COUNTRY COMPARATIVE GUIDES 2023

# The Legal 500 Country Comparative Guides

## Turkey

# DATA PROTECTION & CYBERSECURITY


**Contributor**

Balcıoğlu Selçuk Ardıyok Keki

**Kağan Dora**

Partner | kdora@baseak.com

**Neslihan Kasap**

Senior Associate | ngurser@baseak.com

**Hazal Durak**

Senior Associate | hdurak@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 legislations of the DPL include the following:

- Regulation on the Data Controllers' Registry ("**VERBIS**")
- 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 (collectively 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 30 for further details.*

## 2. Are there any expected changes in the data protection, privacy and cybersecurity landscape in 2023-2024 (e.g., new laws or regulations coming into effect, enforcement of any new laws or regulations, expected regulations or amendments)?

There is an ongoing initiative to amend the DPL with the aim of aligning it with the GDPR. However, neither the timing nor the context of this has been announced. *Please refer to Question 43 for more information.* On the other hand, various plans and strategies are expected to be implemented within the period covered by the Strategy Plan for 2019-2023, including the establishment of new public organisations and committees dealing with cybersecurity. On the other hand, the Turkish Presidency's Digital Transformation Office , which was established in 2018, has been carrying out a series of studies and projects in the area of cybersecurity and data security for the purpose of ensuring digitalization in

 

public services and increasing public awareness thereof.

### 3. Are there any registration or licensing requirements for entities covered by these 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 Data Controller Registry Information System ("**VERBIS**") 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 25 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 laws define personal data or personally identifiable information (PII) versus special category or sensitive PII? What other key definitions are set forth in the 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 process 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 or PII. For example, must a covered entity establish a legal basis for processing personal data or PII in your jurisdiction, or must personal data or PII 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 are being collected.

In addition, Articles 5 and 6 of the DPL regulates 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 where consent is required or typically used in connection with the general processing of personal data or PII?

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 is 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 PII? Are there any categories of personal data or PII

 

## that are prohibited from collection or disclosure?

Article 6 of the DPL sets out special conditions for processing special categories of personal data. 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.

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 10 for conditions of processing health and sexual life data.*

## 9. How do the laws in your jurisdiction address children's personal data?

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 data subject's explicit consent is one of these legal bases. If such 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 an explicit consent; from whom and in what way such consent should be obtained will be subject to variation. In addition, the information notice should be presented to the parent or guardian as well as to the child. The information 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.

## 10. How do the laws in your jurisdiction address health data?

Processing conditions for health data and data related to the 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.

## 11. Do the laws include any derogations, exclusions or limitations other than those already described? 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 VERBIS* | 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 |

## 12. Does your jurisdiction impose requirements of 'data protection by design' or 'data protection by default' or similar? If so, please describe the requirement and how businesses typically meet the requirement.

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.

## 13. Are owners/controllers or processors of personal data or PII required to maintain any internal records of their data processing activities or to establish internal processes or written documentation? If so, please describe how businesses typically meet these

 

**requirements.**

Yes, data controllers that are required to register with VERBIS 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 the personal data.

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

In addition, data controllers that are required to register with VERBIS must prepare a data retention policy. 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.

## 14. Do the laws in your jurisdiction require or recommend having defined data retention and data disposal policies and procedures? If so, please describe these data retention and disposal requirements.

As per the Regulation on Deletion, Destruction or Anonymization Personal Data ("**Deletion Regulation**"), data controllers that are required to register with VERBIS 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 in 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.

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.

## 15. When are you required to, or when is it recommended that you, consult with data privacy regulators in your jurisdiction?

 

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

### 16. Do the laws in your jurisdiction require or recommend conducting risk assessments regarding data processing activities and, if so, in 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 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.

### 17. Do the laws in your jurisdiction require appointment of a data protection officer or a chief information security officer (or other person to be in charge of privacy or data protection at the organization), and what are their legal responsibilities?

The DPL does not require 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, a 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.

### 18. Do the laws in your jurisdiction require or recommend employee training? If so, please describe these training requirements.

There is no specific requirement under the DPL for providing employee trainings. 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 the personal data security. Additionally, in data breach investigations, the DPA generally requests evidence from data controllers demonstrating that employee trainings have been duly provided. Therefore, it is recommended to have regular employee trainings in place.

### 19. Do the laws in your jurisdiction require businesses to provide notice to data subjects of their processing activities? If so, please describe these notice requirements (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.

### 20. Do the laws in your jurisdiction draw any distinction between the owners/controllers and the processors of personal data, and, if so, what are they? (For example, are obligations placed on processors by operation of law, or do they typically only apply through flow-down contractual requirements from the owners/controller?)

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.

### 21. Do the laws in your jurisdiction require minimum contract terms with processors of personal data or PII, or are there any other restrictions relating to the appointment of processors (e.g., due diligence or privacy and security assessments)?

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 20 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.

### 22. Please describe any restrictions on monitoring, automated decision-making or profiling in your jurisdiction, including the use of tracking technologies such as cookies. How are these terms defined, and what restrictions 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. 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.

### 23. Please describe any restrictions on targeted advertising and cross-contextual behavioral advertising. How are these terms or related 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.

 

### 24. Please describe any laws in your jurisdiction addressing the sale of personal data. How is "sale" or 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.

### 25. Please describe any 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. Since direct marketing communications involve personal data processing activities, such activity must be carried in accordance with applicable legal bases.

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.

### 26. Please describe any laws in your jurisdiction addressing biometrics such as facial recognition. How are these 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, 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.*

### 27. Is the transfer of personal data or PII outside the 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? Does a cross-border transfer of personal data or PII require notification to or authorization from a regulator?)

Personal data processed in Turkey can only be transferred 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.

Since the enactment of the DPL, the DPA approved Teb Arval's, Amazon Turkey's, Decathlon Turkey's,the Turkish Football Federation's and Otokoç Otomotiv's undertaking letters on cross-border data transfers.

As of April 2023, the DPA has not yet issued the list of countries with an adequate level of protection. As a

 

result, at this stage all countries are deemed as not providing an adequate level of protection.

On the other hand, in March 2021 the Turkish president announced the "Human Rights Action Plan." One of the overarching aims of this action plan includes harmonization of the DPL with EU standards to ensure the protection of private life in the processing of personal data. It was also announced in the new economic plan that the DPL's provisions on cross-border data transfers will be amended in accordance with the GDPR. Therefore, further amendments are foreseen in relation to the principles governing cross-border data transfers.

## 28. What security obligations are imposed on personal data or PII owners/controllers and on processors, if any, in your jurisdiction?

Data controllers 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, 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.*

## 29. Do the data protection, privacy and cybersecurity laws in your jurisdiction address security breaches, and, if so, how does the law define "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 31 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.

## 30. Does your jurisdiction impose specific security requirements on certain sectors, industries or technologies (e.g., telecoms, infrastructure, artificial intelligence)?

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" 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.

### 31. Under what circumstances must a business report security breaches to regulators, to individuals or to other persons or entities? If breach notification is not required by law, is it recommended by the regulator, and what is the typical custom or practice 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 32 for notification requirements in relation to cybersecurity incidents.*

### 32. Does your jurisdiction have any specific legal requirement or guidance regarding dealing with cybercrime, such as the payment of ransoms in ransomware attacks?

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.

### 33. Does your jurisdiction have a separate cybersecurity regulator? If so, please

 

**provide details.**

Although the authority in charge indicate variety for certain sectors, Information and Communication Technologies Authority acts as a main authority for cybersecurity related matters in Turkey.*Please refer to Question 1 and 30 for detailed information.*

## 34. Do the 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 the rights, how they are exercised, what exceptions exist 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 Question 11 above for the exceptions.*

## 35. Are individual data privacy rights exercisable through the judicial system or 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.

## 36. Does the law in your jurisdiction provide for a private right of action and, if so, in what circumstances?

*Please see our explanations in Question 35.*

## 37. Are individuals entitled to monetary damages or compensation if they are affected by breaches of data protection, privacy and/or cybersecurity laws? Is actual damage required, or is injury of feelings sufficient?

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.

## 38. How are data protection, privacy and cybersecurity laws 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.

As mentioned above under Questions 1 and 30, there is no singular authority to enforce cybersecurity laws. Based on the regulations relating to specific sectors, each authority (in the relevant sector) is competent to

 

enforce applicable rules. For instance, while Information and Communication Technologies Authority is entitled to impose administrative fines on electronic communication service providers for matters related to the application of Electronic Communication Law No. 5809 and violations of cybersecurity, Banking Regulation and Supervision Agency and the Central Bank of the Republic of Turkey carry out the functions of enforcement for banking and finance industry and for payment and electronic money, relatively.

## 39. What is the range of sanctions (including fines and penalties) for violation of data protection, privacy and cybersecurity laws?

| **Administrative Fines Under the DPL** | |
|---|---|
| **Misdemeanor** | **Fine** |
| Violation of obligation to inform | TRY 29,852 to TRY 597,191 |
| Violation of obligation to register with VERBIS | TRY 119,428 to TRY 5,971,989 |
| Noncompliance with liabilities on data security | TRY 89,571 to TRY 5,971,989 |
| Noncompliance with the DPA's decisions | TRY 149,282 to 5,971,989 |

*The above-listed administrative fine amounts are applicable for 2023 and are subject to annual revaluation.*

| **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 |

## 40. Are there any guidelines or rules published regarding the calculation of 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.

## 41. Can personal data or PII owners/controllers appeal to the courts against orders of the regulators?

Yes, data controllers and data subjects can appeal the DPA's decisions before the competent courts if they consider that a decision issued by the DPA is unlawful.

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

Recently, the DPA published a report which summarizes its activities in the past five years ("**Five-Year Report**"), 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, up to date. 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 VERBIS before carrying out data processing activities.

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. The Audit Guide indicates that institutions and organizations should complete their audit no later than December 31, 2022. However, the Digital Transformation Office has not issued any fines regarding non-compliance with audit requirements.

## 43. Are there any proposals for reforming data protection, privacy and/or cybersecurity laws currently under review?

 

**Please provide an overview of any proposed changes and how far such proposals are through the legislative process.**

There is an ongoing initiative to amend the DPL with the aim of aligning with the GDPR. It is expected that these amendments may help businesses overcome several hurdles, such as cross-border transfers of personal data and the processing of special categories of personal data within the scope of the DPL. However, neither the timing nor the context of such amendments has been defined yet.

Furthermore, there are not any known expected changes in cybersecurity landscape in 2023-2024. *Please refer to Question 2 for more information.*

## Contributors

**Kağan Dora**
**Partner**
kdora@baseak.com

**Neslihan Kasap**
**Senior Associate**
ngurser@baseak.com

**Hazal Durak**
**Senior Associate**
hdurak@baseak.com

**Almira Akbay**
**Associate**
aakbay@baseak.com