of the Authority's information and advisory activities.

[10] In a statement made by the President of the Authority, Prof. Dr. Faruk Bilir, in December 2025, and reflected in publicly available news reports, it was disclosed that 56,377 out of 58,640 notices and complaint applications submitted to the Authority had been finalized.

2. Key Announcements

Under this heading, announcements published on the Authority's official website that have an impact on the procedures and principles regarding the protection of personal data are addressed.

2.1. Amounts of Administrative Fines

On 31 December 2025, the Authority published on its official website the updated amounts of administrative fines regulated under Article 18 of the DP Law, which were increased for 2026 in accordance with Article 17/7 of the Misdemeanors Law, effective as of the beginning of each calendar year, by applying the revaluation rate determined and announced for 2026 pursuant to Repeated Article 298 of the Tax Procedure Law No. 213, in the amount of 25.49%. Further details are set out in the table below:

DP LAW ARTICLE	VIOLATED DP LAW ARTICLE	DESCRIPTION	ADMINISTRATIVE FINE AMOUNTS FOR 2026 (TRY)
18/a	10	Failure to fulfil the obligation to inform	85,437 ₺ – 1,709,200 ₺
18/b	12	Failure to fulfil data security obligations	256,357 ₺ – 17,092,242 ₺
18/c	15	Failure to comply with Board decisions	427,263 ₺ – 17,092,242 ₺
18/ç	16	Non-compliance with the VERBİS registration obligation	341,809 ₺ – 17,092,242 ₺
18/d	9	Failure to notify the Board of the SCs	90,308 ₺ – 1.806.177 ₺

2.2.Announcements Regarding Commitment Applications

During 2025, the Board reviewed and resolved three commitment applications, and the relevant decisions were published on the Authority's official website. In this regard, three commitment applications submitted by VF Ege Giyim Sanayi ve Ticaret Limited Şirketi in relation to the cross-border transfer of personal data were found appropriate by the Board.

2.3. Announcement on Granting Permission for the Cross-Border Transfer of Personal Data Based on an Agreement Not Qualifying as an International Treaty

The Authority announced that, by way of the Decision of the Board dated 21 October 2025, permission was granted for the cross-border transfer of personal data within the framework of an arrangement signed between the Directorate General of Migration Management of the Ministry of Interior and the Office of the United Nations High Commissioner for Refugees, which does not qualify as an international treaty. The said decision constitutes the first permission granted under the new cross-border data transfer regime that entered into force in 2024.

3. Other Activities

The Authority continued in 2025 its Wednesday Seminars, which it has been organizing since 2018, as well as its podcast series titled "A Small Awareness Is Enough", which has been ongoing since 2021. In addition, throughout 2025, the Authority organized numerous symposia, seminars, workshops, trainings, visits, and events.

Some of these activities include:

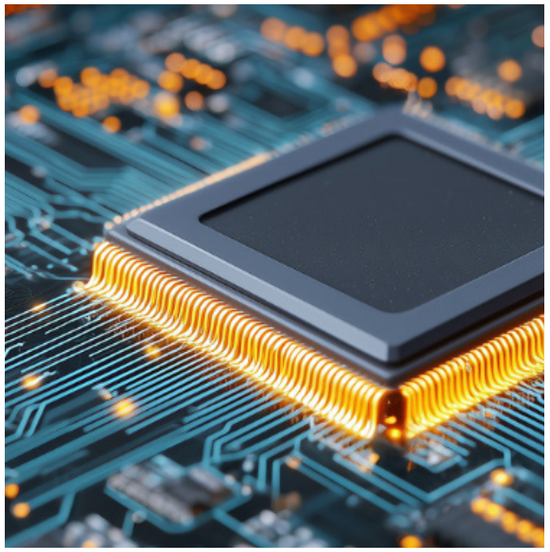
- 44 Years of Data Protection: The Age of Artificial Intelligence from a Privacy Perspective
- 28 January Data Protection Day Event
- Symposium on Current Developments in the DP Law
- Amendments to Personal Data Protection Legislation: New Dynamics and Legislative Compliance Workshop
- Personal Data and Legal Updates: 2025 Perspective Event
- Conference on the DP Law and Its Implementation
- Workshop on the Guide to Good Practices Regarding the Protection of Personal Data in the Payment and Electronic Money Sector
- Symposium on Digital Games and the Protection of Personal Data
- Launch Event: An Academic Perspective on Artificial Intelligence Technologies
- e-Safe Personal Data Protection Summit
- Conference on the Protection of Personal Data in the Age of Artificial Intelligence
- 2nd National Symposium on the Protection of Personal Data
- The Digital Shield of the Future: Cybersecurity and the Protection of Personal Data Event
- Data, Artificial Intelligence, and Law Event
- 10 December Human Rights Day (Symposium on the Right to Privacy and the Protection of Personal Data)
- Selected Current Developments
- Glossary of Terms
- Academic Perspective Publications
- Advisory Content
- Key Considerations
- Cybersecurity Awareness Month

Wednesday Seminars

- Institutionalization of Human Rights: National Human Rights Institutions
- Protection of Personal Data and Artificial Intelligence: Risks and Solutions
- Protection of Children's Personal Data: An Assessment in the Context of Social Media
- The Legal Dimension of Generative Artificial Intelligence: Current Developments and Risks
- Administrative Fines in Personal Data Protection Law
- Assessment of the Legitimate Interest of Data Controllers under the DP Law and the GDPR
- Protection of Personal Data in Law Enforcement Activities
- Personal Data Protection and Privacy in Digital Identity Regulations
- Data Breach Notifications under Law No. 6698
- Assessment of the DP Law & GDPR and Judicial Decisions in the Context of National Security
- The Personal Data Protection Authority as an Independent Administrative Authority
- Assessment of Data Subject Rights under Law No. 6698 in Comparison with the GDPR
- Personal Data Processing Activities Carried Out by Attorneys
- Artificial Intelligence-Based Operations and Activities That May Give Rise to Criminal Liability in Relation to Personal Data
- Data Protection Impact Assessment in the Protection of Personal Data
- Implementation of the Right to Erasure in Artificial Intelligence Systems
- Protection of Personal Data in the Asia-Pacific Region
- Protection of Personal Data in Surveillance Technologies
- The Role of Privacy-Enhancing Technologies in a Data-Protection-Compliant Artificial Intelligence Ecosystem
- Privacy-Enhancing Technologies: Federated Learning and Edge Artificial Intelligence
- Artificial Intelligence and Criminal Law Liability

Projects and Programs

- Digital Literacy Project for a Secure Future
- Project for Training Personal Data Protection Volunteers among University Students
- Awareness Seminars



7

DECISIONS OF THE CONSTITUTIONAL COURT

— 1 —

Constitutional Court's Decision with Application No. 2020/19835 and Decision Date 15 January 2025

(Abdulhalim Altun Application)

In its decision docketed No. 2020/19835 and dated 15 January 2025, the Constitutional Court ruled that the use of personal data obtained within the scope of a security clearance and archive research as a decisive factor in appointments to public office constitutes a violation of the right to request the protection of personal data, which is safeguarded under Article 20 of the Constitution. In the case at hand, the applicant, who had been placed in the position of "data preparation and control operator" at a municipality based on the results of the Public Personnel Selection Examination ("**KPSS**"), was not appointed on the grounds that the security clearance conducted in respect of the applicant yielded a negative result. Following the exhaustion of judicial remedies, the applicant filed an individual application before the Constitutional Court.

In its assessment, the Constitutional Court emphasized that the information obtained within the scope of security clearance and archive research constitutes personal data, and that the regulatory framework governing the collection and use of such data does not contain sufficient, clear, and foreseeable safeguards, thereby failing to satisfy the requirement of legality. On these grounds, the Court held that the right to request the protection of personal data had been violated and ruled that the file be remitted to the relevant administrative court for retrial.

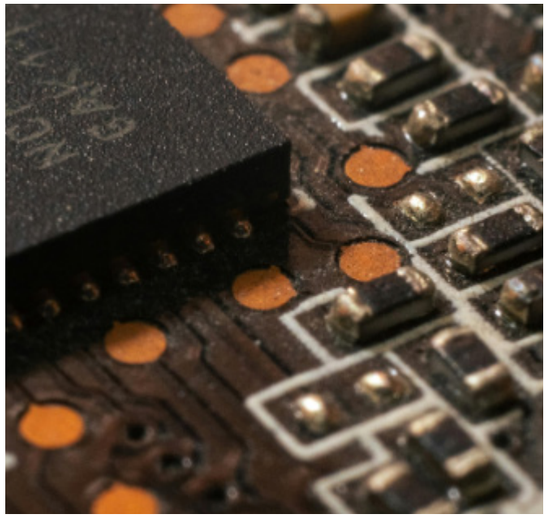
— 2 —

Constitutional Court's Decision with Application No. 2020/1546 and Decision Date 15 January 2025

(Muhsin Aras Application)

In its decision docketed No. 2020/1546 and dated 15 January 2025, the Constitutional Court ruled that the use of personal data obtained within the scope of security clearance and archive research as a decisive factor in appointments to public office constitutes a violation of the right to request the protection of personal data, which is safeguarded under Article 20 of the Constitution. In the case at hand, the applicant, who had been placed as a physician in a public hospital as a result of the state service obligation lottery, was not appointed on the grounds that the security clearance conducted in respect of the applicant yielded a negative result. The action brought against this decision was dismissed by the administrative courts, and the decision thereby became final.

In its assessment, the Constitutional Court emphasized that the information obtained within the scope of security clearance and archive research constitutes personal data, and that the regulatory framework governing the collection, retention, and use of such data in appointments to public office does not contain sufficient, clear, and foreseeable safeguards. In this respect, the Court concluded that the regulation in question was not capable of protecting individuals against arbitrary interference and failed to satisfy the requirement of legality. On these grounds, a violation decision was rendered, and it was ruled that the file be remitted to the relevant administrative court for retrial.



— 3 —

Constitutional Court's Decision with Application No. 2020/35291 and Decision Date 4 February 2025

(Özge Kahraman Application)

In its decision dated 4 February 2025 and numbered Application No. 2020/35291, the Constitutional Court ruled that the dismissal of a lawsuit filed for the erasure of intelligence data obtained as a result of a security clearance, on the grounds that it did not constitute a "final and enforceable administrative act," resulted in a violation of the right to an effective remedy in connection with the right to request the protection of personal data.

In the case at hand, the applicant, who was serving as a research assistant, requested a change of status, which was rejected on the basis of negative information contained in an intelligence report alleging that the applicant had participated in an illegal organization's training camp. Asserting that such information was factually inaccurate, the applicant applied to the Istanbul Provincial Police Department for the erasure of the relevant data. Following the rejection of this request, the applicant filed an action for annulment, which was dismissed by the lower courts without examination on the merits, on the grounds that the intelligence note constituted "a preparatory administrative act rather than an executive act." The applicant subsequently lodged an individual application, arguing that such data would continue to surface throughout her life and that excluding it from judicial review was contrary to law.

The noteworthy points emphasized in the Constitutional Court's assessment may be summarized as follows:

- The Constitutional Court confirmed that data obtained through security clearance and archive research clearly constitute personal data, and that any recording and use of such data amounts to an interference with the right to respect for private life.
- The Court emphasized that, pursuant to Article 20 of the Constitution, everyone has the right to request the erasure of personal data relating to them, and that the State has a positive obligation to provide an effective remedy to ensure the protection of such data and to prevent unlawful interference.
- It was noted in the decision that the administration had directly relied on the intelligence note when rejecting the applicant's request, and that such note therefore constituted data having a direct impact on the applicant's interests, with continuous and serious consequences.
- The lower courts' refusal to examine the merits of the case by characterizing the intelligence note as not being a "final and enforceable act" was described as a narrow interpretation that was detached from the purpose of protecting fundamental rights and freedoms.
- The Constitutional Court stated that the failure to subject such records—which may confront individuals throughout their lives—to judicial scrutiny leaves individuals vulnerable to arbitrariness and renders the right to an effective remedy ineffective.
- For these reasons, the Court unanimously held that the right to an effective remedy, in connection with the right to request the protection of personal data, had been violated.
- In order to eliminate the consequences of the violation, the Court ruled that the file be remitted to the Istanbul 5th Administrative Court for retrial.

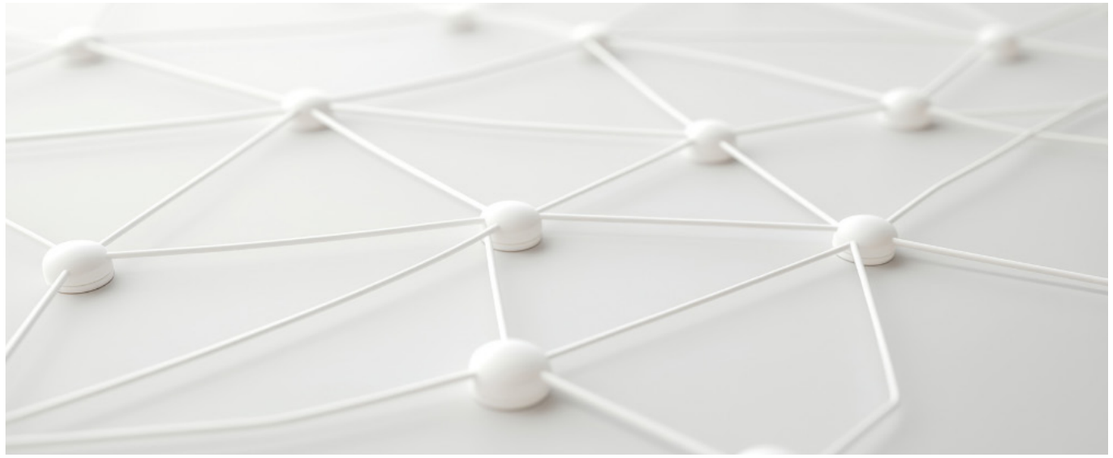
— 4 —

Constitutional Court's Decision with Application No. 2021/6515 and Decision Date 13 March 2025

In its decision dated 13 March 2025 and numbered Application No. 2021/6515, the Constitutional Court held that the recording of prisoners' letters in the National Judiciary Informatics System ("**UYAP**") constituted a violation of the right to request the protection of personal data, as safeguarded under the right to respect for private life, as well as a violation of the freedom of communication. The applicants alleged that, while they were detained in penal enforcement institutions, the letters sent to them or dispatched by them were scanned and recorded in the UYAP system, and that such practice infringed upon their privacy and freedom of communication. The applicants' main argument was that the transfer and retention of letter contents, which constitute personal data, in a digital environment lacked any legal basis and amounted to an arbitrary interference.

The noteworthy points emphasized in the Constitutional Court's assessment may be summarized as follows:

- At the admissibility stage, the Court found that the allegations concerning the right to request the protection of personal data and the freedom of communication were not manifestly ill-founded and were therefore admissible.
- The Constitutional Court noted the absence of rules regulating the scope of measures involving the recording, retention, and use of prisoners' private information and personal data.
- The decision emphasized that there were no legal safeguards defining the limits of the administration's discretionary powers in such interventions or protecting individuals against arbitrariness.
- It was stated that the interference with the right to respect for private life guaranteed under Article 20 of the Constitution and the freedom of communication under Article 22 lacked a lawful basis that complied with procedural requirements and the necessities of a democratic society.
- On the grounds that the interference failed to satisfy the principle of legality, the Court unanimously held that Articles 20 and 22 of the Constitution had been violated.
- In order to eliminate the consequences of the violation, the Court ruled that the file be remitted to the relevant enforcement judgeships and courts for retrial.
- The Court further held that the retrial decision would be sufficient to remedy the violation and therefore rejected the applicants' claims for non-pecuniary damages.



— 5 —

Constitutional Court's Decision with Application No. 2020/15944 and Decision Date 30 April 2025

In its decision dated 20 March 2025 and numbered Application No. 2020/15944, the Constitutional Court held that, in judicial proceedings concerning the sharing of health data, the applicant's right to request the protection of personal data, as safeguarded under Article 20 of the Constitution, had been violated.

The applicant filed an individual application on the grounds that, despite being of full legal age, sensitive health data relating to her medical treatment process had been disclosed to her mother by the treating physician without her knowledge or explicit consent. Following a complaint lodged in this regard, the Public Prosecutor's Office issued an indictment against the relevant physician for the offence of unlawfully obtaining or disclosing personal data. However, the Izmir 2nd Criminal Court of First Instance acquitted the physician, characterizing the act as conduct aimed at protecting and acting in the best interests of the applicant, and holding that the element of intent had not been established in the specific circumstances. The acquittal decision was subsequently upheld upon appellate review and became final. Separately, after the Izmir Chamber of Physicians imposed a warning sanction on the physician, the applicant submitted the relevant documents both to the Regional Court of Appeal ("**RCA**") and to the Constitutional Court by way of an individual application.

The salient points emphasized in the Constitutional Court's assessment may be summarized as follows:

- It was noted that health data constitute special categories of personal data and are subject to enhanced protection under Article 20 of the Constitution.
- In the specific case, it was established that, although the applicant was of full legal age, a medical report containing health information relating to the treatment process had been disclosed to a third party, including the applicant's mother, without the applicant's knowledge or consent.
- The Constitutional Court considered that the judicial authorities had failed to sufficiently examine why a document was disclosed, despite the possibility of providing mere information, and whether such disclosure was necessary or whether a less intrusive method could have been adopted.
- For these reasons, the Constitutional Court concluded that the applicant's right to request the protection of personal data had been violated.

For the foregoing reasons, the Constitutional Court ruled that the applicant's right to request the protection of personal data, as guaranteed under Article 20 of the Constitution, had been violated, and ordered that the file be remitted to the Izmir 2nd Criminal Court of First Instance for retrial in order to eliminate the consequences of the violation.

— 6 —

Constitutional Court's Decision with Application No. 2022/5840 and Decision Date 30 April 2025

In its decision dated 30 April 2025 and numbered Application No. 2022/5840, the Constitutional Court ruled that, in proceedings concerning an objection filed against an administrative fine imposed on an attorney under the DP Law, the right to a reasoned decision, as guaranteed under Article 36 of the Constitution, had been violated, due to the failure of the first-instance court to duly assess the applicant's claims and defenses capable of affecting the outcome.

The applicant was complained to the Board on the grounds that, within the scope of an enforcement proceeding handled by the applicant, four (4) short message service (SMS) messages had been sent to the mobile phone number of the debtor's son. During the investigation conducted by the Board, the applicant was requested to submit information and documentation demonstrating the legal basis for the relevant data processing activity. In his defense, the applicant asserted that the debtor's

son had personally attended a meeting, and that explicit consent had been granted for the recording of contact information, as documented in a meeting record prepared during that meeting. However, despite being requested by the Board, the meeting record supporting the defense was not submitted.

In this context, the Board concluded that the relevant telephone number had been processed without relying on any of the data processing conditions set out under the DP Law, and decided to impose an administrative fine of TRY 50,000 on the applicant.

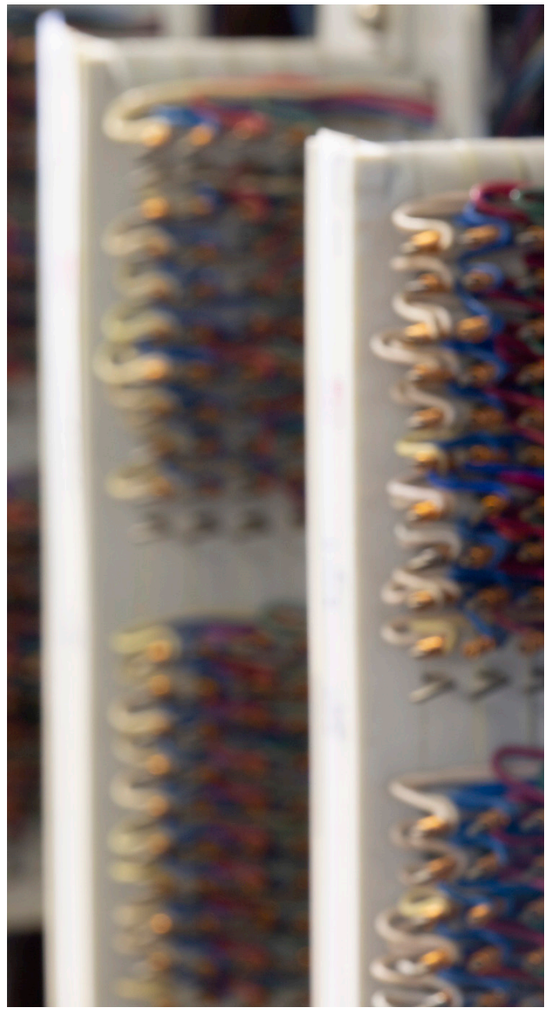
The applicant objected to the administrative fine before the Criminal Judgeship of Peace, arguing that explicit consent had been obtained, that he had been unable to access the relevant document due to the service of notifications during the COVID-19 full lockdown period, and therefore could not submit the meeting record to the Board, although it had been submitted to the court. The applicant further contended that the Board's decision lacked sufficient reasoning as to the departure from the lower limit of the administrative fine.

While finding the substance of the administrative sanction to be lawful, the Criminal Judgeship of Peace ruled that, due to the absence of reasoning justifying the departure from the lower limit, the administrative fine should be reduced to TRY 27,037. The objections lodged by the parties were finally dismissed, following which the applicant filed an individual application on the grounds that his claims and evidence had not been duly assessed.

In its assessment, the Constitutional Court highlighted the following points:

- It was emphasized that the right to a reasoned decision requires courts to assess the parties' claims and objections capable of affecting the outcome by providing clear, relevant, and sufficient reasoning.
- In the specific case, it was established that the applicant's defenses regarding the existence of explicit consent and his inability to submit the relevant document had not been examined at any stage of the proceedings, and that the objections had been dismissed on the basis of abstract reasoning.
- Accordingly, the Constitutional Court held that the applicant's right to a reasoned decision, as guaranteed under Article 36 of the Constitution, had been violated.

The Constitutional Court ruled that, in order to eliminate the consequences of the violation, the file be remitted to the relevant Criminal Judgeship of Peace for retrial.



— 7 —

Constitutional Court's Decision with Decision No. 2025/119 and Decision Date 3 June 2025

In its decision docketed No. 2025/47 and Decision No. 2025/119, dated 3 June 2025, and published in the Official Gazette dated 13 October 2025 and numbered 33046, the Constitutional Court examined the request for the annulment of certain provisions of Presidential Decree No. 177 on the Cybersecurity Directorate. The Court held that the provisions regulating the duties of the service units of the Cybersecurity Directorate by regulation and the rules concerning the establishment of staff positions were not unconstitutional, and therefore rejected the annulment requests.

The members of the GNAT who filed the annulment action argued that determining the duties and powers of the service units of the Directorate by regulation granted the executive branch unlimited regulatory authority, and that matters relating to the establishment of staff positions, which concern principal and permanent public duties, must be regulated exclusively by law. The applicants maintained that these arrangements amounted to an unlawful delegation of legislative power, were incompatible with the principle of separation of powers and the rule of law, and therefore requested both the annulment of the contested provisions and the suspension of their execution.

In its examination, the Constitutional Court determined that the Cybersecurity Directorate had been established as a public legal entity by way of a Presidential Decree, and that, accordingly, regulations concerning its organizational structure and staffing could likewise be enacted by Presidential Decree and therefore fell within the scope of authority ratione materiae. The Court emphasized that the President's discretion in matters relating to the organization of the administration derives from Articles 104 and 123 of the Constitution.

The noteworthy points emphasized in the Constitutional Court's assessment may be summarized as follows:

- **Regulation of Service Units by Secondary Legislation:** The Constitutional Court held that the fundamental duties and powers of the Directorate were clearly defined in the Presidential Decree, and that regulating the subordinate details of service units by way of regulation did not constitute a delegation of executive authority, but rather represented the exercise of administrative operational authority.

- **Authority to Establish Staff Positions:** The Court stated that the establishment of staff positions forming part of the organizational structure of public legal entities through a Presidential Decree was compatible with the Constitution, and that such matters did not fall within a domain reserved exclusively for statutory regulation.

- **Legal Certainty:** The fact that the number and titles of staff positions were explicitly set out in annexed lists was found to be consistent with the principles of legal certainty and foreseeability, which are requirements of the rule of law.

- **Dissenting Opinions:** Dissenting judges argued that assigning the duties of service units directly to regulations without first establishing a basic framework in the Presidential Decree amounted to a delegation of primary regulatory authority in terms of content, and that the establishment of staff positions should, pursuant to Article 128 of the Constitution, be regulated by law, raising an objection on grounds of competence.

The Constitutional Court ultimately ruled, by majority vote, that both contested provisions were not unconstitutional in terms of competence ratione materiae and substantive content, and therefore rejected the annulment requests.

— 8 —

Constitutional Court's Decision with Decision No. 2025/149 and Decision Date 10 July 2025

In its decision docketed No. 2024/98 and Decision No. 2025/149, dated 31 December 2025, the Constitutional Court rejected in its entirety the requests for annulment concerning the provisions of the DP Law challenged within the scope of an abstract norm review action filed on the grounds of the alleged unconstitutionality of certain amendments introduced to the DP Law in 2024 as part of the 8th Judicial Reform Package.

The action was structured around three main regulatory pillars, namely:

i. the expansion of the conditions for the processing of special categories of personal data;
ii. the exceptional regime subjecting cross-border transfers of personal data to the approval of the Board; and
iii. the sanctioning of the notification obligation relating to standard contracts.

The applicants argued that these provisions undermined the principles of legal certainty and legality, conferred excessive discretionary powers on the administration, and resulted in a lack of adequate safeguards with respect to the right to the protection of personal data.

- The Court found that, pursuant to Article 6/3 of the DP Law, both the health-related exception based on the duty of confidentiality and the new exception introduced for non-profit organizations were clearly delineated at the statutory level in terms of their scope, purpose, and limits. The decision emphasized that these exceptions do not render the processing of personal data unlimited; rather, the general principles of the DP Law, data security obligations, oversight by the Board, and data subject rights collectively provide a comprehensive protective framework. In this respect, the Court concluded that the regulations are compatible with the principles of the rule of law and foreseeability.

- With regard to Article 9/9 of the DP Law concerning the cross-border transfer of personal data, the Constitutional Court assessed the requirement to obtain Board approval in exceptional cases where the interests of Türkiye or the data subject may be seriously harmed as a legitimate mechanism that strikes a balance between national security, public interest, and the right to the protection of personal data. When considered together with the regimes of adequacy decisions and appropriate safeguards, the regulation was found not to constitute an arbitrary administrative authorization and to satisfy the requirement of legality.

- In its examination of the administrative fine attached to the notification obligation relating to standard contracts, the Court stated that, when the misdemeanor nature of the sanction, the lower and upper limit system, the revaluation mechanism, and the availability of judicial review are assessed together, the penalty does not violate the principle of proportionality. It was further determined that sufficient constitutional and judicial safeguards exist to prevent the arbitrary exercise of administrative discretion.

Overall, the Constitutional Court does not confine its constitutional review of personal data protection to isolated provisions; instead, it examined the systematic structure of the DP Law, data subject rights, the duties and powers of the Board, as well as the administrative and judicial remedies as a whole. Within this framework, the Court underlined the necessity of assessing regulations permitting the processing of personal data together with the safeguards ensuring the protection of personal data in the course of constitutional review.

Accordingly, the requests for annulment directed at the amendments introduced to the DP Law in 2024 were rejected, and the Court concluded that the new regulations concerning both the processing of special categories of personal data and the cross-border transfer of personal data are not unconstitutional.

8

COMPILATION OF COURT OF CASSATION DECISIONS IN 2025

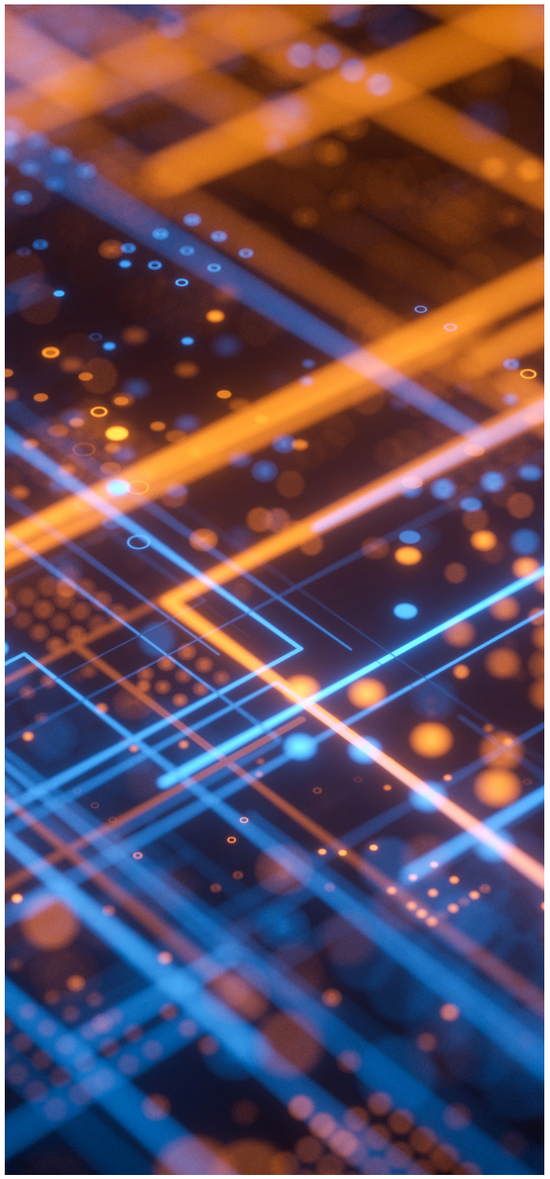
Set out below are notable decisions and assessments rendered by the Court of Cassation in 2025 that are of particular significance for the interpretation and application of data protection and privacy legislation.

— 1 —

Decision of the 12th Criminal Chamber of the Court of Cassation, Case No. 2022/4834, Decision No. 2024/8047, Dated 24 December 2024

In the case under review, the defendant obtained photographs belonging to the complainants from publicly accessible Instagram profiles and published them on a personal social media account without the complainants' consent. The court of first instance convicted the defendant on the grounds that the act constituted the unlawful acquisition and dissemination of personal data. Upon appellate review, the RCA set aside the conviction and acquitted the defendant, taking into account that the photographs had been obtained from public profiles and that no personal data other than the photographs had been shared.

Following the complainants' appeal on points of law, the Court of Cassation emphasised that the concept of personal data is not limited to confidential information, and that information which is known to the public or easily accessible may also qualify as personal data. The Court of Cassation further held that the fact that a photograph has been shared publicly does not deprive it of its personal data character, nor does it grant third parties the right to redistribute such content without the data subject's consent. On these grounds, the Court of Cassation concluded that the defendant's conduct constituted an offence under Article 136 of the TPC, found the acquittal decision unlawful, and reversed it.



— 2 —

Decision of the 12th Criminal Chamber of the Court of Cassation, Case No. 2023/2170, Decision No. 2025/182, Dated 8 January 2025

In the present case, the defendant recorded two individuals walking side by side on a public street from behind for approximately fifteen seconds and shared the footage on a personal social media account. After the recording was noticed by individuals within the complainants' close social circle, a request was made for the removal of the content; however, as the footage remained accessible for a certain period, criminal proceedings were initiated.

The court of first instance assessed the act as a violation of the right to privacy and sentenced the defendant to two years and one month of imprisonment. Upon appellate review, the RCA acquitted the defendant on the grounds that the individuals' faces were not clearly visible and that they could not be directly identified. Following an appeal on points of law, the Court of Cassation held that presence in a public space does not amount to consent to being recorded without authorisation and having such recordings shared on social media. The Court further determined that, when the clothing, physical characteristics of the individuals and the overall context of the incident are assessed together, the persons appearing in the footage were identifiable and that the shared images therefore constituted personal data. In addition, the Court found that the images related to the individuals' private sphere and concluded that, pursuant to the principle of the priority of the special norm, the conduct constituted the offence of violation of the right to privacy. On these grounds, the acquittal decision rendered by the RCA was found unlawful and was reversed.

— 3 —

Decision of the 9th Criminal Chamber of the Court of Cassation, Case No. 2024/13450, Decision No. 2025/700, Dated 20 January 2025

In the present case, the claimant asserted that, while employed in the reporting unit of the defendant company, a file belonging to another customer was inadvertently encrypted and sent to the customer representative responsible for control when responding to a request for an account statement relating to a different customer. Following the unchecked forwarding of the file to the customer, the employment contract was terminated on the grounds of an alleged violation of the DP Law, and the termination reason was reported under Code 49. The claimant requested the correction of the termination code.

The court of first instance held that the appropriate termination code should have been Code 04, noting the absence of concrete evidence demonstrating prior warnings or persistent failure to perform duties. Upon appellate review, the RCA found that the employer had failed to prove that the erroneous transaction had been intentional or repeated and concluded that the termination was not based on just cause. Reviewing the appeal arguments, including the reliance on a DP Law undertaking and the allocation of responsibility to the employee, the Court of Cassation held that the RCA decision was in accordance with procedural rules and substantive law and upheld the judgment.

— 4 —

Decision of the 12th Criminal Chamber of the Court of Cassation, Case No. 2022/7928, Decision No. 2025/729, Dated 21 January 2025

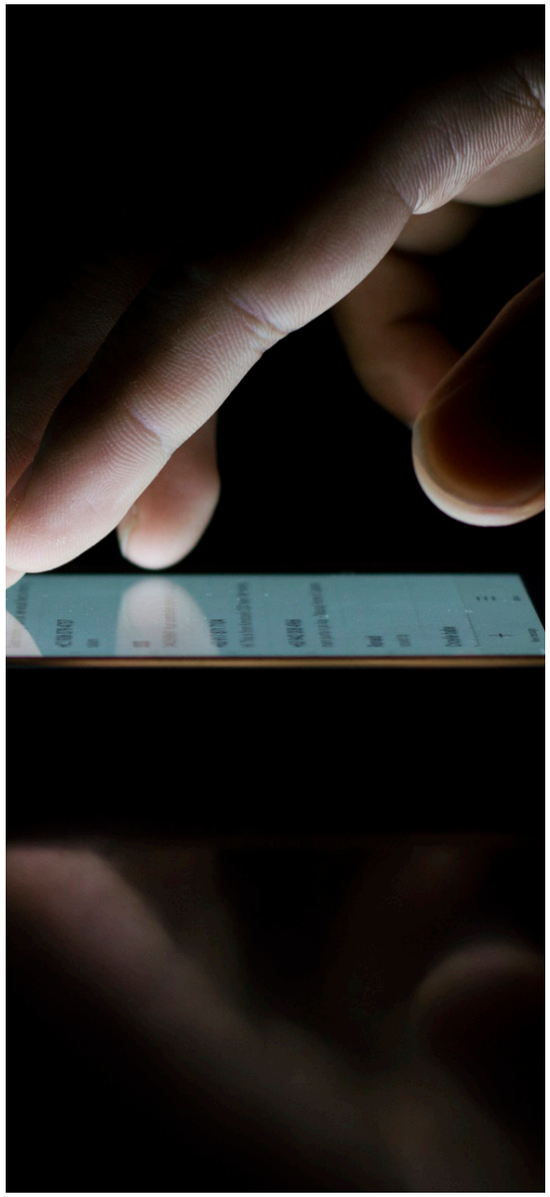
In the present case, a lawyer submitted correspondence exchanged between the complainant and the complainant's spouse as evidence in a labour court action filed against former colleagues and a trade union. Criminal proceedings were initiated on charges of violation of the confidentiality of communications, and the court of first instance sentenced the defendant to ten months' imprisonment.

Upon appellate review, the RCA acquitted the defendant, finding no evidence that the communication content had been shared with third parties or disseminated, and no proof that the conduct was carried out with awareness of unlawfulness. Following an appeal on points of law, the Court of Cassation concluded that the statutory elements of the offence had not been established, rejected the appeal on the merits, and upheld the acquittal.

— 5 —

Decision of the 3rd Civil Chamber of the Court of Cassation, Case No. 2024/4081, Decision No. 2025/1441, Dated 10 March 2025

The 3rd Civil Chamber resolved divergent case law among RCA chambers regarding the availability of preliminary injunctions in actions filed pursuant to Article 319/2 of the TCO. Emphasising the temporary nature of interim relief, the Court held that, pursuant to Article 389 of the Code of Civil Procedure, preliminary injunctions may be granted without addressing the merits where delay would cause serious harm or significantly hinder the acquisition of rights. The Court concluded that a fair balance must be struck between the tenant's right to respect for private life and the lessor's right to property, and that limited viewing of leased premises may be ordered based on the circumstances of each case.



— 6 —

Decision of the 12th Criminal Chamber of the Court of Cassation, Case No. 2022/10008, Decision No. 2025/3790, Dated 14 April 2025

The Court of Cassation held that sharing screenshots of WhatsApp messages to which the defendant was a party within a closed group did not constitute the offence of violation of the confidentiality of communications under Article 132/3 of the TPC. The correspondence did not concern private life and was not disclosed in a public setting. The Court emphasised that disclosure in a closed group with limited participants does not meet the publicity requirement of the offence and upheld the acquittal rendered by the RCA.

— 7 —

Decision of the 12th Criminal Chamber of the Court of Cassation, Case No. 2025/449, Decision No. 2025/4296, Dated 12 May 2025

The Court of Cassation held that a court clerk with authorised access did not commit the offence of unlawful disclosure or acquisition of data under Article 136 of the TPC by querying personal data out of curiosity without an unlawful purpose. The data were accessed through assigned credentials, were not shared with third parties, and no awareness of unlawfulness was established. The Court emphasised that "acquisition" requires unlawful control over data belonging to another and that authorised querying does not meet this threshold. While such conduct may give rise to disciplinary liability, it does not constitute a criminal offence. The acquittal rendered by the RCA was therefore upheld, and the public prosecutor's appeal was dismissed.

9

OTHER KEY DEVELOPMENTS

1. Advertising Board 2024 Annual Report

The 2024 Annual Report published on 6 February 2025 by the Advertising Board operating under the Ministry of Trade of the Republic of Türkiye indicates an intensified level of regulatory scrutiny over digital advertising practices and online commercial activities. Misleading digital practices, personal data violations, manipulative user interface designs, and deceptive review systems are identified as the principal risk areas.

Within the scope of "Dark Commercial Designs", practices such as deliberately complicating subscription cancellation processes, requesting excessive or unnecessary personal data, and indirectly rendering consent to commercial electronic communications mandatory have been classified as unfair commercial practices. The Report emphasises that such practices undermine consumers' freedom of choice and have been expressly prohibited pursuant to the amendments introduced in 2022 to the Regulation on Commercial Advertising and Unfair Commercial Practices.

The Report further determines that fake or artificial intelligence–generated user reviews, as well as "shadow pricing" practices that create a false perception of discounts in digital environments, are misleading to consumers. These practices are noted to erode consumer trust and have been subjected to administrative sanctions.

From both a legislative and enforcement perspective, the Report highlights several key developments strengthening supervisory and enforcement mechanisms, including: the introduction of minimum and maximum thresholds for administrative fines under Law No. 6502 on the Protection of Consumers, the implementation of a settlement mechanism, and the launch of the Advertising Board Module accessible via the e-Government platform.

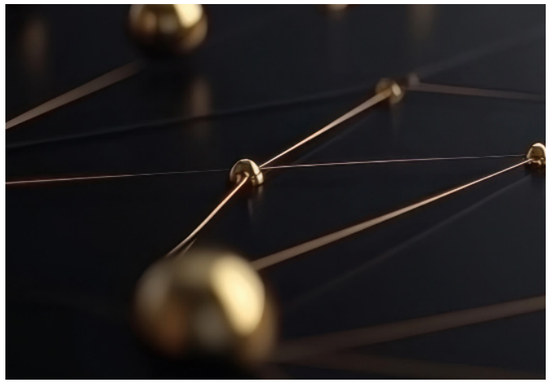
Throughout 2024, a total of 22,299 applications were reviewed. Of the 1,917 files examined in detail, 1,705 were found to be in violation of the applicable legislation. In this context, administrative fines amounting to TRY 277,664,783 were imposed, with the majority of sanctions being directed at advertisers.

2. Information and Communication Technologies Authority 2024 Activity Report

The 2024 Activity Report, published on 20 March 2025 by the Information and Communication Technologies Authority ("ICTA"), provides an overarching framework of the regulatory, supervisory, and coordination activities carried out in the fields of electronic communications, the internet, and information technologies. Within this scope, efforts were undertaken to ensure the operation of digital infrastructures, manage risks arising in the online environment, and facilitate technical cooperation between public authorities and sector stakeholders.

Under the coordination of the National Cyber Incident Response Center (USOM), processes were implemented for the identification and blocking of malicious links, the dissemination of cybersecurity notifications to relevant institutions and organisations, and the monitoring and response to cyber incidents through Cyber Incident Response Teams (CIRTs) established at both sectoral and institutional levels. In this regard, information security risks targeting public institutions and critical infrastructures were monitored, and corresponding technical intervention mechanisms were applied.

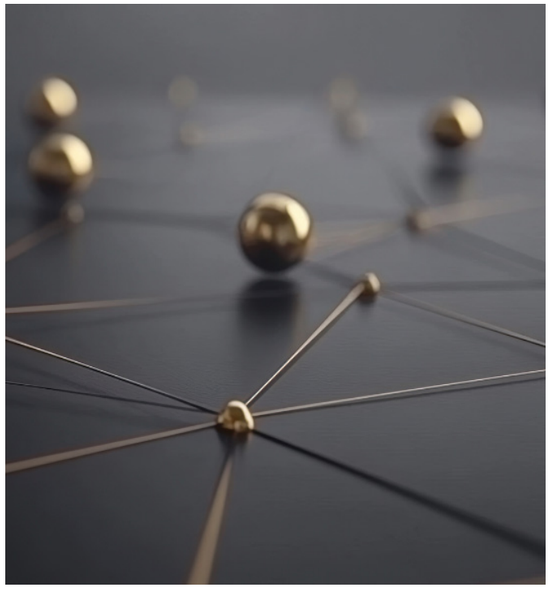
Mechanisms for reporting illegal and harmful online content were actively operated, while activities carried out within the framework of safe internet services continued alongside initiatives aimed at supporting positive digital content in online environments.



3. Information Technology and Infrastructure Criteria for Crypto Asset Service Providers

The document titled "Criteria for the Information Systems and Technological Infrastructures of Crypto Asset Service Providers", published on 30 April 2025 by the Scientific and Technological Research Council of Türkiye – Informatics and Information Security Advanced Technologies Research Center (TÜBİTAK-BİLGEM), sets out the minimum technical and administrative requirements applicable to the information systems and technological infrastructures of crypto asset service providers within the framework of Capital Markets Board regulations.

The document sets out detailed criteria covering, inter alia, hot and cold wallet security, cryptographic key generation and management, multi-signature and threshold cryptography mechanisms, identity and access management, risk management, information security incident handling, physical and environmental security, and the supervision of outsourced services. It further establishes a structured information security framework grounded in senior management oversight, the maintenance of audit trails, and readiness for independent audit.



4. FCIB Activities

4.1. FCIB Presidency – 2024 Activity Report

The 2024 Activity Report, published by the FCIB Presidency on 5 May 2025, provides a quantitative overview of the data collection, analysis, and supervisory activities carried out in the context of combating money laundering and the financing of terrorism.

Throughout 2024, a substantial number of suspicious transaction reports were received, predominantly submitted by banks, payment and electronic money institutions, and crypto-asset service providers. The primary predicate offence categories underlying these reports included tax-related offences, illegal betting and gambling activities, and transactions conducted on behalf of third parties.

As a result of the compliance inspections conducted during the same period, administrative monetary fines exceeding TRY 964 million were imposed.

4.2. Suspicious Transaction Reporting Guidelines

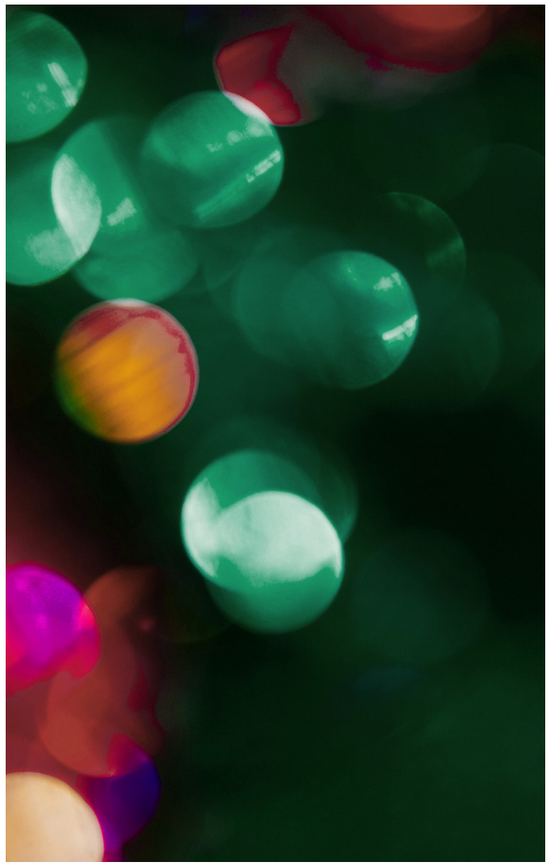
With the announcement published by the FCIB on 13 June 2025, new guidelines were issued to enable obliged entities to submit suspicious transaction reports in line with sector-specific risk profiles and the findings of the most recent National Risk Assessment, within the framework of Law No. 5549 on the Prevention of Laundering Proceeds of Crime. Accordingly, Suspicious Transaction Reporting Guidelines were prepared for the first time for a wide range of obliged parties, including lawyers, accountants, notaries, electronic commerce intermediary service providers, independent audit firms, investment partnerships, and insurance and reinsurance brokers, while certain existing guidelines were also revised and updated.

In parallel with the publication of the guidelines, the "FCIB Online 2.0 System", which enables the electronic submission of suspicious transaction reports, was put into operation; thereby strengthening the institutional infrastructure for the standardisation and digitalisation of reporting processes.

4.3. Update to the Crypto Asset Service Providers Guidelines

The Crypto Asset Service Providers Guidelines, which were updated and published on 30 September 2025, set out the scope and principles of implementation of the obligations imposed on crypto asset service providers within the framework of anti-money laundering legislation and capital markets regulations.

The Guidelines regulate, inter alia, know-your-customer (KYC) and customer identification procedures, remote identity verification practices, data sharing conducted within the scope of the Travel Rule, time and threshold limitations applicable to crypto asset transfers, measures to be applied in business relationships established with politically exposed persons (PEPs), as well as obligations relating to suspicious transaction reporting and compliance programs.



5. Presidential Circular on the Accessibility of Websites and Mobile Applications

The Presidential Circular on the Accessibility of Websites and Mobile Applications, published in the Official Gazette dated 21 June 2025, has rendered the obligation to ensure access to digital services for persons with disabilities and elderly individuals legally binding for both the public and private sectors.

The Circular refers to the Web Content Accessibility Guidelines version 2.2 – Level A as the benchmark standard, which sets forth the minimum technical accessibility requirements for websites and mobile applications. These requirements are based on ensuring that digital content is compatible with screen readers, accessible via keyboard navigation, free from design elements that effectively hinder access to core functionalities, and that user interactions are designed and implemented in an accessible manner.

6. 2025 Action Plan of the Coordination Council for the Improvement of the Investment Environment.

The 2025 Action Plan of the Coordination Council for the Improvement of the Investment Environment, published on 10 July 2025, sets out the general framework for legislative and policy initiatives envisaged in the fields of digitalization and technology-driven sectors.

- It is planned that efforts to ensure the alignment of the DP Law with the GDPR will be finalized under the coordination of the Ministry of Justice.
- It is aimed to establish a legal basis for conducting approval, contract, payroll, and training processes used in human resources management through digital methods.
- The publication of the National Cloud Computing Strategy and the National Data Strategy, as well as the review of regulations concerning data localization, is envisaged.
- It is planned to prepare a new Artificial Intelligence Strategy Document and Action Plan covering the 2026–2030 period.
- Legislative efforts aimed at ensuring alignment with EU regulations on the protection of trade secrets are expected to be submitted to the legislative process.
- Preparatory work to ensure harmonization with EU legislation in the fields of the digital economy and cybersecurity is planned to continue.
- It is aimed to update the legislation on electronic signatures so as to encompass international standards.

7. 2026 Presidential Annual Program

The 2026 Presidential Annual Program, published in the Official Gazette dated 30 October 2025, positions digital transformation and cybersecurity among the priority areas of public policy. Within the scope of the Program, objectives have been set for strengthening information and communication technologies infrastructure, finalizing national strategies on data governance, and enhancing digital public services. In this regard, it is envisaged that regulatory and implementation efforts relating to broadband infrastructure, the data economy, and the e-commerce ecosystem will be advanced in parallel.

With respect to cybersecurity, particular emphasis is placed on secondary legislation initiatives. Key policy priorities include the implementation of national cybersecurity regulations aligned with the EU Directive on Measures for a High Common Level of Cybersecurity Across the Union (the "NIS2 Directive"), the preparation of secondary cybersecurity legislation in line with the EU Cyber Resilience Act ("CRA") and international standards, and the further development of the regulatory framework in this field.

Additionally, other envisaged focus areas include defining the legal and ethical framework for artificial intelligence applications, developing risk management approaches for the use of artificial intelligence within the judiciary and public administrations, and strengthening digital government and open data infrastructures.

8. Bill on the Approval of the Digital Economy Partnership Agreement

Following its signature on 6 November 2024, the Digital Economy Partnership Agreement, which regulates cooperation on digital trade among the member states of the Organization of Turkic States, was submitted to the approval process in Türkiye through a Bill dated 27 November 2025. The Agreement addresses the protection of personal data in the context of cross-border data flows as a shared principle. It envisages that the contracting states shall establish a national legal framework for the protection of personal data, adopt clear and accessible rules governing data transfers, make publicly available information regarding individuals' rights and businesses' obligations, and ensure transparency in data protection practices.

B.STRUCTURE AND SUPERVISORY ACTIVITIES OF THE BOARD AND AUTHORITY

STRUCTURE AND ORGANIZATION OF THE BOARD AND THE AUTHORITY

The Authority is composed of the Board, and the Presidency. The Authority is organized into eight Board Members, excluding the President of the Authority and the Vice President, and seven presidential departments.

With the appointment of Dr. Ayşenur KURTOĞLU and HASAN AYDIN as Board Members pursuant to Presidential Decree No. 2025/176, published in the Official Gazette dated 17 May 2025, the current structure of the Board is as follows:

President of the Authority / Member of the Board	**Prof. Dr. Faruk BİLİR**
Vice President of the Authority / Member of the Board	Hasan AYDIN
Member of the Board	Şaban BABA
Member of the Board	Murat KARAKAYA
Member of the Board	Bayram ARSLAN
Member of the Board	Dr. Ayşenur KURTOĞLU
Member of the Board	Tamer AKSOY
Member of the Board	Recep KESKİN
Member of the Board	Cennet ALAS ŞEKERBAY
Member of the Board	MUHAMMED SERDAR CAFOĞLU

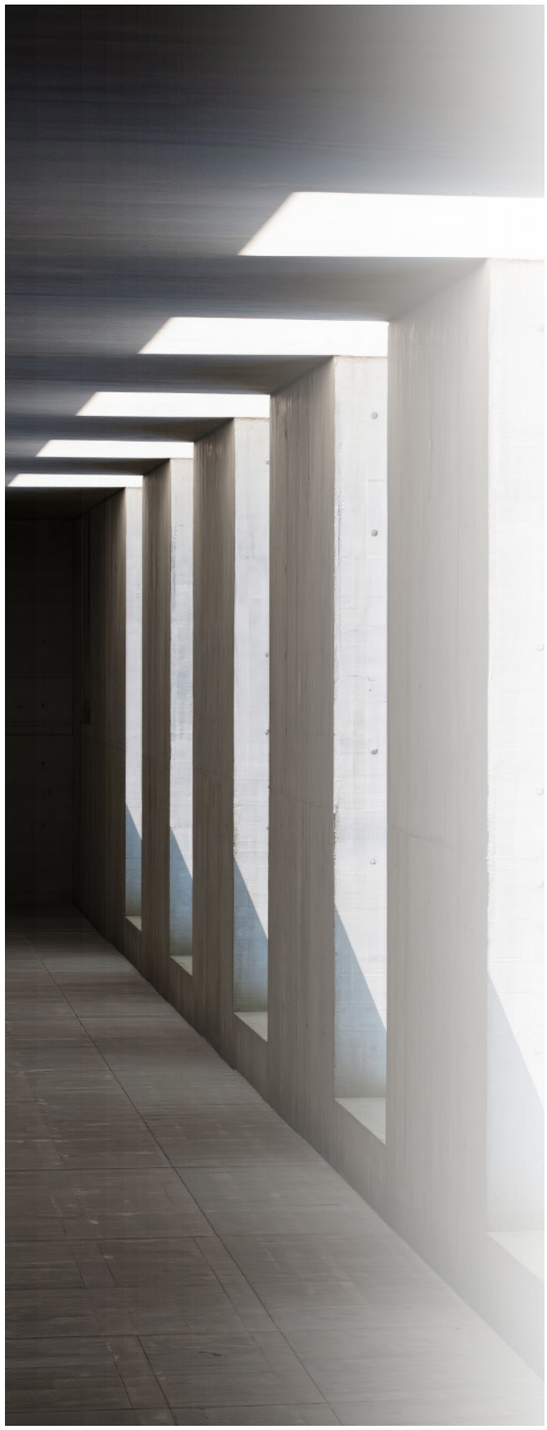
Presidential Departments

- Data Governance Department
- Inspection Department
- Legal Affairs Department
- Data Security and Information Systems Department
- Guidance, Research and Corporate Communications Department
- Human Resources and Support Services Department
- Strategy Development Department

The Authority published its first activity report in 2018 and has continued this practice for the years 2019, 2020, 2021, 2022, 2023, and 2024. As of the date of publication of this study, the Authority has not yet publicly released its activity report for 2025. Nevertheless, as detailed under Section A.VII.1. the Authority published a report titled "The Personal Data Protection Authority in Its 8th Year" on 29 December 2025, in which it shared detailed information regarding its activities carried out between 2017 and April 2025. While the statistical data included in this publication were compiled as of April 2025, the President of the Authority, Prof. Dr. Faruk Bilir, subsequently shared more up-to-date consolidated information regarding the Authority's activities since its establishment through various public statements made following the end of 2025. Accordingly,

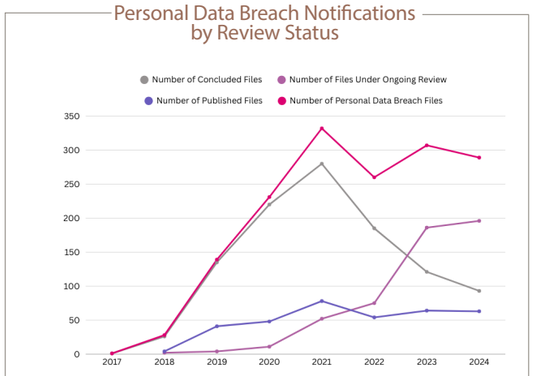
- As a result of the inspections conducted since the Board commenced its operations in 2017, a total of TRY **1,297,282,000** in administrative fines has been imposed.
- Within the scope of cross-border transfers of personal data, **3,857** SCs have been notified to the Authority.
- Approval has been granted to **13** undertakings.
- Of the **58,640** notices and complaints submitted to the Authority, **56,377** have been concluded.
- Out of **1,917** personal data breach notifications, **403** have been published on the Authority's website.
- **1,350** legal opinions have been issued on matters falling within the Authority's remit.
- A total of **332** decisions and **10** principle decisions have been published on the Authority's website.
- The year-by-year statistical data are presented below, compiled from the activity reports published by the Authority with respect to its activities in previous years.

The year-by-year statistical data are presented below, compiled from the activity reports published by the Authority with respect to its activities in previous years.

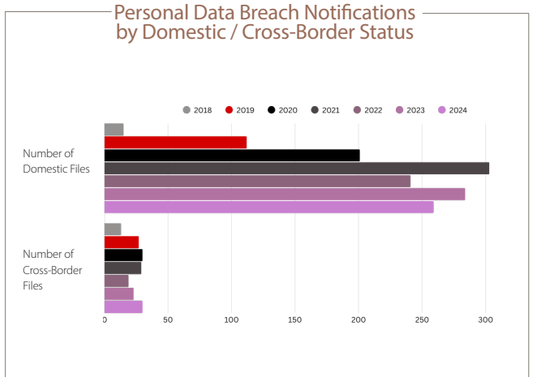


1. Personal Data Breach Notifications

The number of personal data breach notifications for the years 2017, 2018, 2019, 2020, 2021, 2022, 2023, and 2024 is presented in the charts and tables below.



	2017	2018	2019	2020	2021	2022	2023	2024	SUM
Number of Personal Data Breach Files	1	28	139	231	332	260	307	289	1,587
Number of Concluded Files	1	26	135	220	280	185	121	93	1,061
Number of Files Under Ongoing Review	-	2	4	11	52	75	186	196	526
Number of Published Files	-	4	41	48	78	54	64	63	352



	2017	2018	2019	2020	2021	2022	2023	2024	SUM
Number of Domestic Files	-	15	112	201	303	241	284	259	1,415
Number of Cross-Border Files	1	13	27	30	29	19	23	30	172
SUM	1	28	139	231	332	260	307	289	1,587

2. Statistical Data on the Board's Activities

According to the information disclosed in the Activity Reports published by the Authority for the years 2019, 2020, 2021, 2022, 2023, and 2024, the statistical data are as follows:

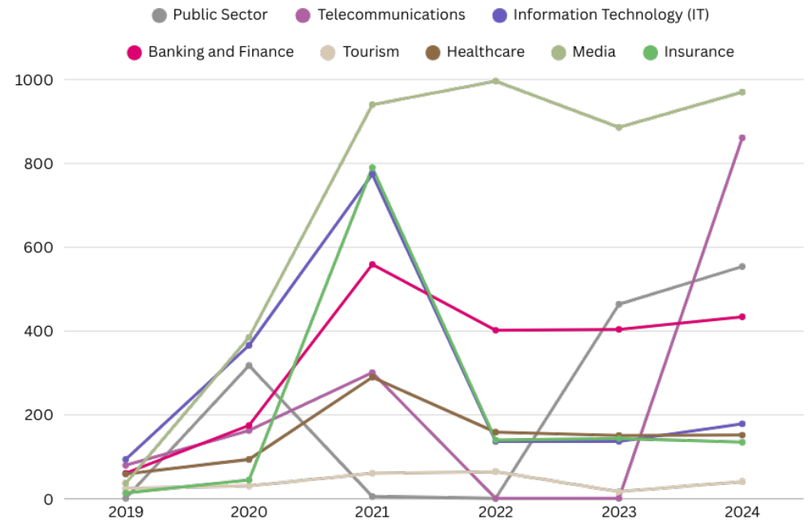
3. Complaints

The number of notices, complaints, and applications submitted up to 31 December 2024 is presented below.[12]

3.1. Sectoral Distribution of Complaints

The sectoral distribution of complaints for the years 2019, 2020, 2021, 2022, 2023, and 2024 is set out in the table below:

[12] In statements made by the President of the Authority, Prof. Dr. Faruk Bilir, in December 2025, as reported in publicly available news, it was disclosed that 56,377 out of 58,640 notices and complaints submitted to the Authority had been concluded

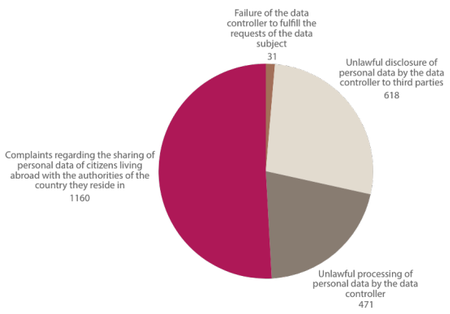


SECTOR	Number of Complaints (2019)	Number of Complaints (2020)	Number of Complaints (2021)	Number of Complaints (2022)	Number of Complaints (2023)	Number of Complaints (2024)
Public Sector	1,157	318	5,663	1,277	464	554
Telecommunications	80	163	301	1,190	1,356	861
Information Technology (IT)	94	366	774	137	137	179
Banking and Finance	61	175	559	402	404	434
Tourism	25	31	61	65	17	41
Healthcare	59	94	290	159	151	152
Media	37	385	940	996	886	970
Insurance	14	45	790	140	144	135
Human Resources	4	11	282	362	252	194
Services (General)	389	709	1,111	4,331	2,336	1,624
SUM	**2.280**	**2.297**	**10.060**	**9.059**	**9.396**	**8,275**

3.2. Distribution of Complaints by Subject

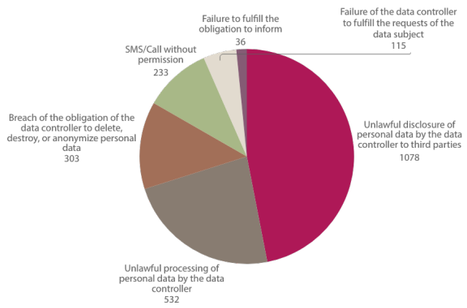
The subject-based distribution of complaints for the years 2019, 2020, 2021, 2022, 2023, and 2024 is presented in the tables below.

a) Distribution of Complaints in 2019[13]



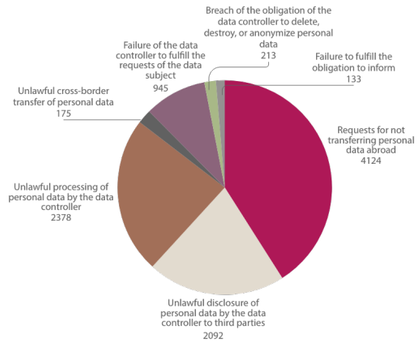
SUM: 2280

b) Distribution of Complaints in 2020[14]



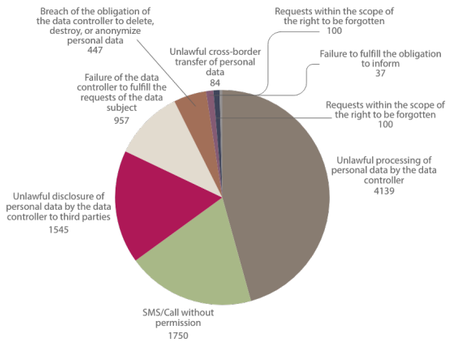
SUM: 2.297

c) Distribution of Complaints in 2021[15]



SUM: 10.060

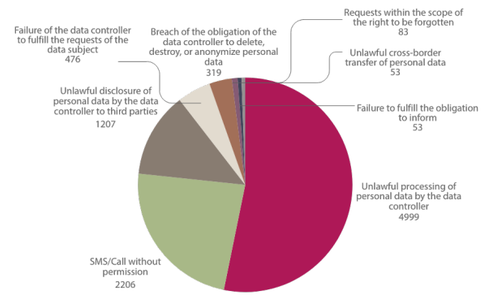
d) Distribution of Complaints in 2022[16]



SUM: 9. 059

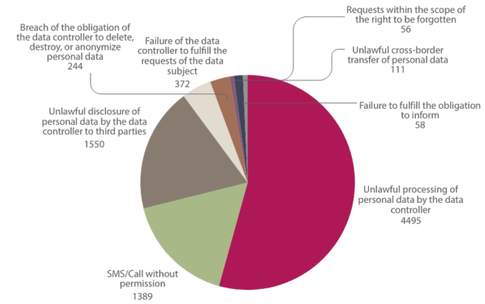
[13] Derived from the Authority's 2023 Activity Report.
[14] Derived from the Authority's 2023 Activity Report.
[15] Derived from the Authority's 2023 Activity Report.
[16] Derived from the Authority's 2023 Activity Report.

e) Distribution of Complaints in 2023[17]



SUM: 9.396

f) Distribution of Complaints in 2024[18]



SUM: 8.275

[17] Derived from the Authority's 2023 Activity Report.
[18] Derived from the Authority's 2023 Activity Report.

4. Statistical Overview of VERBIS Registrations, Applications, and System Activities

As of 31 December 2024, the statistical data regarding registrations and applications submitted to VERBIS are as follows:

Number of Applications	Number of Approved Applications	Number of Rejected Applications	Number of Appointed Contact Person
234,579	194,867	7,861	220,365

Performance Indicator	31 December 2024
VERBIS Application Approvals	234,579
VERBIS Application Update Transactions	8,400
Calls Received Regarding VERBIS Applications	85,090
Number of Notification Inquiries	1,814,779

5. Undertaking Applications

During 2025, the Board finalized three undertaking applications, bringing the total number of approved undertaking applications to 13.

Below is the list of all data controllers whose undertaking applications have been approved:

Data Controller	Undertaking Approval Date
TEB Arval Araç Filo Kiralama Anonim Şirketi	9 September 2021
Amazon Turkey Perakende Hizmetleri Ltd. Şti. ve Amazon Turkey Yönetim Destek Hizmetleri Ltd. Şti.	4 March 2023
Turksport Spor Ürünleri San. Tic. Ltd. Şti. (Decathlon Türkiye)	22 Jun 2021
Türkiye Futbol Federasyonu	18 January 2022
Otokoç Otomotiv Ticaret ve Sanayi Anonim Şirketi	30 March 2023
Google Reklamcılık ve Pazarlama Limited Şirketi	17 August 2023
Celltrion Healthcare İlaç Sanayi ve Limited Şirketi	25 January 2024
Bosch Termoteknik Isıtma ve Klima Sanayi ve Ticaret Anonim Şirketi	2 May 2024
Huawei Telekomünikasyon Dış Ticaret Limited Şirketi	28 May 2024
VF Ege Giyim Sanayi ve Ticaret Limited Şirketi	12 March 2025

6. SCs Notifications

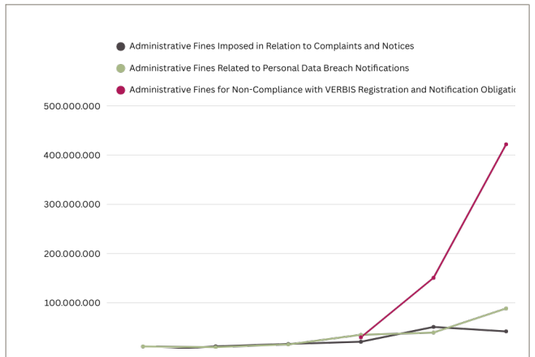
In statements made by the President of the Authority, Prof. Dr. Faruk Bilir, as reported in publicly available news, it was disclosed that, as of the end of 2025, **3,857** SCs relating to cross-border transfers of personal data had been notified to the Authority.

7. Binding Corporate Rules Applications

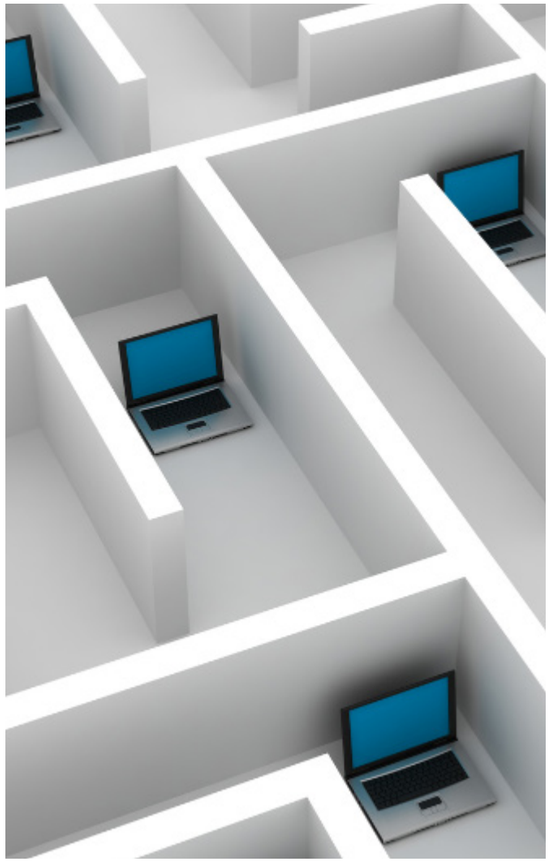
As stated in the 2024 Activity Report, although three Binding Corporate Rules applications had been submitted by 2025, these applications were not accepted due to procedural and substantive deficiencies.

8. Sanctions

The administrative fines imposed for the years 2019, 2020, 2021, 2022, 2023, and 2024 are set out in the table below:



	2019	2020	2021	2022	2023	2024
Administrative Fines Imposed in Relation to Complaints and Notices	1.905.000	11.497.000	16.351.000	20.738.000	50.917.000	41.907.101
Administrative Fines Related to Personal Data Breach Notifications	11.200.828	9.893.000	15.395.000	34.955.000	39.455.000	88.384.000
Administrative Fines for Non-Compliance with VERBIS Registration and Notification Obligations[18]	-	-	-	29.790.000	150.710.000	421.897.000
SUM	TRY 13.105.828	TRY 21.390.000	TRY 31.746.000	TRY 85.483.000 TL	TRY 241.082.000	TRY 552.188.101[19]



8.1. Highest Administrative Fines

The table below lists the twenty-one highest administrative fines imposed by the Board, as announced to the public on the Board's official website, based on the decisions issued since 2018[20]. An examination of the decisions imposing the highest administrative fines indicates that, in the vast majority of cases, the underlying data breaches arose not from administrative shortcomings, but rather from deficiencies in information systems, the failure to implement technical measures in a timely and adequate manner, or the failure to notify the Board within the prescribed timeframe.

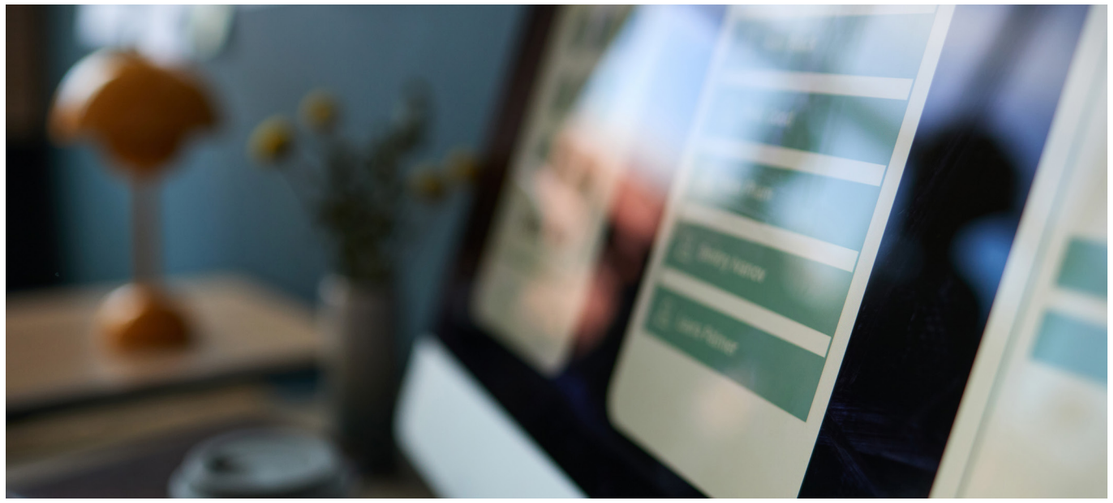
[18] The deadline for compliance with VERBIS registration and notification obligations was set as 31 December 2021. Through an announcement dated 21 April 2022, the Authority stated that administrative sanctions would be imposed for non-compliance with VERBIS registration and notification obligations. Accordingly, no administrative fines were imposed during the 2017–2021 period in this respect.

[19] In statements made by the President of the Authority, Prof. Dr. Faruk Bilir, in December 2025, as reported in publicly available news, it was disclosed that a total of TRY 1,297,282,000 in administrative fines had been imposed as a result of inspections carried out since the Board commenced its operations in 2017.

[20] Within the scope of this study, decisions published on the Board's official website have been taken into account. In addition, it should be noted that administrative fines of higher amounts have also been reported in various media outlets, which are not reflected on the Authority's official website.

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

Article 12/1: Failure to take necessary technical and administrative measures to prevent unlawful processing of personal data.
Article 12/3: Failure to audit compliance with the DP Law within the organization.
Article 12/5: Failure to notify the Board and pertaining persons within a reasonable time about the processed personal data being unlawfully obtained by others.
Article 15/5: Failure to comply with the instructions and orders of the Board for the elimination of violations.
As indicated in the table above, the majority of sanctions imposed in decisions published by the Board are based on Article 18/1 (b), regulating administrative fines due to non-compliance with data security rules outlined in Article 12 of the DP Law. The reason for this lies in the fact that the DP Law provides sanctions only for violations of Article 10, 12, 15, and 16, without specifying any penalties for breaches of Article 4, 5, and 6. Therefore, the enforcement predominantly relies on Article 18/1 (b), emphasizing non-compliance with data security regulations.



2

BOARD PRINCIPLE DECISIONS

1.Principle Decision on the Processing of Personal Data by Sending Verification Codes via SMS to Data Subjects During the Provision of Products and Services[21]

The Board's Principle Decision No. 2025/1072, titled "Principle Decision on the Processing of Personal Data by Sending Verification Codes via SMS to Data Subjects During the Provision of Products and Services", was published in the Official Gazette dated 26 June 2025.

In the course of its examinations, the Board determined that, during product and service provision processes, the information obligation had not been duly fulfilled, and that explicit consent for commercial electronic communications had been obtained in a misleading manner through SMS messages containing verification codes. Within this framework, the following points were particularly emphasized in the Principle Decision:

- In SMS messages sent in relation to product and service provision processes, the purpose of the verification code must be clearly stated prior to transmission; the consequences of sharing the code must be conveyed to data subjects in a clear and comprehensible manner, in line with a layered information approach.

- The sending of a verification code must not be combined with different processes such as membership approval, consent for personal data processing, or consent for commercial electronic communications; separate and freely given explicit consent must be obtained for each process.

- The processes of fulfilling the information obligation and obtaining explicit consent must be carried out independently of one another.

- Where explicit consent for the sending of commercial electronic communications is obtained via an SMS verification code, compliance with the DP Law must be ensured.

- The completion of the provision of a product or service must not be made conditional upon obtaining explicit consent for commercial electronic communications.

- Explicit consent should either be requested after the completion of the product or service provision, or measures should be taken to prevent the formation of any perception that sharing the verification code is mandatory for the provision of the service.

- Data controllers should conduct regular training and awareness activities for their employees to ensure that the relevant processes are carried out in compliance with the law.

Finally, the Board reiterated that, under the DP Law, data controllers are obliged to ensure the lawful processing of personal data, and reminded that administrative sanctions pursuant to Article 18 of the DP Law may be imposed in cases where necessary technical and administrative measures are not taken.

2. Principle Decision on the Retention of Copies of Turkish Identity Cards of Individuals Receiving Accommodation Services in the Tourism and Hospitality Sector

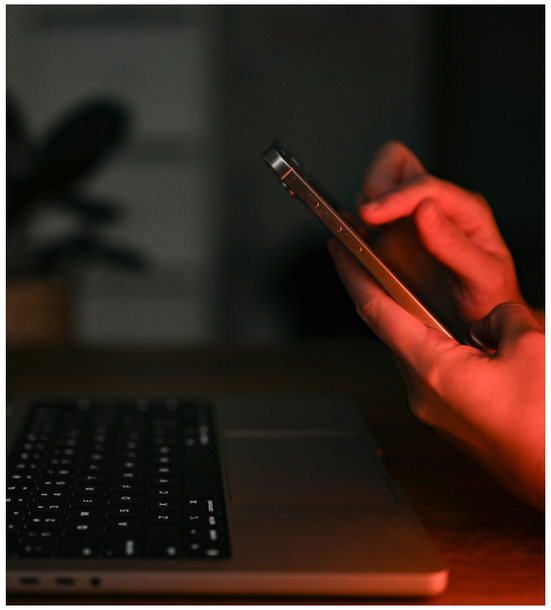
The Board's Principle Decision No. 2025/2120, titled "Principle Decision on the Retention of Copies of Turkish Identity Cards of Individuals Receiving Accommodation Services in the Tourism and Hospitality Sector", was published in the Official Gazette dated 9 December 2025. The Principle Decision addresses the legal nature, under the DP Law, of the practice of obtaining copies of Turkish identity cards during the provision of accommodation services in the tourism and hospitality sector.

- The Board held that the recording by accommodation facilities of guests' identity information—such as name, surname, and Turkish identity number—is lawful pursuant to Article 5(2)(a) of the DP Law and Article 5(2)(ç) of the DP Law, on the grounds that such processing is required under the Identity Notification Law and related secondary legislation and is necessary for the data controller's compliance with its legal obligations.

- The practice of obtaining and retaining photocopies of Turkish identity cards or identity booklets was found to be unlawful on the grounds that it violates the principle of proportionality, may lead to the unlawful processing of special categories of personal data (such as religion and blood type contained in older-format identity cards) within the scope of Article 6 of the DP Law, and that identity verification can be carried out without retaining a photocopy of the identity document.

Accordingly, the Board states that tourism and hospitality establishments must cease the practice of obtaining copies of identity documents and that existing records must be destroyed in accordance with Article 7 of the DP Law. It further clarifies that, for invoicing purposes, the mandatory information listed under Articles 230 and 240 of the Tax Procedure Law may be processed.

The Board also indicated that, should this practice continue, administrative sanctions may be imposed pursuant to Articles 12 and 18 of the DP Law.



[21] For further details, see https://www.morogluarseven.com/news-and-publications/principle-decision-of-the-personal-data-protection-board-regarding-the-processing-of-personal-data-by-sending-a-verification-code-via-sms-to-data-subjects-during-the-provision-of-products-and/

3

OTHER DECISION SUMMARIES

1.Board Decision on the VERBIS Registration Obligation

With its Decision No. 2025/1572 dated 4 September 2025, the Board restructured the exemption regime applicable to the VERBIS registration and notification obligation. The relevant amendments were published in the Official Gazette on 1 October 2025 and entered into force on the same date.

Within this framework, while the Board maintained the existing exemption granted to data controllers with fewer than 50 employees and an annual financial balance sheet total below TRY 100 million, it introduced a specific exemption for data controllers whose principal activity consists of the processing of special categories of personal data. Accordingly, natural or legal persons meeting both of the following criteria were exempted from the VERBIS registration and notification obligation:

i. having fewer than 10 employees annually, and
ii. having an annual financial balance sheet total below TRY 10 million.

C. EXPECTED DEVELOPMENTS

LEGISLATIVE AMENDMENTS

I. Legislative Amendments

Against this background, amendments to the DP Law and implementation-oriented regulatory instruments have been introduced through a gradual and incremental process. Notably, alignment efforts gained momentum as of 2024, and throughout 2025, legislative amendments were translated into practice through principle decisions and guidance documents issued by the Board. Nevertheless, an assessment of the DP Law's normative structure and internal system reveals that material structural and conceptual divergences from the GDPR continue to persist.

In this regard, the Medium-Term Program for the 2026–2028 period indicates that efforts aimed at aligning the DP Law with the GDPR are expected to be completed by the third quarter of 2026. This policy objective suggests that the ongoing alignment process is unlikely to remain confined to secondary legislation and non-binding guidance, and that more comprehensive and systemic amendments at the statutory level may be placed on the legislative agenda.

Looking ahead, it is anticipated that the DP Law will be further aligned with the principles of transparency, accountability, and risk-based regulation embedded in the GDPR, accompanied by targeted yet impactful structural revisions designed to enhance the effectiveness of the data protection framework in practice. In particular, expectations focus on a measured but functional expansion of the DP Law's conceptual scope to better capture modern data processing activities, especially in relation to profiling, the definition of personal data breaches, and the clearer identification of actors involved in data transfers.

Moreover, the explicit incorporation of transparency and accountability principles into the DP Law may extend data controllers' obligations beyond mere compliance, introducing

a duty to demonstrate and document compliance. From this perspective, a reassessment of the current VERBIS-centered compliance model appears likely, potentially paving the way for a more dynamic accountability framework grounded in record-keeping, risk assessments, and internal control mechanisms.

Finally, from an enforcement standpoint, one of the most prominent reform expectations concerns the transformation of the sanctions regime from a system based on fixed monetary penalties to a turnover-based and proportionate fine structure, calibrated to the nature of the infringement and the economic capacity of the data controller. Should such a model be adopted, the sanctions framework under the DP Law would be expected to converge more closely with the GDPR's penalty regime, thereby enhancing both its deterrent effect and practical effectiveness.

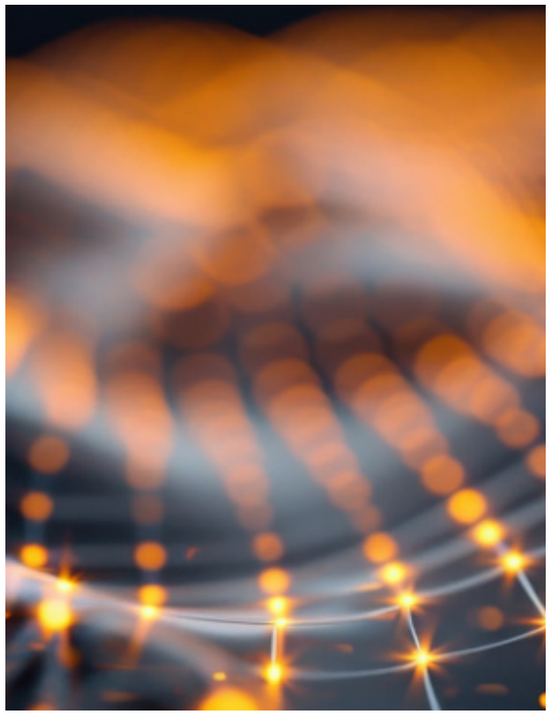
II. Artificial Intelligence

As detailed under Section A.II.1. Developments in the Field of Artificial Intelligence although a comprehensive and uniform regulatory framework governing artificial intelligence has not yet entered into force in Türkiye, it is evident that the legislative process is actively ongoing and that the regulatory landscape may undergo significant development in the near future. At present, the agenda of the Grand National Assembly of Türkiye includes numerous draft bills that directly or indirectly address artificial intelligence, covering a wide range of issues such as the legal nature of AI systems, content generated or replicated through the use of AI, the liability of digital platforms, the protection of personal data, and sanctions regimes. However, as these proposals remain at the committee stage and have not yet completed the legislative process, they do not currently give rise to binding legal obligations.

That said, when assessed collectively, the substance of these legislative proposals suggests a regulatory trajectory that places particular emphasis on deepfake and manipulative content, the auditability and oversight of AI-enabled services, the obligations of platforms and service providers, the protection of special categories of personal data, and the strengthening of administrative sanctions. From the perspective of entities that develop, deploy, or provide services based on artificial intelligence technologies, this signals that more detailed and stringent compliance obligations may emerge in the medium term.

At the same time, an examination of Türkiye's policy documents indicates that the regulatory approach is not confined to domestic legal considerations but is instead shaped by a strategic objective of alignment with EU legislation. In this regard, the Medium-Term Program explicitly states that efforts to harmonize national legislation with the EU Artificial Intelligence Act ("**AI Act**") are targeted for completion by the second quarter of 2026. Against this backdrop, it appears likely that core elements of the AI Act—including a risk-based regulatory approach, additional obligations for high-risk AI systems, principles of transparency and human oversight, as well as data governance and accountability mechanisms—will be gradually reflected in Turkish law.

Accordingly, while the entry into force of a binding and comprehensive artificial intelligence law in the short term is not anticipated, it is expected that, over the medium term, the regulatory framework in Türkiye will evolve in parallel with the AI Act, through sector-specific and phased regulatory initiatives. This evolution is likely to result in a more predictable yet more demanding compliance regime, particularly for digital platforms, data-intensive industries, and providers of AI-based services.



III. Cybersecurity

As outlined under Section A.II.2. 2. Legislative Developments in the Field of Cybersecurity the Cybersecurity Law No. 7545, which was published and entered into force on 19 March 2025, has established a national security–oriented framework to address cyber threats across a broad scope encompassing both the public and private sectors. With this Law, a comprehensive umbrella regulation in the field of cybersecurity has entered into force for the first time, providing legal safeguards for key areas such as the identification and mitigation of cyber risks, the formulation of national policies and strategies, the protection of critical infrastructures, and incident response mechanisms. The Cybersecurity Law also provides for the establishment of the Cybersecurity Directorate under the Presidency and delineates the scope of its duties, powers, and responsibilities.

That said, the adoption of secondary legislation governing the implementation of the Cybersecurity Law remains pending, and the completion of detailed regulatory instruments setting out the procedures and principles of application is still anticipated. In this regard, the 2026 Presidential Annual Program identifies digital transformation and cybersecurity among the priority areas of public policy, emphasizing the effective implementation of the existing legal framework, the strengthening of institutional capacity, and the finalization of implementation-oriented regulations. Accordingly, it is expected that, during 2026, the secondary legislation required for the implementation of the Cybersecurity Law will enter into force, cybersecurity standards across both the public and private sectors will be reinforced, and an application framework aligned with international regulations will be established.

Moreover, in line with the EU acquis alignment approach adopted under the Medium-Term Program, it is envisaged that, in the medium term, secondary cybersecurity legislation aligned with the EU Directive on Measures for a High Common Level of Cybersecurity Across the Union (the "**NIS2 Directive**") and the EU Cyber Resilience Act ("**CRA**") will be placed on the regulatory agenda. Within this scope, the introduction of more detailed technical and administrative obligations—particularly for critical infrastructures, digital service providers, and data-intensive sectors—stands out among the expected developments.

APPENDIX 1 KEY TERMS

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

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

Data Controller refers to a natural or legal person who determines the purposes and means of processing personal data and is responsible for the establishment and management of the data recording system.
Data Processor means a natural or legal person who processes personal data on behalf of a data controller, based on the authority given by the data controller.

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

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

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

AUTHORS

C. HAZAL BAYDAR, LL.M.
PARTNER
hbaydar@morogluarseven.com

CANSU ÖZGÜVEN, LL.M.
SENIOR ASSOCIATE
cozguven@morogluarseven.com

AYŞEGÜL DAĞHAN
ASSOCIATE
adaghan@morogluarseven.com

MOROĞLU ARSEVEN

TURKISH DATA PROTECTION LAW

ROUNDUP | 2026