COUNTRY COMPARATIVE GUIDES 2024

The Legal 500 Country Comparative Guides

Turkey

DATA PROTECTION & CYBERSECURITY

Contributor

Balcıoğlu Selçuk Ardıyok Keki

Kağan Dora

Partner | kdora@baseak.com

Cansu Duman

Senior Associate | cduman@baseak.com

Irmak Ulusinan

Associate | iulusinan@baseak.com

Almira Akbay

Associate | aakbay@baseak.com

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

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

TURKEY
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 by them; 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. In a number of decisions, it has mentioned that it would follow the territorial scope applicable to the EU's General Data Protection Regulation ("**GDPR**"). 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, there is no general cybersecurity law which regulates all sectors. Yet, 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.

Please refer to Question 35 for further details.

2. Are there any expected changes in the data protection, privacy or cybersecurity landscape in 2024–2025 (e.g., new laws or regulations coming into effect, enforcement of such laws and regulations, expected regulations or amendments (together, "data protection laws"))?

There had been an ongoing initiative to amend the DPL with the aim of aligning it with the GDPR for some time and this amendment has been published in the Official Gazette dated March 12, 2024, and numbered 32487 ("**Amendment**"). The Amendment especially affects the current rules on cross-border transfers of personal data, processing of special categories of personal data and jurisdiction over the administrative the decisions of the DPA and is set to take effect on June 1, 2024.

According to the Amendment, a new regulation regarding the implementation of the rules on cross-border transfers will be published by the DPA as well.

However, no specific timeline is provided for when this new regulation will be published by the DPA.

There is also another amendment expected on the DPL which aims to fully harmonize the DPL with the GDPR.

Please refer to Question 48 for more information.

3. Are there any registration or licensing requirements for entities covered by these data protection laws, and if so what are the requirements? Are there any exemptions?

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.

4. How do these data protection laws define “personal data,” “personal information,” “personally identifiable information” or any equivalent term in such legislation (collectively, “personal data”) versus special category or sensitive personal data? What other key definitions are set forth in the data protection laws in your jurisdiction?

Personally identifiable information (PII) is not a term used in the DPL. 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 the personal data based on the authority granted by and on behalf of the data controller.

5. What are the principles related to the general processing of personal data in your jurisdiction? For example, must a covered entity establish a legal basis for processing personal data, or must personal data only be kept for a certain period? Please outline any such principles or "fair information practice principles" in detail.

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 8 for conditions of processing special categories of personal data.

6. Are there any circumstances for which consent is required or typically obtained in connection with the general processing of personal data?

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.

7. 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)?

Although there are no direct rules or regulations related to the content of the consent form, the DPA's guidelines set forth principles on this matter. Accordingly, the consent form must include the purpose of the data processing as well as the personal data to be processed. It is also recommended to provide information on the right to withdraw consent at any time. Additionally, the consent form must be written in plain and simple language and the text size of such form must not be too small. On the other hand, the DPL does not set out any requirement as to the form of the consent. Data controllers can obtain consent in any form (e.g., through a tick-box, verbally, in writing, etc.) so long as it allows them to demonstrate that consent is duly obtained.

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.

8. What special requirements, if any, are required for processing sensitive personal data? Are any categories of personal data prohibited from collection or disclosure?

Article 6 of the DPL sets out special conditions for processing special categories of personal data and these rules have been completely changed with the Amendment. Within this scope, a distinction must be made for the legal bases for processing special categories of personal data applicable until June 1, 2024, and after.

- **Until June 1, 2024:** This data, excluding health data and sexual life data, can only be processed if such processing is explicitly foreseen under applicable laws, or if the data subject's explicit consent is obtained.
- **As of June 1, 2024:** 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.

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.

Please see Question 9 for conditions of processing health and sexual life data.

9. How do the data protection laws in your jurisdiction address health data?

As Article 6 of the DPL which sets out special conditions for processing special categories of personal data has been amended a distinction must be made for the legal bases for processing health and sexual life data applicable until June 1, 2024, and after.

Until June 1, 2024: Processing conditions for health data and data related to sexual life are even more restricted. Under the DPL, this data can only be processed with the data subject's explicit consent, unless the following requirements are met:

Data is processed by those who are under the obligation of secrecy or authorized institutions and organizations; **and** data is processed for the purposes of **(i)** protection of public health, **(ii)** operation of preventive medicine, **(iii)** medical diagnosis, **(iv)** treatment, and care services, **(v)** planning and management of health services and **(vi)** financing of health services.

As of June 1, 2024: All special categories of personal data including health and sexual life may be processed based on one of the legal bases provided in Question 8.

10. Do the data protection laws in your jurisdiction include any derogations, 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

11. Do the data protection laws in your jurisdiction address children's and teenagers' personal data? If so, please describe how.

There are no specific rules which address children's and teenager's personal data directly. However, the implementation of the rules under the DPL are affected by general rules regarding the legal capacity of minors.

Accordingly, under the Turkish Civil Code ("**TCC**"), any person under the age of 18 is considered a minor. Although the DPL does not stipulate special provisions for processing children's data, personal data can be processed by relying on legal bases foreseen under the DPL. Obtaining the data subject's explicit consent is one of these legal bases. If such a legal basis is chosen when processing a minor's personal data, the validity of explicit consent will depend on whether the minor is of **(i)** absolute legal incapacity or **(ii)** limited legal incapacity as stipulated under the TCC.

In this respect, depending on whether the minor is able to understand the results of their explicit consent; from whom (i.e., the minor or their legal guardian) and in what way such consent should be obtained vary. In addition, the privacy notice should be presented to the parent or guardian as well as to the child. The privacy notice addressed to the child should contain a plain and simple language which makes it easier for the child to understand the consequences of relevant processing activities.

12. Do the data protection laws in your jurisdiction address online safety? Are there any additional legislative regimes that address online safety not captured above? If so, please describe.

The DPL and its secondary regulations do not directly address online safety aside from regulating obligations regarding personal data security in general, however, the Law on the Regulation of Broadcasts via Internet and Prevention of Crimes Committed through Such Broadcasts numbered 5651 ("**Internet Law**") regulates the obligations and responsibilities of content providers, hosting providers, access providers and collective use providers, the principles and procedures for combating certain offences committed on the internet through content, hosting and access providers as well as the obligations of social network providers.

The Internet Law imposes various obligations on content, hosting and access providers which may be considered related to online safety, such as, the obligation to retain traffic data regarding the services they provide for a specific period (for access providers and hosting providers) and the obligation to provide a minimum set of identifying information on their own platforms (for content, hosting and access providers).

The Internet Law also imposes various obligations

related to online safety on social network providers. According to paragraph 7 Additional Article 4 of the Internet Law, social network providers are obliged to take the necessary measures to provide differentiated services specific to children and according to paragraph 13 of the same article, social network providers are obliged to comply with the regulations regarding user rights to be published by the Information Technologies and Communication Authority ("**ITCA**").

These obligations are solidified within the Procedures and Principles Regarding Social Network Providers ("**SNP Guidelines**") published by ITCA on April 1, 2023.

As per Article 14 of the SNP Guidelines, social network providers who provide content, advertising and other services to users who can be identified as children must consider including but not limited to the matters below while providing these services:

- The age of the child,
- Consideration of the best interests of the child,
- Prevention of risks of child sexual abuse and commercial exploitation,
- Ensuring minimum data processing with high-level privacy settings to protect the child's personal data.

13. Is there any regulator in your jurisdiction with oversight of children's and teenagers' personal data, or online safety in general? If so, please describe, including any enforcement powers. If this regulator is not the data protection regulator, how do those two regulatory bodies work together?

There is no regulator who oversees compliance with rules regarding children's and teenagers' personal data *per se* however, ITCA is responsible for monitoring compliance with the rules provided under the Internet Law mentioned under Question 12 above.

As per the Internet Law, ITCA is authorized to impose administrative fines, per violation, for non-compliance with the rules specified under Question 12 above.

ITCA is a separate authority from the DPA, however as their powers and responsibilities focus on different areas of law, matters which would require them to work together are very limited.

14. Are there any expected changes to the online safety landscape in your jurisdiction in 2024–2025?

There is no publicly available information regarding any potential changes to the online safety landscape in Turkey on this date.

15. Does your jurisdiction impose 'data protection by design' or 'data protection by default' requirements or similar? If so, please describe the requirement(s) and how businesses typically meet such requirement(s).

The DPL does not provide a "data protection by design" or "data protection by default" per se. However, any data processing activity must be in compliance with the DPL, and therefore data controllers must assess the status of compliance of any potential data processing activity before conducting such activity.

16. Are controllers and/or processors of personal data required to maintain any internal 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, companies 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 17 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.

17. 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.

18. Under what circumstances is a controller operating in your jurisdiction required or recommended to consult with the applicable data protection regulator(s)?

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

19. Do the data protection laws in your jurisdiction require or recommend risk assessments in connection with data processing activities and, if so, under what circumstances? How are these risk 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, as indicated in detail under Question 32 below, the Amendment introduces new transfers mechanisms for cross-border transfers of personal data to be utilized by both data controllers and processors. That being said, by way of requiring information on whether data subjects have the means to exercise their rights and to have recourse to effective legal remedies in the recipient country in cases where cross-border persona data transfer is occurred based on appropriate safeguards, we opine that DPA after the effective date of the Amendment, will be recommending an assessment like Transfer Impact Assessment in the EU.

20. Do the data protection laws in your jurisdiction require a controller's appointment of a data protection officer, chief information security officer, or other person responsible for data protection, and 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 designation of a personnel who is in charge of the information security. In this respect, contrary to discretional approach in relation to 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.

21. 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).

There is no specific requirement under the DPL for providing employee training. However, in its Guideline on Technical and Administrative Measures, the DPA considers it 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.

22. 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.

23. Do the data protection laws in your jurisdiction draw any distinction between the controllers and the processors of personal data, and, if so, what are they?

Please see Question 4 for definitions of data controller and data processor under the DPL.

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.

24. Do the data protection laws in your jurisdiction place obligations on processors by operation of law? Do the data protection laws in your jurisdiction require minimum contract terms with processors of personal data?

The DPL neither requires minimum contract terms to be incorporated into the agreements to be executed with the data processor nor does it foresee any restriction on the appointment of data processors. As indicated in Question 23 above, data controllers are jointly responsible with the data processors for ensuring data security. Data controllers are required to audit the data processors to ensure compliance with the DPL.

Although the DPL does not set forth any minimum contract terms, under the Data Security Guideline, the DPA recommends having a written agreement in place between the data controller and the data processor to ensure data security. This agreement should stipulate that the data processor will **(i)** process the personal data upon the instructions of the data controller for the purposes specified under the agreement in accordance with the DPL, **(ii)** be subject to a duty of confidentiality for an indefinite term, **(iii)** comply with the data retention policy of the data controller and **(iv)** notify the data controller in the event of a data breach. The DPA also recommends that the categories and types of personal data transferred to the data processor should be specifically indicated to the extent the nature of the agreement permits.

25. Are there any other restrictions relating to the appointment of processors (e.g., due diligence, privacy and security assessments)?

There are no other restrictions explicitly relating to the appointment of processors.

26. 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 terms defined, and what restrictions on their use are imposed, if any?

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 Guidelines, which is heavily based on the EU's cookie guidelines. In the Cookie Guidelines, 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 Guidelines state 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.

27. Please describe any restrictions on targeted advertising and/or cross-contextual behavioral advertising. How are these terms or any similar terms defined?

There is no definition of cross-contextual behavioural

advertising under the DPL. However, the Cookie Guidelines 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.

28. Please describe any data protection laws in your jurisdiction addressing the sale of personal data. How is the term "sale" or such related terms defined, and what restrictions are imposed, if any?

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.

29. Please describe any data protection laws in your jurisdiction addressing telephone calls, text messaging, email communication, or direct marketing. How are these terms defined, and what restrictions are imposed, if any?

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.

30. Please describe any data protection laws in your jurisdiction addressing biometrics, such as facial recognition. How are such terms defined, and what restrictions are imposed, if any?

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 8 for the conditions for processing biometric data.

31. 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 2024 that necessary legal regulations will be made to meet the needs arising from AI technologies.

32. 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 which sets out rules and restrictions regarding cross-border transfers of personal data has been amended with the aim of harmonization with the rules envisaged under chapter 5 of the GDPR.

Therefore, a distinction must be made for the cross-border transfer mechanisms which may be utilized until June 1, 2024, and after.

- **Until June 1, 2024:** Personal data processed in Turkey can only be transferred by data controllers to another country if:
    - Explicit consent of the data subject is obtained; or
    - The data is processed on the basis of the one of the exceptions provided under Article 5 and 6 of the DPL, and either **(i)** the destination country is among the countries designated by the DPA as a country with an adequate level of protection, or **(ii)** a written undertaking is executed between the transferor and transferee to ensure adequate protection, and the prior approval of the DPA has been obtained.

For intragroup data transfers, the binding corporate rules mechanism may also be implemented instead of the above-stated undertaking mechanism.

- **As of June 1, 2024:** According to the transitional clause in the Amendment, until September 1, 2024, explicit consent as described under the regime as it was regulated before the Amendment, above may be continued to be utilized for cross-border transfers.

On the other hand, as of June 1, 2024, 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 will be possible 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 mentioned within the Amendment include, **(i)** executing binding corporate rules approved by the DPA, **(ii)** execution of standard contractual clauses to be published by the DPA and notifying the DPA within 5 business days of execution of these clauses, and **(iii)** existence of a written contract whose provisions are sufficient enough to ensure adequate level of protection and approval of such written contract by the DPA.

- **Transfers for specific situations:** In addition to the aforementioned, the Amendment permits the transfer of personal data abroad even in the absence of appropriate safeguards or adequacy decisions. Consequently, 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).

The Amendment further states that the DPA will publish a new regulation pertaining to the application of the cross-border transfer regulations.

33. What security obligations are imposed on data controllers and processors, if any, 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 8 for the relevant DPA decision.*

34. Do the data protection laws in your jurisdiction address security breaches and, if so, how do such laws define a "security breach"?

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). *Please refer to Question 36 for further information on notification requirements.*

Other than notification requirements regulated under the DPL, there are sector-specific regulations that govern the necessary steps to be taken in case of a security breach. In this regard, certain specific actors such as banks, social network providers and telecommunication companies, are under the obligation to notify relevant authorities in the event of security breaches.

35. Does your jurisdiction impose specific security requirements on certain sectors, industries or technologies (e.g., telecom, infrastructure, AI)?

Yes, cybersecurity requirements exist for certain specific sectors (such as banking and finance, health, electronic communications or energy sectors), rather than a generally applicable law. 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 July 2020, the Turkish Presidency's Digital Transformation Office issued an Information and Communication Security Guide ("**Guide**"), which is in line with the Circular. The Guide provides the details of the information security measures applicable to public institutions and private organizations that fall under the scope of the Circular.

Additionally, in late August 2021, Digital Transformation Office of the Presidency of Turkey published Turkey's National Artificial Intelligence Strategy ("**Strategy**"), which determines Turkey's strategy for artificial intelligence ("**AI**") implementation. Among other things, the Strategy sets forth a general security recommendation to be applied to AI implementation. AI systems should be constructed in a way so as to avoid undesirable damage and vulnerabilities to ensure the security of humans, the environment and the biological ecosystem. After publication of the Strategy, the DPA published its own guideline: "Recommendations on the Protection of Personal Data in the Field of Artificial Intelligence" (*Please see Question 31 for details*) which includes general recommendations on using personal data within the scope of AI systems. In this guideline, the DPA generally highlights that AI systems should be designed so as to ensure the security of personal data.

36. Under what circumstances must a business report security breaches to regulators, impacted individuals, law enforcement, or other persons or entities? If breach notification is not required by law, is it recommended by the applicable regulator in your jurisdiction, and what is customary in this regard in your jurisdiction?

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.

Please see below Question 37 for notification requirements in relation to cybersecurity incidents.

37. Does your jurisdiction have any specific legal requirements or guidance for dealing with cybercrime, such as in the context of ransom payments following a ransomware attack?

Ransomware attacks are not subject to a specific regulation under Turkish law. The National Cybersecurity Response Center ("**USOM**") published on its website a notification regarding the increase in the number of ransomware attacks and advised of certain measures to take in the event of such attacks, such as notifying USOM within 72 hours of an attack and providing evidence of the attack. Furthermore, specific ransomware attacks by certain bodies are publicly notified on websites of the Information and Communication Technologies Authority and USOM. These notifications include details of the attack, its impact and possible solutions for prevention.

Furthermore, the Turkish Criminal Code defines the following situations as crimes related to data processing systems; *unlawfully accessing or continuously staying in information systems, blocking or breaking the operation of information systems and altering or destroying data; misuse of bank or credit cards; using devices, software, passwords or other security codes to commit such crimes and producing, importing, delivering, transporting, storing, accepting, selling, supplying, purchasing or carrying such items*. Penalties for such crimes range from six months to seven years of imprisonment.

38. Does your jurisdiction have a separate cybersecurity regulator? If so, please provide details.

Although the authority in charge indicate variety for certain sectors, ITCA acts as a main authority for cybersecurity related matters in Turkey.

39. Do the data protection laws in your jurisdiction provide individual data privacy rights, 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, any exceptions and any other relevant details.

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 10 above for the exceptions.

40. Are individual data privacy rights exercisable through the judicial system, enforced by a regulator, or both?

Data subjects must first apply to the data controller in writing. If the data controller rejects the application, replies insufficiently or not at all, within 30 days of receipt of the request, the data subject is entitled to file a complaint before the DPA. Additionally, 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.

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

Please see our explanations in Question 40.

42. Are individuals entitled to monetary damages or compensation if they are affected by breaches of data protection law? Does the law require actual damage to have been sustained, or is 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.

43. How are data protection laws in your jurisdiction 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 for breaching the obligations set out under the DPL.

44. 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 47,303 to TRY 946,308
Violation of obligation to register with VERBİS	TRY 189,245 to TRY 9,463,213
Noncompliance with liabilities on data security	TRY 141,934 to TRY 9,463,213
Noncompliance with the DPA's decisions	TRY 236,557 to TRY 9,463,213
Failure to notify the DPA within 5 business days of the execution of the standard contractual clauses for cross-border transfers	TRY 50,000 to TRY 1,000,000

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

45. 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.

46. Can controllers operating in your jurisdiction appeal to the courts against orders of the regulators?

Yes, data controllers can appeal the DPA's decisions before the competent courts if they consider that a decision issued by the DPA is unlawful. Moreover, the Amendment changes the jurisdiction over administrative fines imposed by the DPA. Starting from June 1, 2024, the administrative courts will have jurisdiction over the disputes arising out of the administrative fines, not the criminal courts of peace.

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

Last year, the DPA published a Five-Year Report which summarizes its activities from the beginning of its establishment, which is in 2017. The Five-Year Report indicates that the DPA has issued in the total amount of TRY 74,116,828 administrative fine until the year 2023. However, there are no recent data on enforcement activity of the DPA for the years 2023 and 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.

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 March 1, 2024. Currently, there is no publicly available information whether any fines issued by Digital Transformation Office as a result of non-compliance with audit requirements.

48. Are there any proposals for reforming data protection laws in your jurisdiction currently under review? Please provide an overview of any proposed changes and the legislative status of such proposals.

As explained under Question 2 above, the Amendment which introduced changes mainly on Articles 6 (processing of special categories of personal data), Article 9 (cross-border transfer mechanisms) and Article 18 (misdemeanors and jurisdiction) will take effect as of June 1, 2024. Additionally, until September 1, 2024, explicit consent as described under the regime as it was regulated before the Amendment, above may be continued to be utilized for cross-border transfers.

On the other hand, another amendment which will affect all provisions of the DPL is expected for full harmonization with the GDPR. According to the Presidential Annual Program for 2024, 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 2024.

Contributors

Kağan Dora
Partner
kdora@baseak.com

Cansu Duman
Senior Associate
cduman@baseak.com

Irmak Ulusinan
Associate
iulusinan@baseak.com

Almira Akbay
Associate
aakbay@baseak.com