Legal 500
Country Comparative Guides 2025

Türkiye

Data Protection & Cybersecurity

Contributor

Balcıoğlu Selçuk Eymirlioğlu Ardıyok Keki Attorney Partnership

Kağan Dora

Partner | kdora@baseak.com

Neslihan Kasap

Senior Associate | nkasap@baseak.com

Cansu Duman

Senior Associate | cduman@baseak.com

Emir Gönen

Senior Associate | egonen@baseak.com

Almira Akbay

Associate | aakbay@baseak.com

Anıl İçintek

Associate | aicintek@baseak.com

This country-specific Q&A provides an overview of data protection & cybersecurity laws and regulations applicable in Türkiye.

For a full list of jurisdictional Q&As visit **legal500.com/guides**

Türkiye: Data Protection & Cybersecurity

1. Please provide an overview of the legal and regulatory framework governing data protection, privacy and cybersecurity in your jurisdiction (e.g., a summary of the key laws; who is covered; what sectors, activities or data do they regulate; and who enforces the relevant laws).

Protection of personal data is mainly regulated by Article 20/3 of the Turkish Constitution and the Personal Data Protection Law (the "**DPL**"), which came into force on April 7, 2016. The Turkish Constitution mainly sets forth that each individual has right to request protection of their personal data. The DPL regulates general principles of data processing and imposes several obligations on data controllers and data processor for their data processing activities. Secondary regulations of the DPL include the following:

- Regulation on the Data Controllers' Registry ("**VERBİS**")
- Regulation on Erasure, Destruction and Anonymization of Personal Data
- Communiqué on Rules and Procedures for Application to Data Controller
- Communiqué on Rules for Fulfilling the Obligation to Inform Data Subjects

The DPL applies to **(i)** natural persons whose personal data are processed and **(ii)** natural or legal persons who process such data, wholly or partly by automatic means, or otherwise than by automatic means that form part of a data registry. The DPL applies to all data processing activities, regardless of the sector in which that data controller is operating. In addition, several regulations are specific to sectors such as banking, capital markets, telecommunication, health, payment services, etc.

The DPL does not have a specific provision on its territorial scope. The Turkish Personal Data Protection Authority and Board (the "**DPA**") is the regulatory authority that enforces the DPL and the recently published Guidelines on Cross-Border Data Transfers by the DPA make reference to the principle of territoriality regulated under the Turkish Penal Code since there is no explicit provision in the DPL for determining of its territorial scope. However, the Guidelines further underline the fact that the strict application of the principle of territoriality does not serve the purpose of ensuring an effective protection in view of the emergence and widespread use of technologies that enable cross-border data processing. The DPA therefore concludes that when interpreting the territorial scope, the principle of effect should be applied instead of the principle of territoriality. In fact, in one of the example scenarios provided in the Guidelines, the DPA illustrates that processing activity in relation to orders received through a website operated by a third country company that is not resident in Turkey but targets data subjects in Turkey falls within the territorial scope of the DPL. Accordingly, in broader terms, the DPA applies the DPL to data processing activities that concern individuals in Turkey and/or have a consequence on individuals in Turkey.

With respect to legal and regulatory framework governing cybersecurity, Turkey adopted its first comprehensive law in the field of cybersecurity called the Cybersecurity Law No. 7545 "**CSL**" on 19 March 2025. The CSL establishes a unified cybersecurity framework, consolidating cybersecurity activities under the newly created Cybersecurity Directorate ("**Directorate**") and the restructured Cybersecurity Board, bringing together responsibilities previously held by the Ministry of Transport and Infrastructure, the Information and Communication Technologies Authority, and the Digital Transformation Office of the Presidency.

That being said, cybersecurity requirements exist for certain specific sectors such as banking and finance, health, electronic communications, or energy sector. In this regard, for specific industries there are certain security requirements. Unlike legal and regulatory framework governing data protection, sectors covered by cybersecurity regulations and their enforcement authorities are subject to variation.

2. Are there any expected changes in the data protection, privacy or cybersecurity landscape in 2025 - 2026 (e.g., new laws or regulations coming into effect, enforcement of such laws and regulations, expected regulations or amendments)?

There has been an ongoing initiative to fully harmonize the DPL with the GDPR for some time. According to the Presidential Annual Program for 2025 and the Medium-Term Program (2025-2027), published in the Official

Gazette, it is stated that the efforts to harmonize the DPL with the GDPR will be accelerated, with plans to complete the harmonization by the fourth quarter of 2025.

Within 2025, following the enactment of the CSL, we expect secondary regulations specific to cybersecurity to be introduced in order to clarify the details of its implementation.

3. Are there any registration or licensing requirements for entities covered by these data protection and cybersecurity laws, and if so what are the requirements? Are there any exemptions? What are the implications of failing to register / obtain a licence?

The DPL requires real persons and legal entities processing personal data to register with VERBİS before carrying out personal data processing activities. The registration process is carried out through an online system and is free of charge.

During registration, data controllers must provide the following information to the DPA (from a drop-down list):

- Data subject categories
- Personal data categories
- Processing purposes
- Data recipients
- Retention periods
- Information on a cross-border transfer
- Administrative and technical measures taken for data protection.

The registration obligation applies if the data controller fulfils any of the following:

- Who are resident abroad and carry out personal data processing activities that have a consequence on individuals in Turkey,
- Who are resident in Turkey;
  - and has more than 50 employees **or** whose yearly financial balance exceeds TRY 100 million or
  - and whose main operations are based on processing special categories of personal data.

Under the decisions of the DPA, the following types of data controllers are exempt from this obligation:

- Persons who process personal data as part of any data recording system, solely through non-automatic means,
- Notaries,
- Associations, foundations, and unions established in Turkey that process personal data limited to their areas of activity,
- Political parties,
- Lawyers,
- Independent accountants, financial advisors and certified public accountants,
- Mediators,
- Customs brokers and authorized customs brokers.

The above-listed exemptions do not apply to data controllers that are resident abroad.

Failure to register with VERBIS may result in administrative fines ranging from TRY 272,380 and TRY 13,620,402 for the year 2025.

As regards the cybersecurity laws; the CSL stipulates that certain companies will be subject to certification, authorization, and accreditation requirements although the details are not specified. We opine that more information on the obligations regarding licensing may be clarified through secondary regulations.

4. How do the data protection laws in your jurisdiction define “personal data,” “personal information,” “personally identifiable information” or any equivalent term in such legislation (collectively, “personal data”)? Do such laws include a specific definition for special category or sensitive personal data? What other key definitions are set forth in the data protection laws in your jurisdiction (e.g., “controller”, “processor”, “data subject”, etc.)?

Under the DPL, **personal data** means any information relating to an identified or identifiable natural person.

Data relating to race, ethnic origin, political opinions, philosophical beliefs, religion, sect or other beliefs, appearance and dressing, membership in an association, foundation or trade-union, health, sexual life, criminal conviction and security measures, biometrics and genetics are considered as **special categories of personal data**.

Other key definitions include:

- **Data Processing:** Any operation that is performed on personal data as part of a data filing system, wholly or partially by automated or non-automated means. This includes collection, recording, storage, protection, alteration, adaptation, disclosure, transfer, retrieval, making data available for collection, categorization or

preventing its use.
- **Data Controller:** The natural or legal person who determines the purpose and means of the data processing and is responsible for establishing and managing the data registry system.
- **Data Processor:** The natural or legal person that processes personal data based on the authority granted by and on behalf of the data controller.
- **Data subject:** The natural person whose personal data is processed.
- **Data Controller Representative:** A legal entity resident in Turkey or a natural person who is a citizen of the Republic of Turkey authorized to represent non-resident data controllers in the matters such as such as receiving or accepting notifications and correspondence by the TR DPA, transmitting the requests directed at the data controller by the TR DPA, transmitting the data controller's response to the data subjects and conducting transactions concerning VERBIS on the data controller's behalf.

5. What principles apply to the processing of personal data in your jurisdiction? For example: is it necessary to establish a "legal basis" for processing personal data?; are there specific transparency requirements?; must personal data only be kept for a certain period? Please provide details of such principles.

Personal data processing activities must be conducted in compliance with the following principles that are outlined as "fair processing principles." They are:

- Conformity with the law and good faith,
- Being accurate and if necessary, up to date,
- Being processed for specified, explicit, and legitimate purposes,
- Being relevant, limited and proportionate to the purposes for which the data are being processed,
- Being stored only for the time designated by relevant legislation or necessitated by the purpose for which the data is being collected.

In addition, Articles 5 and 6 of the DPL regulate the legal bases for processing of personal data. Data controllers must rely on a legal basis while processing personal data. Principally, under Article 5/1, personal data cannot be processed in the absence of explicit consent. However, explicit consent will not be required if any one of the legal bases listed below are present:

- Processing is explicitly foreseen under the applicable laws,
- Processing is mandatory for the protection of life or to prevent the physical injury of a person or of any other person, in cases where that person cannot express his/her consent due to physical disability or that person's consent is legally invalid,
- Processing is directly linked to and necessary for the conclusion or performance of an agreement, where the personal data belongs to the parties of that agreement,
- Processing is mandatory for fulfilling the legal obligations of the data controller,
- The data is made manifestly public by the data subject,
- Processing is mandatory for the establishment, exercise or protection of any right,
- Processing is based on the legitimate interest of the data controller.

Please see Question 7 for conditions of processing special categories of personal data.

As regards the transparency requirements, data controller that meet certain criteria should register with VERBİS, which is a public registry, before carrying out personal data processing activities. Please see Question 3 for information to be provided in the VERBİS system. Moreover, as per Article 10 of the DPL, a data controller is required to inform each data subject related to any data processing activity while obtaining personal data and before carrying out such processing activity, regardless of the lawful ground. Information notices must consist of the following:

- Contact information of the data controller or its' representative,
- Purpose of personal data processing activity,
- Legal ground of personal data processing activity,
- Methods of personal data collection,
- Recipient of personal data and purpose of personal data transfer,
- Data subject's rights as stipulated under Article 11 of the Turkish DPL.

6. Are there any circumstances for which consent is required or typically obtained in connection with the processing of personal data? What are the rules relating to the form, content and administration of such consent? For instance, can consent be implied, incorporated into a broader document (such as a terms of service) or bundled with other matters (such as consents for multiple processing operations)?

In cases where none of the legal bases listed under Question 5 is presented, explicit consent is required for the processing activity.

Explicit consent must be given freely (i.e., the data subject must have a real choice) by a clear affirmative act, based on a specific subject matter and obtained upon providing necessary information to the data subject.

Where processing is based on explicit consent, the burden of proof is on the data controller that the data subject has granted its explicit consent. Data subjects have the right to withdraw their consent at any time.

Consent should be explicit; it cannot be incorporated into a broader document such as the terms of service or privacy notices nor can it be bundled with other matters. Principally, consent should be obtained separately for each processing activity. Also, the consent will be deemed invalid if the data controller requires consent as a pre-condition for providing its services.

7. What special requirements, if any, are required for processing particular categories of personal data (e.g., health data, children's data, special category or sensitive personal data, etc.)? Are there any prohibitions on specific categories of personal data that may be collected, disclosed, or otherwise processed?

Article 6 of the DPL sets out special conditions for processing special categories of personal data. Accordingly, all special categories of personal data (including health and sexual life) may be processed based on one of the following legal bases:

- The data subject has explicitly consented,
- Processing is explicitly provided for under the law,
- Processing is necessary for the protection of life or physical integrity of a person themselves or of any other person, who is unable to disclose their consent due to a physical disability or whose consent is not deemed legally valid,
- Processing relating to personal data which has been made public by the data subject provided that the processing is limited to the data subject's aim of making such data public,
- Processing is necessary for the establishment, exercise or defence of legal rights,
- Processing is necessary for the protection of public health, preventive medicine, medical diagnosis, treatment and care services, planning, management and financing of health services by persons under the obligation of secrecy or authorized institutions and organizations,
- Processing is necessary for complying with legal obligations in the fields of employment, occupational health and safety, social security, social services and welfare,
- Processing is carried out by foundations, associations and other non-profit organizations or other establishments with a political, philosophical, religious or trade union aim, on the condition that the processing complies with the legislation to which these organizations are subject and their purposes, limited to their fields of activity and not disclosed to third parties; and relates to the members or to former members of these organizations or to persons who have regular contact with them.

Moreover, data controllers must take the necessary administrative and technical measures announced by the DPA in its decision dated January 31, 2018 and numbered 2018/10 to ensure the security of such data.

8. Do the data protection laws in your jurisdiction include any derogations, exemptions, exclusions or limitations other than those already described? If so, please describe the relevant provisions.

Article 28 of the DPL sets forth full and partial exemptions for the below-listed activities:

Full exemptions from the DPL – *Listed activities are fully exempted from the DPL.*	personal data processing by natural persons for purely personal activities or for household activities
	personal data processing for official statistics through anonymizing the data for purposes such as research, planning and statistics
	personal data processing with artistic, historical, literary or scientific purposes, or within the scope of freedom of expression provided that national defense, national security, public security, public order, economic security, right to privacy or personal rights are not violated so long as the process doesn't constitute a crime
	personal data processing within the scope of preventive, protective and intelligence activities carried out by public institutions and organizations duly authorized and assigned by law to maintain national defense, national security, public security, public order or economic security
	personal data processing by judicial authorities or execution authorities with regard to investigation, prosecution, judicial or execution proceedings
Partial exemptions -*Listed activities are exempted from the obligation to inform data subjects, to respond data subjects' request (except for the request for compensation) and to register with VERBİS*	necessary processing for the prevention of committing a crime or for criminal investigation
	processing of data that have been made public by the data subject himself/herself
	necessary processing for performance of supervision or regulatory duties and disciplinary investigations and prosecution, to be carried out by the assigned and authorized public institutions and organizations and by public professional organizations, in accordance with the law
	necessary processing for the protection of economic and financial interests of the state that are related to budget, tax and financial matters

9. Does your jurisdiction require or recommend risk or impact assessments in connection with personal data processing activities and, if so, under what circumstances? How are these assessments typically carried out?

The DPL does not directly recognize "Data Protection Impact Assessment." However, data controllers are required to process personal data in line with general

data processing principles. Therefore, although this concept is not directly regulated, data controllers should carry out risk assessments before conducting any personal data processing activity.

Additionally, in its decisions the DPA introduced a "legitimate interest balance test." This must be carried out if the data is processed and/or transferred by relying on the data controller's legitimate interest. In such a case, the data controller must demonstrate that it has an existing, specific and clearly legitimate interest; and this interest does not override the rights and freedoms of data subjects.

Moreover, although the DPL or its secondary legislation do not emphasize the need to conduct transfer impact assessments, the amended TR DPL states that a controller or processor may transfer personal data to a third country only if appropriate safeguards are in place and provided that data subjects have enforceable rights and effective remedies in the destination country. The TR DPA may therefore require appropriate documentation (i.e. TIAs) to demonstrate compliance with this obligation.

10. Are there any specific codes of practice applicable in your jurisdiction regarding the processing of personal data (e.g., codes of practice for processing children's data or health data)?

There are no specific codes of practice applicable in Turkey regarding the processing of personal data. That being said, certain guidelines such as "Protection of Minors' Personal Data – Things to be Considered by Product and Service Developers", Recommendations for Protection Privacy in Mobile Applications, Guideline on the Processing of Special Categories of Personal Data, Guideline on Issues to be Considered in the Processing of Genetic Data and Guideline on Issues to be Considered in the Processing of Biometric Data are published by the DPA to further elaborate on the processing of certain personal data categories. Nevertheless, data controllers and data processors should comply with general principles of data processing set forth under the DPL. Please see Question 1 for details.

11. Are organisations required to maintain any records of their data processing activities or establish internal processes or written documentation? If so, please describe how businesses typically meet such requirement(s).

Yes, data controllers that are required to register with VERBİS must prepare a personal data processing inventory and keep it up to date. This inventory must stipulate the data controller's personal data processing activities; they must be based on its business processes and include:

- The reasons and legal grounds for processing,
- The personal data categories,
- The data recipient groups,
- The data retention period,
- Which personal data (if any) will be transferred to foreign countries and the technical and
- The administrative measures in place in order to provide protection of personal data.

In practice, organizations can keep such inventory records as excel sheets or can use data management software developed for inventory keeping.

As regards establishing internal processes or written documentation, data controllers that are required to register with VERBİS must prepare a data retention and destruction policy (*please see Question 12 for details*). Furthermore, as per the DPA's decision dated 24 January 2019, data controllers must implement a data breach incident plan, which should include matters such as the internal reporting line, responsible persons for notification and the assessment process of possible outcomes of breaches.

12. Do the data protection laws in your jurisdiction require or recommend data retention and/or data disposal policies and procedures? If so, please describe such requirement(s).

As per the Regulation on Deletion, Destruction or Anonymization Personal Data ("**Deletion Regulation**"), data controllers that are required to register with VERBİS are also obliged to draft a data retention and destruction policy. This policy should at least include following items:

- Purpose of issuing the policy,
- The recording mediums regulated by the policy,
- Definitions of technical and legal terms used in the policy,
- Explanations of the legal, technical or other reasons requiring storage and disposal of personal data,
- Technical and organizational measures taken to prevent unlawful processing of and access to personal data and to store personal data securely,
- Technical and organizational measures taken for lawful disposal of personal data,
- Definitions of titles, units and job descriptions of

those who are involved in personal data storage and disposal processes,
- Table demonstrating storage and disposal periods,
- Periodical destruction periods,
- Any alterations being made to the current policy, if any.

According to the Deletion Regulation, data controllers are required to define retention periods for each type of personal data and delete/destruct or anonymize the personal data periodically (these can be at most six months). Also, data controllers should keep the records related to the deletion, destruction and anonymization of personal data for three years, excluding other legal obligations.

Additionally, under the DPL, personal data must be retained for the period provided under applicable laws or for a period necessary for the purpose of the data processing. Data controllers should consider the following when determining retention periods necessary for the purposes of data processing:

- The customary period generally accepted within the relevant sector,
- The period required for the data processing and the term of the legal relationship with the data subject,
- The period required for satisfying the legitimate interest of the data controller in accordance with the rules of law and good faith,
- The legal period for continuance of risks, costs and duties of processing,
- The fact that whether the retention period is suitable for true and up-to-date processing,
- The statutory retention period arising from applicable law, and
- The limitation period for exercise of a right relating to personal data.

Data controllers should also delete, destruct or anonymize the personal data ex officio or upon the data subject's request, if the purposes of processing no longer exist.

13. Under what circumstances is it required or recommended to consult with the applicable data protection regulator(s)?

The DPL, unlike GDPR, does not require data controllers or data processors to consult with the DPA before carrying out data processing activities.

14. Do the data protection laws in your jurisdiction require the appointment of a data protection officer, chief information security officer, or other person responsible for data protection? If so, what are their legal responsibilities?

The DPL does not require the appointment of a data protection officer. However, it is advisable to establish a privacy committee or appoint a person who will be responsible for the implementation of internal privacy policies and procedures to ensure compliance with the DPL.

Furthermore, there are no general requirement to appoint a chief information security officer under Turkish legislation. However, certain regulated sectors such as banking, payment services and telecommunication entail the designation of personnel who is in charge of information security. In this respect, contrary to the discretional approach in relation to the requirement of appointment of a data protection officer, these regulated sectors oblige actors that fall within the scope of related legislations to appoint an information security officer. For instance, a telecommunications operator must designate an information security management system. Similarly, personnel must be assigned with duties, powers and responsibilities regarding the information security management system in payment sector and such personnel should continuously monitor the compliance of the information security management system with the legislation on information security standards, take the necessary measures to ensure compliance and regularly report on the compliance status.

15. Do the data protection laws in your jurisdiction require or recommend employee training related to data protection? If so, please describe such training requirement(s) or recommendation(s).

There is no specific requirement or recommendation under the DPL for providing employee training. However, in its Guideline on Technical and Administrative Measures, the DPA considers employee training as one of the necessary administrative measures that data controllers should take in order to ensure personal data security. Additionally, in data breach investigations, the DPA generally requests evidence from data controllers demonstrating that employee training has been duly provided. Therefore, it is recommended to have regular employee training in place.

16. Do the data protection laws in your jurisdiction require controllers to provide notice to data subjects of their processing activities? If so, please describe such notice requirement(s) (e.g., posting an online privacy notice).

Data controllers must provide data subjects with the following information at the time of collecting their personal data, in clear and simple language:

- The identity of the data controller and its representative, if any,
- The purpose(s) for processing the personal data,
- The purposes for transferring the personal data and the persons to which the data may be transferred,
- The method and legal grounds for collecting the personal data,
- The data subjects' rights under Article 11 of the DPL.

If personal data is not collected from the data subject, the information provision obligation must be fulfilled **(i)** within a reasonable period after the collection of personal data, **(ii)** (if the personal data will be used for communication with data subject) at the time of the first contact with data subject, and **(iii)** (if the personal data will be transferred), at the time of the first transfer of personal data.

The information obligation must be complied with in all cases, whether data processing is based on explicit consent or on another legal ground.

17. Do the data protection laws in your jurisdiction draw any distinction between the responsibility of controllers and the processors of personal data? If so, what are the implications?

The provisions of the DPL and its secondary legislation are applicable to data controllers; thus, liability lies with the data controller. However, data controllers are jointly responsible with data processors for taking the necessary technical and administrative measures to ensure the appropriate level of security, to prevent illegal access to personal data and to ensure the protection of personal data. On the other hand, the Amendment introduces new provisions that are also applicable to data processors (e.g., obligations in relation to cross-border personal data transfers) and the DPA may impose an administrative fine to data processors for failure to notify the DPA within 5 business days of the execution of the standard contractual clauses for cross-border transfers.

18. Please describe any restrictions on monitoring, automated decision-making or profiling in your jurisdiction, including through the use of tracking technologies such as cookies. How are these or any similar terms defined?

Under the DPL, there are no specific provisions related to monitoring or profiling activities through tracking technologies. However, the use of cookies and other trackers for processing personal data must be performed in compliance with the DPL's principles since cookies are considered personal data according to the interpretation of the DPA within the scope of the definition of personal data provided under the DPL.

In June 2022, the DPA published Cookie Guideline, which is heavily based on the EU's cookie guidelines. In the Cookie Guideline, the DPA lists several types of cookies and explicit consent requirement for the use of such cookies, according to the purpose of each cookie type. For instance, the Cookie Guideline states that cookies used for online behavioral advertising require explicit consent. In addition, the consent requirement extends to all cookies used in advertising (e.g., cookies used for the purpose of frequency capping, financial logging, ad affiliation, click fraud detection, research and market analysis, product improvement and debugging). On the other hand, the DPA states that several types of cookies (functional cookies, website security cookies, load balancing session cookies, etc.) might be used by relying on legal bases (e.g., legitimate interest) other than explicit consent.

In addition to above, pursuant to the Banking Sector the Good Practices Guide updated by the DPA on January 2025, the DPA lists the criteria to be considered in automated decision making, including but not limited to the following:

- If the data controller is able to achieve its desired purpose with a less intrusive method (e.g., by using anonymous data), it cannot be said that the automated decision-making activity is based on legitimate interest.
- The type, nature, source and amount of personal data to be processed should be evaluated and excessive processing activities should be prevented (e.g., representative data may be used to model real personal data).
- Risk assessment in data processing should be made in a more sensitive manner, taking into account the characteristics of artificial intelligence and big data.

19. Please describe any restrictions on targeted advertising and/or behavioral advertising. How are these terms or any similar terms defined?

There is no definition of targeted advertising and/or behavioural advertising under the DPL. However, the Cookie Guideline state that online behavioural advertising practices constitute of; **(i)** monitoring data subjects' activities on the internet, **(ii)** analysing and profiling these activities, **(iii)** matching the advertisements with the ads and displaying these ads to relevant data subjects. Nevertheless, any activity should comply with the general rules and principles stipulated under the DPL.

20. Please describe any data protection laws in your jurisdiction restricting the sale of personal data. How is the term "sale" or such related terms defined?

Turkish law does not regulate the sale of personal information. As the sale would inherently require the transfer of personal data, any such transfer to third parties should be carried out by considering the transfer rules stipulated under Article 8 and 9 of the DPL.

21. Please describe any data protection laws in your jurisdiction restricting telephone calls, text messaging, email communication, or direct marketing. How are these terms defined?

Law No. 6563 on the Regulation of Electronic Commerce ("**E-Commerce Law**") and its secondary regulations regulates commercial marketing communications. Commercial electronic messages are defined as messages containing data, audio or visual content that are transmitted electronically for commercial purposes by making use of communication channels such as telephone, call centers, faxes, automated calling machines, smart voice recording systems, email and SMS. Therefore, direct marketing activities fall within the scope of the E-Commerce Law. As a general rule, in order to send commercial electronic messages, the recipients' consent should be obtained, except for the exceptions foreseen in the E-Commerce Law (e.g., sending transactional messages). Moreover, since direct marketing communications involve personal data processing activities, such activity must also be carried out in accordance with applicable legal bases under the DPL.

Under the E-Commerce Law, a central database, known as the Commercial Electronic Message Management System ("**IYS**"), was established. The system is designed to store all consent records (opt-in records) of subscribers/users that can be reviewed and monitored by the government and subscribers/users via the system. Companies wishing to send B2B or B2C electronic communications in all sectors are required to register with IYS and to transfer their consent records (for B2C communication only) to IYS.

22. Please describe any data protection laws in your jurisdiction addressing biometrics, such as facial recognition. How are such terms defined?

Biometric data is considered a special category of personal data under the DPL, but the DPL does not define what comprises biometric data. The DPA, in several decisions and within its Guide on Matters to be Considered in the Processing of Biometric Data published on September 17, 2021, has defined biometric data by referring to the GDPR's definition, which is *personal data resulting from specific technical processing relating to the physical, physiological or behavioral characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data.*

Please see Question 7 for the conditions for processing biometric data.

23. Please describe any data protection laws in your jurisdiction addressing artificial intelligence or machine learning ("AI").

There are no data protection laws in Turkey addressing artificial intelligence or machine learning. On the other hand, in its Recommendations on the Protection of Personal Data in the Field of Artificial Intelligence and the Bulletin numbered 1 and dated July 2023, DPA underlines that AI practices based on personal data processing must be in compliance with the DPL and suggests the following, among others:

- Personal data processing principles must be adhered to, and a data security-based approach must be adopted,
- A perspective that focuses on preventing and reducing potential risks and considers human rights, the functioning of democracy, and ethical values should be adopted,
- If a high risk is foreseen in terms of protection of personal data, a DPIA should be implemented, and the legality of the data processing activity should be decided within this framework,

- Data protection by design and default should be implemented,
- If special categories of personal data will be processed, technical and administrative measures should be applied more strictly,
- If the same result can be achieved without processing personal data, anonymization of the collected personal data should be preferred,
- The data controller or data processor status of the parties should be determined at the beginning of the practice and the legal relationship in this regard, in accordance with the DPL and the secondary legislation,
- Individuals should be given the right to object to data processing activities by using the technologies that affect their views and personal development.

Finally, it is announced in the Presidential Annual Program for 2025 and the Medium-Term Program (2025-2027) that necessary legal regulations will be made to meet the needs arising from AI technologies. In its Activity Report for the year 2024, the DPA also stated that in 2025, two more studies on artificial intelligence are planned to be published.

24. Is the transfer of personal data outside your jurisdiction restricted? If so, please describe these restrictions and how businesses typically comply with them (e.g., does a cross-border transfer of personal data require a specified mechanism or notification to or authorization from a regulator?)

Article 9 of the DPL and the Regulation on Cross-Border Transfers ("**Regulation**") set out rules and restrictions regarding cross-border transfers of personal data. In this respect, the following mechanisms may be utilized for cross-border transfers of personal data by both data controllers and processors:

- **Adequacy decisions:** The cross-border transfer of personal data to a country, specified sector within that country or an international organization can be realized in the existence of **(i)** any of the legal bases provided under the DPL (e.g., legitimate interest or contractual necessity) and **(ii)** an adequacy decision adopted for the country to which data will be transferred, or a specified sector within that country or an international organization to which the transfer shall be made.
- **Appropriate safeguards:** In the event that the DPA does not adopt an adequacy decision, cross-border personal data transfers may nevertheless occur if **(i)** one of the legal bases set forth under the DPL is present, **(ii)** the data subject has the means to exercise their rights and to have recourse to effective legal remedies in the recipient country and **(iii)** the parties have provided one of the following appropriate safeguards provided under the DPL. The safeguards include, **(i)** execution of binding corporate rules approved by the DPA, **(ii)** execution of standard contracts published by the DPA and notifying the DPA within 5 business days of execution of these contracts, and **(iii)** execution of an undertaking letter and approval of the undertaking letter by the DPA.
- **Transfers for specific situations:** In addition to the aforementioned, for a variety of legal bases, including explicit consent, personal data may be transferred outside of Turkey in the absence of an adequate decision or appropriate safeguards provided that such transfers will not be repetitive (i.e., the transfers will only take place one or a few times).

Moreover, the Guidelines on Cross-Border Data Transfers provide details on procedures and principles regarding cross border personal data transfers and shed light on the territorial scope of the DPL, which has been highly controversial in terms of application of the DPL to data controllers abroad.

25. What personal data security obligations are imposed by the data protection laws in your jurisdiction?

Data controllers and data processors are obliged to ensure that all necessary technical and organizational measures for ensuring an appropriate level of security is in place to prevent unlawful processing of personal data, to prevent unlawful access to personal data and, to ensure the protection of personal data.

There is no exhaustive list of measures to be taken by the data controllers or data processors, and data controllers themselves are expected to decide which security measures should be adopted in order to ensure the appropriate level of security in line with the nature of the personal data and the risks posed by the data processing activity concerned. In its Data Security Guidelines, the DPA recommends certain administrative and technical measures including:

- Regular awareness trainings,
- Preparation of the relevant policies for personal data processing (e.g., data retention policy, data security policy, etc.),
- Carrying out a risk analysis to define the risks and solutions related to the data processing activities,

- Carrying out internal periodical and/or random audits,
- Preparing an access authorization matrix and ensuring authorization controls,
- Ensuring network security and application security,
- Conducting penetration tests,
- Deletion, destruction and anonymization of personal data.

On the other hand, for the processing of special category personal data, the DPL stipulates that "sufficient measures," as determined by the DPA, must be adopted. *Please refer to Question 7 for the relevant DPA decision.*

26. Do the data protection laws in your jurisdiction impose obligations in the context of security breaches which impact personal data? If so, how do such laws define a security breach (or similar term) and under what circumstances must such a breach be reported to regulators, impacted individuals, law enforcement, or other persons or entities?

The DPL does not explicitly define "security breach." However, the DPL provides that if personal data is obtained illegally by third parties, the data controller must inform the DPA and the relevant data subject(s) as soon as possible.

Pursuant to the DPA's decision dated 24.01.2019 and numbered 2019/10 on Procedures and Principles Regarding Notification of Data Breaches, the DPA indicated that the term "as soon as possible" should be interpreted as 72 hours after becoming aware of the data breach. Therefore, in the event of a security breach affecting personal data, the data controller must notify the DPA within 72 hours after becoming aware of the data breach.

Data subjects must also be notified via appropriate methods as soon as possible after determination of the persons affected by the data breach. Unlike the GDPR, the DPL does not recognize the "risk-based approach" in terms of data breach notification requirements; thus, all personal data breaches require notification.

A notification submitted to the DPA should include the following information, among others:

- A description of the nature of the data, where possible the categories and approximate number of personal data and individuals concerned,
- The contact details of the data controller,
- A description of the likely consequences of the breach, and
- The remedial measures taken or proposed to be taken by the data controller.

The following information should be included in the notification made to the data subjects:

- The date of the breach,
- Information about the categories of personal data affected by the breach,
- The likely consequences of the breach,
- The measures taken or proposed to be taken to reduce or eliminate possible adverse effects,
- The names and contact details of the persons who can provide information about the breach or the full contact details of the data controller.

There is also certain legislation specific to certain sectors, such as telecommunications and finance, that requires notification of security breaches to the relevant sectoral regulatory bodies.

27. Do the data protection laws in your jurisdiction establish specific rights for individuals, such as the right to access and the right to deletion? If so, please provide a general description of such rights, how they are exercised, and any exceptions.

As per the DPL, all data subjects have the right to apply to the controller about themselves:

- To learn whether their personal data is being processed,
- To request information regarding the processing of their personal data,
- To learn the purposes for which their data is being processed and whether the data are used in accordance with these purposes,
- To know the third parties to whom their personal data are transferred domestically or abroad,
- To request a rectification of their personal data in the event the data are incompletely or inaccurately processed,
- To request the deletion or destruction of their personal data,
- To request the transmission to third parties who have received transfers of their personal data of requests for correction, deletion and destruction of their personal data,
- To object to the processing of personal data that leads to an unfavorable consequence for the data subject, in cases where the processed data has been

analyzed only through automatic systems,
- To request compensation for damage arising from the unlawful processing of their personal data.

Although the data subject's right to access is not expressly regulated under the DPL, the DPA recognizes this right within the scope of data subject's right to obtain information. Data subjects may exercise the above-stated rights in line with the Communiqué on Rules and Procedures for Application to Data Controller.

Please refer to Question 8 above for the exceptions.

28. Do the data protection laws in your jurisdiction provide for a private right of action and, if so, under what circumstances?

The DPL reserves data subjects' rights to seek damages in cases of violations of personal rights; therefore, data subjects can claim damages before the courts in this respect.

The Turkish Criminal Code defines several unlawful data processing activities as a crime. Thus, data subject can also file a complaint before the public prosecutor's office if the activities in question also constitute a crime.

29. Are individuals entitled to monetary damages or compensation if they are affected by breaches of data protection law? Does the law require actual and material damage to have been sustained, or is non-material injury to feelings, emotional distress or similar sufficient for such purposes?

Individuals are entitled to request compensation for damage arising from the unlawful processing of their personal data or unlawful access to an information system and similar acts in relation to cybersecurity. Damage may be material as well as non-material.

30. How are data protection laws in your jurisdiction typically enforced?

The DPA has a range of powers it can exercise, including investigating whether the personal data is processed in line with the DPL—either upon a complaint or ex officio—if it learns of an alleged violation, or it can take temporary measures (e.g., restricting or stopping the processing of personal data). The DPA can also impose administrative fines on data controllers or processors for breaching the obligations set out under the DPL.

31. What is the range of sanctions (including fines and penalties) for violation of data protection laws in your jurisdiction?

Administrative Fines Under the DPL	
Misdemeanor	**Fine**
Violation of obligation to inform	TRY 68,083 to TRY 1,362,021
Violation of obligation to register with VERBİS	TRY 272,380 to TRY 13,620,402
Noncompliance with liabilities on data security	TRY 204,285 to TRY 13,620,402
Noncompliance with the DPA's decisions	TRY 340,476 to TRY 13,620,402
Failure to notify the DPA within 5 business days of the execution of the standard contractual clauses for cross-border transfers	TRY 71,965 to TRY 1,439,300

Criminal Penalties Under the Turkish Criminal Code	
Crime	**Penalty**
Recording personal data unlawfully	Imprisonment from one to three years* (*Up to four and a half years in cases of unlawful recording of special categories of personal data)
Delivering, acquiring, or publishing personal data unlawfully	Between two- and four-years' imprisonment
Not destroying data that should be destroyed	Between one- and three-years' imprisonment
Unlawfully accessing or continuously staying in information systems, blocking, or breaking the operation of information systems and altering or destroying data	Imprisonment or judicial fine up to one year
Unlawfully monitoring data transfers within or between information systems by technical means without accessing the system	Imprisonment from one to three years
Preventing or disrupting the functioning of an information system	Imprisonment from one to five years* (*Up to ten years if these acts have been committed on an information system that belongs to a bank or credit institution or a public institution or organization.)
Corrupting, destroying, altering, or making inaccessible the data in an information system, placing data in the system, sending existing data to another location	Imprisonment from six months to three years* (*Up to six years if these acts have been committed on an information system that belongs to a bank or credit institution or a public institution or organization.)
Using devices, software, passwords, or other security codes to commit crimes and producing, importing, delivering, transporting, storing, accepting, selling, supplying, purchasing, or carrying such items	Imprisonment from one year up to three years and judicial fine up to five thousand days

32. Are there any guidelines or rules published regarding the calculation of such fines or thresholds for the imposition of sanctions?

The DPL defines the above non-compliance items resulting administrative fines as "misdemeanors," which are regulated under the Law on Misdemeanors numbered 5326. As per Article 17 of the Law on Misdemeanors, in cases where the law foresees an administrative fine between lower and upper limits, when calculating the administrative fine to be applied, the authorities should consider the **(i)** unjust aspects of misdemeanor, **(ii)** fault of the perpetrator and **(iii)** economic conditions of the perpetrator.

33. Are enforcement decisions open to appeal in your jurisdiction? If so, please provide an overview of the appeal options.

Yes, the DPA's decisions can be appealed before the competent courts (i.e., administrative courts) if the relevant decision issued by the DPA is unlawful.

34. Are there any identifiable trends or regulatory priorities in enforcement activity in your jurisdiction?

On 30 December 2024, the DPA published the Activity Report for the year 2024 which summarizes its activities for the year 2024. The Activity Report indicates that the DPA has issued in the total amount of TRY 552,668,000 administrative fines in 2024. Moreover, the Activity Report indicates that 1345 standard contracts were notified to the DPA in 2024.

That being said, the DPA actively aims for achieving effective compliance with the DPL through ex-officio investigations and data subject complaints. Subjects that the DPA gives utmost importance are, among others, data controllers' obligation to inform, lawful use of explicit consent as a legal basis and registration to VERBİS before carrying out data processing activities. For instance, the DPA officially published a public announcement on its website stating that administrative sanctions have been started to be imposed on data controllers who are found to have failed to fulfil their obligation to register with VERBİS and the DPA's ex-officio investigations on data controllers that failed to fulfil their obligation to register with VERBIS continue.

35. Do the cybersecurity laws in your jurisdiction require the implementation of specific cybersecurity risk management measures and/or require that organisations take specific actions relating to cybersecurity? If so, please provide details.

The CSL mandates organizations to implement the necessary measures as prescribed by legislation and report any vulnerabilities or cyber incidents identified within their service areas to the Directorate. Additionally, the Turkish Presidency's Digital Transformation Office has issued the Information and Communication Security Guide ("**Guide**"), which outlines the information security measures applicable to both public institutions and private organizations. The guide details cybersecurity measures based on various application and technology areas, sectors, and asset groups. Examples include web verification, developing a cybersecurity incident response plan, conducting penetration tests, and implementing security measures for remote working.

36. Do the cybersecurity laws in your jurisdiction impose specific requirements regarding supply chain management? If so, please provide details of these requirements.

According to the Guide, within the scope of the supply chain management, a mechanism should be established to monitor the status of critical components related to the supplied service/product, and that provisions regarding supply chain security should be included in contracts made with contractors.

37. Do the cybersecurity laws in your jurisdiction impose information sharing requirements on organisations?

As per Articles 6 and 18 of the CSL, the Directorate may request the organizations to share information and relevant files. Also, Article 7 of the CSL foresees that organizations that are operating under the CSL are required to promptly and primarily provide the Directorate with any data, information, documents, hardware, software, and any other type of contribution requested within the scope of the duties and activities of the Directorate.

38. Do the cybersecurity laws in your jurisdiction require the appointment of a chief information security officer, regulatory point of contact, or other person responsible for cybersecurity? If so, what are their legal responsibilities?

There is no general requirement to appoint a chief information security officer, regulatory point of contact, or other person responsible for cybersecurity under CSL. However, certain regulated sectors, such as banking, payment services and telecommunication entail the designation of personnel who is in charge of the information security, as stated under Question 14.

39. Are there specific cybersecurity laws / regulations for different industries (e.g., finance, healthcare, government)? If so, please provide an overview.

Yes. Since those sectors are among the critical sectors cybersecurity requirements exist for certain specific sectors (such as banking and finance, health, electronic communications or energy sectors). For instance, banking regulations require banks to prepare information systems policies, procedures, and process documents, as well as an information systems risk management procedure. Additionally, the board of directors of the bank

is obligated to establish an information security management system and ensure its implementation across the entire organization.

In addition to sector specific, security requirement and regulations, the Presidential Circular on Information and Communication Security Measures numbered 2019/12 ("**Circular**") outlines measures for the security of critical data, including requirements for the domestic localization of data and limitations on the use of cloud services. Even though the Circular mainly focuses on public institutions and organizations, it nevertheless applies to private organizations that provide public services in critical infrastructure sectors (i.e., health, electronic communications, energy, water management, banking and finance and transportation).

In parallel with the Circular, the Guide provides details of the information security measures applicable to public institutions and private organizations that fall under the scope of the Circular.

40. What impact do international cybersecurity standards have on local laws and regulations?

The Information and Communication Technologies Authority and the Digital Transformation Office play key roles in aligning national policies with global standards, in Turkey. For instance, the National Cybersecurity Strategy and Action Plans are frequently developed in consideration of international best practices. In this respect, international cybersecurity standards, such as those developed by ISO (e.g., ISO/IEC 27001) or frameworks like the NIST Cybersecurity Framework, often serve as benchmarks for national cybersecurity practices.

41. Do the cybersecurity laws in your jurisdiction impose obligations in the context of cybersecurity incidents? If so, how do such laws define a cybersecurity incident and under what circumstances must a cybersecurity incident be reported to regulators, impacted individuals, law enforcement, or other persons or entities?

The CSL defines cyber incident as "*violation of the confidentiality, integrity, or availability of information systems or data*". As per the CSL, organizations are obliged to notify the Directorate without delay of any vulnerability or cyber incidents detected in the area in which they provide services. However, the CSL does not foresee any obligation to report the impacted individuals.

42. How are cybersecurity laws in your jurisdiction typically enforced?

Since CSL was newly adopted and came into force on 19 March 2025, there have been no findings yet regarding the implementation of the CSL. The Directorate has a range of powers it can exercise, including on-site auditing.

43. What powers of oversight / inspection / audit do regulators have in your jurisdiction under cybersecurity laws.

As per the CSL, Directorate has the power to audit the organizations with respect to any act or transaction falling within the scope of the CSL, when deemed necessary in relation to its duties specified in this CSL. For this purpose, the Directorate may conduct on-site inspections or have such inspections carried out by third parties.

The Directorate is authorized, within the scope of their audit activities, to examine data, documents, electronic infrastructure, devices, systems, software, and hardware in electronic environments; to obtain copies, digital versions, or samples thereof; to request written or verbal explanations on the matter; to prepare the necessary reports; and to inspect facilities and operations.

44. What is the range of sanctions (including fines and penalties) for violations of cybersecurity laws in your jurisdiction?

Administrative Fines Under the CSL	
Misdemeanor	**Fine**
· Not taking legally prescribed cybersecurity measures, · Not promptly reporting vulnerabilities or incidents to the Directorate, · Not procuring cybersecurity products, systems, and services for public institutions and critical infrastructures by the Directorate's authorized experts, manufacturers, or companies	TRY 1,000,000 to TRY 10,000,000
· Failure to obtain approval from the Directorate for the export of cybersecurity products subject to licensing, · Failure to notify the Directorate of mergers, demergers, share transfers, or sales (for companies that produce cybersecurity products, systems, software, hardware, and services)	TRY 10,000,000 to TRY 100,000,000
· Failure to provide the requested information, documents, and materials during audits	TRY 100,000* to TRY 1,000,000* (*If these obligations are not fulfilled by commercial companies, an administrative fine shall be imposed up to five percent of the gross sales revenue, on the condition that such amount is no less than TRY 100,000)

Criminal Penalties Under the CSL	
Crime	**Penalty**
Failure to provide the information, documents, software, data, and hardware requested by the authorities	Imprisonment from one to three years and a judicial fine from 500 to 1,500 days
Failure to obtain required approvals, authorizations, or permits	Imprisonment from two to four years and a judicial fine from 1,000 to 2,000 days
Failure to fulfill obligation to maintain confidentiality	Imprisonment from 4 to 8 years
Making accessible, sharing or offering for sale (either for free or for a fee) personal data or institutional data classified under critical public services, without the consent of the individuals or institutions involved, due to a data breach in cyberspace	Imprisonment from 3 to 5 years
Knowingly creating or spreading false content regarding a cybersecurity data breach with the intent to cause public anxiety, or to target institutions or individuals, despite being aware that no such data breach occurred	Imprisonment from 2 to 5 years
Conducting a cyberattack against the elements constituting the national power of Turkey in cyberspace, or storing any data obtained as a result of such an attack in cyberspace	Imprisonment from 8 to 12 years** (*Provided that the act does not constitute another offense requiring a more severe penalty) (**Those who distribute, transfer, or offer such data for sale shall be sentenced to imprisonment from 10 to 15 years)
Abuse of duties and powers arising from CSL or causing data breach by acting contrary to duties related to the protection of critical infrastructures against cyberattacks	Imprisonment from 1 to 3 years

45. Are there any guidelines or rules published regarding the calculation of such fines or thresholds for the imposition of sanctions?

As for the judicial fines stipulated in the CSL that are imposed on a daily basis, the number of days is determined by taking into account the minimum and maximum limits of the penalty prescribed for each offense. The determined number of days is then converted into a judicial fine, ranging from a minimum of 100 TRY to a maximum of 500 TRY per day, depending on the offender's social and economic circumstances.

For thresholds determined in relation to misdemeanors, *please see Question 33.*

46. Are enforcement decisions open to appeal in your jurisdiction? If so, please provide an overview of the appeal options.

CSL foresees both judicial, criminal and monetary sanctions. These sanctions can be appealed before competent courts (i.e., administrative and criminal courts depending on the type of sanction).

47. Are there any identifiable trends or regulatory priorities in enforcement activity in your jurisdiction?

Turkey is eager to develop new strategies and projects in relation to cybersecurity legislative framework in critical sectors such as banking, health, telecommunications and energy. The Digital Transformation Office has published the Information and Communication Security Audit Guide ("**Audit Guide**") in 2021. The Audit Guide elaborates on audit processes that public institutions and enterprises providing critical infrastructure services must carry out in order to ensure the security of critical data. Public institutions and enterprises were expected to submit their audit results by 30 March 2025. However, there is currently no publicly available information whether any fines were issued by Digital Transformation Office as a result of non-compliance with audit requirements.

Contributors

Kağan Dora
Partner
kdora@baseak.com

Neslihan Kasap
Senior Associate
nkasap@baseak.com

Cansu Duman
Senior Associate
cduman@baseak.com

Emir Gönen
Senior Associate
egonen@baseak.com

Almira Akbay
Associate
aakbay@baseak.com

Anıl İçintek
Associate
aicintek@baseak.com