Turkey


Tuna Çakırca


İpek Batum

Çiğdemtekin Çakırca Arancı Law Firm

1 Relevant Legislation and Competent Authorities

1.1 What is the principal data protection legislation?

The principal data protection legislation is **Personal Data Protection Law** no. 6698 ("**PDPL**"). The secondary legislation of the PDPL consists of:

- **Regulation on the Deletion, Destruction or Anonymization of Personal Data**, which entered into force on 1 January 2018;
- **Regulation on the Data Controllers Registry**, which entered into force on 1 January 2018 ("**Registry Regulation**");
- **Communique on the Procedures and Principles of Application to Data Controller**, published by the Personal Data Protection Authority ("**Authority**"), which entered into force on 10 March 2018; and
- **Communique on Principles and Procedures for Fulfilment of Informing Obligation**, published by the Authority, which entered into force on 10 March 2018.

Additionally, guidelines and Q&As published by the Authority and decisions of the Personal Data Protection Board ("**Board**") play a significant role in the interpretation and implementation of the PDPL and secondary legislation. The Board has the authority to regulate certain aspects of the PDPL and secondary legislation and to decide on specific data breaches.

1.2 Is there any other general legislation that impacts data protection?

Article 20 of the Turkish Constitution sets out that every person has the right to request protection of his/her personal data, which she/he should be informed of, have access to and able to request the correction and deletion of such personal data. The Constitution also envisages that personal data can only be processed with explicit consent or when regulated by law.

Turkish Criminal Code no. 5237 stipulates imprisonment of persons who unlawfully deliver data to another person, or publish or acquire the same through illegal means, and those who fail to destroy personal data despite their duty to do so, prosecution of which is initiated upon a complaint.

Pursuant to Turkish Civil Code no. 4271, it is possible to claim material and moral damages due to the violation of protection of civil rights, which includes breach of the right to privacy.

Since the PDPL was prepared in parallel to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data no. 108 and EU Directive no. 95/46/EC, such legislation is also an important guide for the purpose of the interpretation of the PDPL and the secondary legislation.

1.3 Is there any sector-specific legislation that impacts data protection?

There are several sector-specific laws and regulations that impact data protection, including:

- Law on the Regulation of Electronic Commerce no. 6563;
- Banking Law no. 5411;
- Law on Bank Cards and Credit Cards no. 5464;
- Law on Turkish Civil Aviation no. 2920;
- Law on Electronic Communications no. 5809;
- Law on Internet Broadcasting and Crimes Committed through Internet Broadcasting no. 5651;
- Electronic Signature Law no. 5070;
- Law on Postal Services no. 6475;
- Law on Payment and Security Reconciliation Systems Payment Services and Electronic Money Organisations no. 6493;
- Regulation on Distance Contracts published in the Official Gazette, dated 17 November 2014, no. 29188;
- Regulation on Patient Rights published in the Official Gazette, dated 1 August 1998, no. 23420;
- Regulation on Protection and Privacy of Personal Health Data published in the Official Gazette, dated 20 October 2016, no. 29863;
- Regulation on Electronic Communication and Commercial Electronic Messages published in the Official Gazette, dated 15 July 2015, no. 29417;
- Regulation on International Health Tourism and Health of Tourists published in the Official Gazette, dated 13 July 2017, no. 30123; and
- Regulation on the Safety of Passenger Ships and the Registration of Passengers on Ships published in the Official Gazette, dated 12 December 2007, no. 26728.

1.4 What authority(ies) are responsible for data protection?

The Authority is primarily responsible for the regulation of data protection activities and supervision of compliance therewith. The

Regulation on the Organization of the Personal Data Protection Authority regulates the duties, power and responsibilities of the Authority.

The Board is the decision-making body of the Authority, and the duties, powers and responsibilities of the Board are regulated under the Regulation on Working Procedures and Principles of the Personal Data Protection Board.

2 Definitions

2.1 Please provide the key definitions used in the relevant legislation:

- "**Personal Data**"

  Personal data includes any and all kinds of information relating to an identified or identifiable natural person.
- "**Processing**"

  Processing includes all acts performed on the personal data, including, but not limited to, collection, recording, storage, preservation, alteration, adaptation, disclosure, transfer, retrieval, making available for collection, categorisation, blocking, whether fully or partially through automatic or non-automatic means which form part of a filing system.
- "**Controller**"

  A data controller is the natural or legal person who determines the objectives and means of processing personal data and is responsible for the establishment and the management of a data recording system. Board decision dated 13 September 2018, no. 2018/106, sets out that an unidentified person cannot be a data controller.
- "**Processor**"

  A data processor is the natural or legal person who processes the personal data with the authority granted by the data controller and in the name of the data controller.
- "**Data Subject**"

  A data subject is the natural person whose personal data are processed.
- "**Sensitive Personal Data**"

  Sensitive Personal Data, i.e. *Special Category of Personal Data* under the PDPL, is exhaustively listed as data relating to race, ethnic origin, political opinions, philosophical beliefs, religion, sect or other beliefs, appearance and dress, membership of association, foundation or trade-union, health, sexual life, criminal conviction and security measures, and biometrics and genetics.
- "**Data Breach**"

  A data breach is processing of any kind of data in breach of the PDPL and secondary legislation.

Other key definitions – please specify (e.g., "Pseudonymous Data", "Direct Personal Data", "Indirect Personal Data").

- "**Explicit Consent**"

  Explicit consent must be informed, related to a specific issue and based on free will.
- "**Anonymisation**"

  Anonymisation is rendering personal data anonymous so that the data does not relate to an identified or identifiable natural person even through crosschecking with other data.
- "**Data Record System**"

  Data record system is defined as any recording system through which personal data are processed subject to specific criteria.
- "**Data Controllers Registry Information System**"

  The Data Controllers Registry Information System ("**VERBIS**") is the online registry kept by the Authority on which certain data controllers must register.

3 Territorial Scope

3.1 Do the data protection laws apply to businesses established in other jurisdictions? If so, in what circumstances would a business established in another jurisdiction be subject to those laws?

The PDPL does not restrict its applicability to persons/businesses resident in Turkey/subject to Turkish law; therefore, any natural or legal persons who process data are subject to the PDPL and its secondary legislation regardless of the law under which it is established. In addition, as per the Registry Regulation, data controllers who are not resident in Turkey are also obliged to register with VERBIS through their representatives who are resident in Turkey before starting data processing.

4 Key Principles

4.1 What are the key principles that apply to the processing of personal data?

- **Transparency**

  The data processing mechanism must be clear, accessible, understandable and concrete.
- **Lawful basis for processing**

  Data must be processed lawfully and in conformity with the rules of good faith.
- **Purpose limitation**

  Data obtained and processed must only be used for specific, explicit and legitimate purposes.
- **Data minimisation**

  Processed data must be relevant and limited to what is necessary in relation to the processing purposes.
- **Proportionality**

  Data must be processed proportionally to the processing purposes.
- **Retention**

  Data must be retained only for the period that is necessary for the processing purposes or as set out in the applicable legislation.

Other key principles – please specify

- **Accuracy and Being Up to Date**

  Processed data must be accurate, and up to date if necessary.

5 Individual Rights

5.1 What are the key rights that individuals have in relation to the processing of their personal data?

- **Right of access to data/copies of data**

  Each person has the right to learn whether his/her personal data are processed, to request information, to learn the purpose of his/her data processing and whether data are used in accordance with their purposes and to know the third

parties in Turkey or abroad to whom personal data have been transferred.

- **Right to rectification of errors**

  Each person has the right to request rectification in case personal data are processed incompletely or inaccurately and to request notification of these operations to third parties to whom personal data have been transferred.

- **Right to deletion/right to be forgotten**

  Each person has the right to request deletion, destruction or anonymisation of his/her personal data and to request notification of these operations to third parties to whom personal data have been transferred.

- **Right to object to processing**

  Each person has the right to object to processing of her/his personal data which is processed exclusively through automated systems and leads to an unfavourable consequence for the data subject.

- **Right to restrict processing**

  The right to restrict processing is not specifically mentioned under the PDPL. However, each person has the right to restrict processing as the PDPL does not permit the retention of data other than via the explicit consent of the data subject and grants the right to object against the whole processing system.

- **Right to data portability**

  The right to data portability is not regulated under the PDPL.

- **Right to withdraw consent**

  Every person has the right to withdraw his/her explicit consent to be applicable proactively.

- **Right to object to marketing**

  Please refer to question 9.4.

- **Right to complain to the relevant data protection authority(ies)**

  In case the data controller rejects the data subject's application, replies insufficiently or does not reply within 30 days, the data subject may file a complaint with the Board within 30 days from the date on which he is notified of the reply and, in any event, within 60 days following the date of application.

Other key rights – please specify

- **Right to Compensation**

  Each person has the right to request compensation for the damages arising from unlawful processing of personal data.

6 Registration Formalities and Prior Approval

6.1 Is there a legal obligation on businesses to register with or notify the data protection authority (or any other governmental body) in respect of its processing activities?

Prior to processing personal data, natural or legal persons are obliged to register with VERBIS as per the Registry Regulation. The Board has the authority to set forth exemptions to such obligation. Under such authority, the Board has determined in its various decisions that notaries, lawyers, political parties, trade unions, financial consultants, and data controllers whose annual average employee number is less than 50 and annual total balance sheet is less than TL 25,000,000 are exempt from registration requirements.

6.2 If such registration/notification is needed, must it be specific (e.g., listing all processing activities, categories of data, etc.) or can it be general (e.g., providing a broad description of the relevant processing activities)?

The registry application must be specific and include data as explained under question 6.5.

6.3 On what basis are registrations/notifications made (e.g., per legal entity, per processing purpose, per data category, per system or database)?

Registration should be made by each data controller, *i.e.* a natural or legal person who processes any kind of personal data.

6.4 Who must register with/notify the data protection authority (e.g., local legal entities, foreign legal entities subject to the relevant data protection legislation, representative or branch offices of foreign legal entities subject to the relevant data protection legislation)?

Every natural and legal person, including foreign real persons and legal entities who process personal data, are obliged to register with VERBIS. Foreign entities are obliged to register through their representatives who are resident in Turkey.

6.5 What information must be included in the registration/notification (e.g., details of the notifying entity, affected categories of individuals, affected categories of personal data, processing purposes)?

A data controller is initially obliged to appoint a contact person who is responsible for responses to the requests raised by data subjects and for communication with the Authority. Upon approval of such person by the Authority, the following information must be submitted to VERBIS:

- Processing purposes.
- Group(s) of data subjects and explanations regarding data categories of such data subjects.
- Recipients to whom the personal data may be transferred.
- Personal data envisaged to be transferred abroad.
- Measures taken to safeguard the personal data.
- Maximum period of time necessitated for the processing purposes or applicable legislation.

6.6 What are the sanctions for failure to register/notify where required?

Data controllers who fail to meet the VERBIS registration obligation shall be required to pay an administrative fine ranging from TL 20,000 to TL 1,000,000.

6.7 What is the fee per registration/notification (if applicable)?

Registration is free of charge.

6.8 How frequently must registrations/notifications be renewed (if applicable)?

Any changes in the registered information should be registered with VERBIS within seven days.

6.9 Is any prior approval required from the data protection regulator?

While data uploaded to VERBIS is not subject to approval, the contact person responsible for communication is approved by the Authority.

6.10 Can the registration/notification be completed online?

VERBIS registration process is completed online.

6.11 Is there a publicly available list of completed registrations/notifications?

Yes, there is a publicly available list of completed registrations. The publicly available information in VERBIS is categorised in the form of main headings such as the identity and address of the data controller, purpose of processing, security measures and retention periods.

6.12 How long does a typical registration/notification process take?

- Contact person registration to VERBIS can be completed within two to five days.
- The data registration process depends on the scope of personal data, but a typical data registration process can be completed within one working week.

7 Appointment of a Data Protection Officer

7.1 Is the appointment of a Data Protection Officer mandatory or optional? If the appointment of a Data Protection Officer is only mandatory in some circumstances, please identify those circumstances.

Unlike the General Data Protection Regulation (EU) 2016/679 ("**GDPR**"), the appointment of a Data Protection Officer is not regulated in the PDPL. Therefore, appointing a Data Protection Officer is optional.

7.2 What are the sanctions for failing to appoint a Data Protection Officer where required?

This is not applicable in Turkey.

7.3 Is the Data Protection Officer protected from disciplinary measures, or other employment consequences, in respect of his or her role as a Data Protection Officer?

This is not applicable in Turkey.

7.4 Can a business appoint a single Data Protection Officer to cover multiple entities?

This is not applicable in Turkey.

7.5 Please describe any specific qualifications for the Data Protection Officer required by law.

This is not applicable in Turkey.

7.6 What are the responsibilities of the Data Protection Officer as required by law or best practice?

This is not applicable in Turkey.

7.7 Must the appointment of a Data Protection Officer be registered/notified to the relevant data protection authority(ies)?

This is not applicable in Turkey.

7.8 Must the Data Protection Officer be named in a public-facing privacy notice or equivalent document?

This is not applicable in Turkey.

8 Appointment of Processors

8.1 If a business appoints a processor to process personal data on its behalf, must the business enter into any form of agreement with that processor?

There are no legal requirements to enter into any form of agreements with a data processor. However, such an agreement is highly recommended.

8.2 If it is necessary to enter into an agreement, what are the formalities of that agreement (e.g., in writing, signed, etc.) and what issues must it address (e.g., only processing personal data in accordance with relevant instructions, keeping personal data secure, etc.)?

Data controllers have a duty of care in choosing, instructing and supervising data processors. Therefore, it is recommended to enter into a written agreement with data processors and to include in such agreement provisions on the security measures to be taken, retention periods and recourse rights.

9 Marketing

9.1 Please describe any legislative restrictions on the sending of electronic direct marketing (e.g., for marketing by email or SMS, is there a requirement to obtain prior opt-in consent of the recipient?).

Pursuant to the Law on the Regulation of Electronic Commerce no. 6563 ("**LREC**"), electronic marketing messages by email or SMS can be sent on condition that opt-in consent of the recipient is obtained prior to communication, which may be obtained in writing

or by any means of communication. The scope of all electronic marketing messages must be in line with the consent provided by the recipient.

The LREC sets out an exemption for craftsmen and merchants, to whom electronic marketing messages can be communicated until the subject opts out of receiving the messages.

In any case, all electronic marketing messages must include means for the recipient to exercise their opt-out right along with the information listed in the legislation.

9.2 Please describe any legislative restrictions on the sending of marketing via other means (e.g., for marketing by telephone, a national opt-out register must be checked in advance; for marketing by post, there are no consent or opt-out requirements, etc.).

The LREC defines electronic marketing as all messages in electronic format and lists marketing by telephone, call centres, facsimile, automatic dialling equipment and smart voice recorder systems in a non-exhaustive manner. Therefore, the restrictions explained above will also apply to the marketing messages via these means.

On the other hand, marketing via physical means such as sending post does not fall under the LREC and is subject to general rules of the PDPL.

9.3 Do the restrictions noted above apply to marketing sent from other jurisdictions?

The service provider, *i.e.* the sender of the electronic marketing message, is defined in the LREC as natural or legal persons engaging in electronic commercial activities regardless of whether they are subject to foreign law or Turkish law. Therefore, the restrictions explained above should be applied to electronic marketing messages sent from other jurisdictions as well.

9.4 Is/are the relevant data protection authority(ies) active in enforcement of breaches of marketing restrictions?

In its decision no. 2018/119, dated 16 October 2018, the Board announced that data controllers, or data processors on behalf of data controllers, must cease electronic marketing communication if opt-in consent of the recipient is not obtained. The Board also repeated the duty of the data controller to take all necessary technical and organisational measures in order to prevent unlawful access to personal data and security thereof. In the event of non-compliance with these obligations, an administrative fine shall be imposed pursuant to Article 20 of the PDPL and that a criminal complaint shall be made against the data controller pursuant to the Turkish Criminal Code.

9.5 Is it lawful to purchase marketing lists from third parties? If so, are there any best practice recommendations on using such lists?

While there are no specific restrictions in relation to the purchase of marketing lists from third parties, transfers of personal data through the purchase of marketing lists is subject to the PDPL and the explicit consent of the data subject should be obtained for the transfer. In case the personal data is transferred abroad, the foreign country to which personal data will be transferred must also have an adequate level of protection. The transfer of personal data abroad is explained in detail under section 11.

9.6 What are the maximum penalties for sending marketing communications in breach of applicable restrictions?

As per the LREC, businesses may be exposed to administrative fines ranging between TL 1,550 and TL 31,051 (for 2019) in case of breach of the restrictions explained above. In case the marketing communications are sent to multiple recipients at once, the fines may be implemented by increasing the amount up to 10 times. Additionally, if applicable to the specific case, sanctions under the PDPL may also apply.

10 Cookies

10.1 Please describe any legislative restrictions on the use of cookies (or similar technologies).

There are no specific legislative restrictions on the use of cookies; therefore, it is at the discretion of the data controller to publish a cookie policy. However, in case the data collected via cookies or similar technologies relate to an identifiable person, then the general principles of the PDPL shall apply. Also, EU Directive 2002/58/EC, which sheds light as to how the Authority may interpret the legal status of cookies or similar technologies, requires users' informed consent before storing cookies on a user's device and/or tracking them. In light of the above, it is advised for data controllers to publish cookie policies on their websites.

10.2 Do the applicable restrictions (if any) distinguish between different types of cookies? If so, what are the relevant factors?

No, there is no distinction made between different types of cookies.

10.3 To date, has/have the relevant data protection authority(ies) taken any enforcement action in relation to cookies?

No, there has been no enforcement action in relation to cookies to date.

10.4 What are the maximum penalties for breaches of applicable cookie restrictions?

There is no maximum penalty for breaches of applicable cookie restrictions.

11 Restrictions on International Data Transfers

11.1 Please describe any restrictions on the transfer of personal data to other jurisdictions.

Under the PDPL, personal data may only be transferred abroad with explicit consent of the data subject.

The exception to such rule is that the foreign country to which personal data will be transferred shall have an adequate level of protection, and if an adequate level of protection is not available in such country, data controllers in Turkey and abroad may only transfer

data abroad with permission of the Board and a commitment provided to the Board undertaking security of the personal data. Pursuant to the PDPL, countries with an adequate level of protection are yet to be announced by the Board.

11.2 Please describe the mechanisms businesses typically utilise to transfer personal data abroad in compliance with applicable transfer restrictions (e.g., consent of the data subject, performance of a contract with the data subject, approved contractual clauses, compliance with legal obligations, etc.).

Data controllers mostly prefer obtaining explicit consent from data subjects and entering into data protection agreements with data processors setting out undertakings relating to protection of personal data, retention periods and audit rights, in certain cases. Additionally, data processors choose to obtain assurances from data controllers that explicit consent of data subject has been obtained and that there are recourse rights available relating thereto.

11.3 Do transfers of personal data to other jurisdictions require registration/notification or prior approval from the relevant data protection authority(ies)? Please describe which types of transfers require approval or notification, what those steps involve, and how long they typically take.

For the purpose of the permission to be obtained from the Board as explained under question 11.1, the Board has published two forms of letters of undertaking: (i) to be executed when data is transferred from one data controller to another; and (ii) to be executed when data is transferred from a data controller to a data processor, each to be signed by both the transferor and transferee.

12 Whistle-blower Hotlines

12.1 What is the permitted scope of corporate whistle-blower hotlines (e.g., restrictions on the types of issues that may be reported, the persons who may submit a report, the persons whom a report may concern, etc.)?

Pursuant to the guidelines issued by the Authority, businesses should define each employee's role in compliance with data protection legislation and train their employees regarding different aspects of the same.

Therefore, while there are no regulations on corporate whistle-blower hotlines, businesses may establish whistle-blowing mechanisms.

Additionally, public companies are obliged to establish committees for risk detection and internal audit, and detection of incompliance with data protection legislation is advised to be included within the scope of such committees' duties.

12.2 Is anonymous reporting prohibited, strongly discouraged, or generally permitted? If it is prohibited or discouraged, how do businesses typically address this issue?

Anonymous reporting is not prohibited or discouraged in the PDPL.

13 CCTV

13.1 Does the use of CCTV require separate registration/notification or prior approval from the relevant data protection authority(ies), and/or any specific form of public notice (e.g., a high-visibility sign)?

There are no specific regulations on the usage of CCTV from a data protection perspective; therefore, the general principles of the PDPL shall apply to CCTV. The PDPL does not require the explicit consent of the data subject if (i) other laws explicitly permit data processing, (ii) processing is necessary in order to protect the life or physical integrity of the data subject or another person where the data subject is physically or legally incapable of giving consent, (iii) execution or performance of an agreement between the data controller and data subject requires data processing, (iv) processing is required for the data controller to comply with its legal obligations, (v) the data subject already made such data available to the public, (vi) processing is necessary for the institution, usage, or protection of a right, and (vii) processing is required for protecting legitimate interests of data controller as long as such processing does not breach the fundamental rights and freedoms of the data subject. In the absence of these circumstances, the data controller must obtain the explicit consent of the data subject. Where one or more of such circumstances exist, the data controller is under the obligation to inform the data subject of the identity of the data controller, processed data, the purpose of processing, transferees, means of collection of data and which of the circumstances listed above exists.

In light of the above, data controllers may use CCTV for the purpose of protecting their legitimate interests, such as the security of certain areas. In order to fulfil their obligation to inform, data controllers which use CCTV are advised to place visible signs displaying the information stated above.

13.2 Are there limits on the purposes for which CCTV data may be used?

In addition to the consent/obligation to inform the obligation above, CCTV can only be used in case such usage is proportionate, limited to processing purposes and minimised for its present purpose, among other general principles.

14 Employee Monitoring

14.1 What types of employee monitoring are permitted (if any), and in what circumstances?

Employers collect their employees' personal data for several reasons, such as regulatory reasons, security reasons and performance review. General rules of data protection shall be applicable to employee monitoring; i.e. explicit consent of the employee is required in the absence of the circumstances listed under question 13.1. It must be noted that all processing must comply with the general principles, such as proportionality, limitation to purpose, minimisation and protection of legitimate interests of the data controller. If data processing is not compliant with these principles, the explicit consent provided by the employee will not be valid.

E-mail monitoring is an example of a permitted extent of employee monitoring. According to the general principles of the PDPL and a ruling of Turkish Constitutional Court, which was issued to prior to promulgation of the PDPL, employers can monitor corporate e-mail accounts with the condition that they inform the employees; however, monitoring of private e-mail accounts of employees is unlikely to be justified as being in the employer's legitimate interests.

14.2 Is consent or notice required? Describe how employers typically obtain consent or provide notice.

While employers must obtain explicit consent from employees in the absence of the circumstances stipulated under question 13.1, notice to employees as to how their personal data is processed is sufficient in case such circumstances exist.

For the purpose of the above, employers include data protection clauses in their employment agreements, whereby employees provide their explicit consent. Relating to the personal data which is processed on the basis of the circumstances stated under question 13.1, employers perform their obligation to inform through notices provided to and acknowledged by employees either electronically or manually. Employers also choose to place visible notifications in relation to any CCTV.

14.3 To what extent do works councils/trade unions/employee representatives need to be notified or consulted?

There is no specific legislation regulating this area.

15 Data Security and Data Breach

15.1 Is there a general obligation to ensure the security of personal data? If so, which entities are responsible for ensuring that data are kept secure (e.g., controllers, processors, etc.)?

Yes, the PDPL states that it is the data controllers' obligation to prevent unlawful processing of personal data and to prevent unlawful access to personal data by taking all necessary technical and organisational measures to provide an appropriate level of security. In January 2018, the Authority issued a guideline describing such technical and organisational measures, including, but not limited to, preparation of data inventory, conducting internal audits, training, registration to VERBIS, preparation of an authorisation matrix, conducting penetration tests, managing system access, retaining access logs, setting up firewalls and providing physical security of media on which data is stored.

15.2 Is there a legal requirement to report data breaches to the relevant data protection authority(ies)? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

Yes; in case of a data breach, the data controller is under the obligation to notify the data subject and the Authority of such situation as soon as possible. In Board resolution no. 2019/10, dated 24 January 2019, it is stated that "as soon as possible" should be interpreted as 72 hours and if the data controller fails to meet such period, an explanation relating to the delay must be provided to the Board. The data controller must use the Personal Data Notification Form published by the Authority for the purpose of such notification. The Board may also choose to declare such situation on its website.

15.3 Is there a legal requirement to report data breaches to affected data subjects? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

Yes; please refer to question 15.2 above. Additionally, the notification should be made to the data subject's contact address. If providing notice to the data subject is not possible, the data controller may choose another form of notice such as publication on its official website.

15.4 What are the maximum penalties for data security breaches?

In case of failure to take necessary security measures and notify the Authority of the breach, the Board may impose an administrative fine ranging from TL 15,000 to TL 1,000,000 on the data controller.

16 Enforcement and Sanctions

16.1 Describe the enforcement powers of the data protection authority(ies).

Investigatory Power	Civil/Administrative Sanction	Criminal Sanction
The Authority	Breach of obligation to inform – administrative fine ranging from TL 5,000 to TL 100,000.	N/A
The Authority	Breach of data security obligations – administrative fine ranging from TL 15,000 to TL 1,000,000.	N/A
The Authority	Failure to register with VERBIS and maintaining up-to-date registered data – administrative fine ranging from TL 20,000 to TL 1,000,000.	N/A
The Authority	Breach of the Board's resolutions – administrative fine of TL 25,000 to TL 1,000,000.	N/A
Criminal Courts	Unlawful recording of personal data.	1 to 3 years of imprisonment
Criminal Courts	Unlawful transfer, transmission and collection of personal data.	2 to 4 years of imprisonment
Criminal Courts	Failure to destroy personal data.	1 to 2 years of imprisonment

16.2 Does the data protection authority have the power to issue a ban on a particular processing activity? If so, does such a ban require a court order?

As per the PDPL, the Board has the duty and authority to render decisions on duties, authorities and obligations of data controllers. Therefore, the Board may issue a ban on a particular processing activity; however, decisions of the Board are administrative actions, cancellation of which can be claimed before administrative courts.

Additionally, circumstances which fall under criminal courts' jurisdiction cannot be decided upon by the Board.

16.3 Describe the data protection authority's approach to exercising those powers, with examples of recent cases.

Based on recent decisions in 2018 and 2019, the Authority exercises its powers upon data subject's complaints rather than *ex officio* investigations, and the majority of decisions are related to imposing administrative fines due to unlawful transfers of personal data to third parties.

16.4 Does the data protection authority ever exercise its powers against businesses established in other jurisdictions? If so, how is this enforced?

There have been no publicly announced cases where the Authority imposed an administrative fines on foreign persons; however, in its resolution no. 2019/10, the Board stated that in case of a data breach in another jurisdiction which has effects in Turkey, a foreign data controller is also under the notification obligations as mention under question 15.2.

17 E-discovery / Disclosure to Foreign Law Enforcement Agencies

17.1 How do businesses typically respond to foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies?

For foreign e-discovery requests or requests for disclosure from foreign law enforcement agencies, businesses should respond in accordance with the mutual judicial assistance treaties.

17.2 What guidance has/have the data protection authority(ies) issued?

The Authority has not yet issued any guidance on e-discovery.

18 Trends and Developments

18.1 What enforcement trends have emerged during the previous 12 months? Describe any relevant case law.

Data controllers are obliged to notify the data subjects and the Authority in case of a data breach and the Board may declare such situation on its website. The first of these data breach disclosures was published by the Authority on 4 May 2018. In this first example of the Board's data breach announcement, a data breach occurred in a company that provides transportation services. As stated in this resolution, 103,337 customers and 900 drivers resident in Turkey have been affected by this data breach. To date, the Board has published 22 data breach disclosures, and this number is increasing after Board resolution no. 2019/10, which explains in detail the data breach disclosure procedure together with the time limitations for data breach disclosures.

18.2 What "hot topics" are currently a focus for the data protection regulator?

The Authority and data protection foundations frequently hold summits and symposiums on data protection matters. The "hot topics" discussed in such summits and symposiums are VERBIS, GDPR's effect on innovation, data privacy aspects of artificial intelligence, big data, and blockchain.

Acknowledgment

The authors would like to thank Köksal Kaplan for his assistance in preparing this chapter. Köksal is an associate at Çiğdemtekin Çakırca Arancı Law Firm, specialising in corporate law.

Tel: +90 212 227 00 61 / Email: kkaplan@cdcalaw.com

Tuna Çakırca

Çiğdemtekin Çakırca Arancı Law Firm
Levent Mah. Zambaklı Sk.
No.10 Besiktas
Istanbul
Turkey

Tel: +90 212 227 00 61
Email: tcakirca@cdcalaw.com
URL: www.cdcalaw.com

Tuna Çakırca is a leading IT, M&A/corporate and capital markets lawyer. Her M&A experience includes representation of both sell- and buy-side clients in a wide range of sectors. She has also represented underwriters, issuers and/or selling shareholders, most recently for electricity and telecommunications companies. Additionally, Ms. Çakırca has extensive experience in representing foreign and local companies in connection with their corporate, commercial, regulatory, employment and real estate matters. She continues to assist many multinational companies in their day-to-day businesses in such areas. Prior to joining CCA, Ms. Çakırca was a senior associate at Chadbourne & Parke and prior to that she was an associate at Kinstellar and at White and Case. Tuna has been recognised as a key figure in IT sector in Turkey and as one of the leading corporate and M&A lawyers in Turkey.

İpek Batum

Çiğdemtekin Çakırca Arancı Law Firm
Levent Mah. Zambaklı Sk.
No.10 Besiktas
Istanbul
Turkey

Tel: +90 212 227 00 61
Email: ibatum@cdcalaw.com
URL: www.cdcalaw.com

İpek Batum specialises in corporate and commercial transactions, particularly in the areas of corporate law, IT law, data protection, mergers and acquisitions as well as dispute resolution. She assists local and foreign clients both on a daily and transactional basis.

ÇİĞDEMTEKİN • ÇAKIRCA • ARANCI
LAW OFFICE

Çiğdemtekin Çakırca Arancı Law Firm (CCA) is a full-service law firm with offices in Istanbul and Ankara, with highly recommended strong expertise in corporate and M&A practice, and IT law. The firm's strong local and international practice offers specialised legal advice to corporations, financial institutions and investors operating in a broad range of industries. Our firm comprises highly experienced partners and lawyers, all of whom are bilingual and have studied at recognised law schools in Turkey and/or abroad. We are committed to assisting clients with practical solutions to reach their business goals. We achieve this by closely monitoring legislation, case law and administrative practice, while thoroughly considering our client's business priorities. With our knowledge, experience and strong network, we ensure all legal matters and transactions are handled in an efficient, responsive and timely manner. Prominent international legal directories and peer-reviewed publications recognise CCA as a leading firm.