TURKEY

Gönenç Gürkaynak and İlay Yılmaz | ELIG, Attorneys-at-Law

1. LEGISLATION

1.1 Name/title of the law

The Data Protection Law (the Law), which has been pending since 2003 is published in the Official Gazette of 7 April 2016. This is the first separate and dedicated legislation covering general data protection in Turkey. The Law is based on EU Data Protection Directive 95/46/EC (the Directive), though it differs from the Directive in certain aspects.

A number of provisions applicable to data protection and privacy can also be found in a variety of other Turkish laws, including the Constitution of the Republic of Turkey of 9 November 1982 (the Constitution), and there are certain sector-specific regulations on this matter as well. The general provisions that are applicable to data protection and privacy are as follows:

- Article 20 (Privacy of Private Life) and article 22 (Freedom of Communication) of the Constitution.
- Article 24 (Protection of Personality against Violations) of the Turkish Civil Code (Civil Code).
- Article 135 (Recording of Personal Data), article 136 (Unlawfully Disseminating or Capturing Data), article 138 (Failure to Destroy Data) and article 244 (Preventing and Impairing the System, Altering or Destroying Data) of the Turkish Criminal Law (Criminal Code), which regulate unlawful storage of, transmission, reception or alteration of, and destruction of or failure to destroy personal data, respectively.

Moreover, the Regulation on Security of Electronic Communications, effective as of 13 July 2014, contains certain provisions on data security in the context of electronic communications.

Turkey also has a regulation on electronic commerce, entitled the Law on Regulation of Electronic Commerce (Law on E-Commerce), which regulates the principles and procedures regarding electronic commerce and imposes certain obligations on the main actors in electronic commerce with respect to the protection and processing of personal data. The Law on E-Commerce came into effect on 5 December 2014.

In addition, there are some sector-specific regulations particular to data protection and privacy, including:

- The Regulation on Processing and Protection of Privacy of Personal Data in the Electronic Communications Sector.
- The Regulation on Protection and Sharing of the General Health Insurance Data.
- The Regulation on Data Privacy and Principles and Procedures Regarding Security of Confidential Data in the Official Statistics.

Turkey is a party to the United Nations Universal Declaration of Human Rights and the Convention for the Protection of Human Rights and Fundamental Freedoms, and has signed the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data. The Law on Ratification of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of the Council of Europe (Convention 108) is published in the Official Gazette of 18 February 2016 and came into force on the same date.

1.2 Pending legislation

The secondary legislation relating to the implementation of the Law will enter into force within one year following the publication of the Law (that is, within one year after 7 April 2016).

1.3 Scope of the law

The Law aims to protect the fundamental rights and freedoms of the people with respect to the processing of personal data, particularly regarding the privacy of private life, and to regulate the procedures and principles along with the obligations to be followed by natural persons and legal entities that are processing personal data. The Law is applicable to natural persons whose data is processed and natural persons or legal entities that process personal data.

1.3.1 The main players

The main players stipulated under the Law are:

- The "data controller" is the natural person or legal entity that sets the objectives and means of processing personal data and is in charge of the establishment and management of the data filing system.
- The "data processor" is the natural person or legal entity that processes personal data based on the authority given by and on behalf of the data controller.
- The "data subject" is the natural person whose personal data is processed.
- The "Authority" is the Personal Data Protection Authority.
- The "Board" is the Personal Data Protection Board.

Under the Criminal Code, the person subject to the provisions is "the perpetrator" who commits the crimes stipulated under the Criminal Code on data protection, and "the prosecutor" prosecutes the crimes on data protection *ex officio* pursuant to the Criminal Code. Under the Civil Code, the main actors are "the person whose personal rights are violated" and "the person who violates another person's personal rights".

1.3.2 Types of data

Under Turkish law, all information relating to identified or identifiable natural persons or legal entities is deemed to be personal data. Also, according to the High Court of Appeals' precedents, personal data is defined as:

"information … that a person has not presented to an unauthorized third party and has shared with a limited entourage by disclosing it, that is not known by everybody and/or easily accessible, and which is identifying or making that person identifiable, and distinguishes that person from the other individuals in the society and is suitable to set forth its characteristics".

Data concerning the racial or ethnic origin, political opinions, philosophical beliefs, religion, sect or other beliefs, clothing and appearance, association, foundation or trade union membership, health or sex life of a person and criminal conviction or security measures regarding a person, along with their biometric and genetic information, are deemed to be special categories of personal data and may not be processed except with the explicit consent of the data subject. The processing of personal data without the explicit consent of the data subject is prohibited, and the

exceptions for processing special categories of personal data (such as religious belief or political opinion) are more limited than for the processing of other personal data, such as the name and surname of the data subject.

The sector-specific regulations also describe additional types of data. The Regulation on Processing and Protection of Privacy of Personal Data in the Electronic Communications Sector provides three types of data other than personal data: location data, traffic data and data. "Location data" is defined as certain data determining the geographical location of a device that belongs to a user of public electronic communications services and which is processed in the electronic communication network or through an electronic communication service. "Traffic data" is defined as any type of data processed in the transmission of communication in an electronic communication network or for the purposes of invoicing. The term "data" is defined as all information identifying the user or subscriber, including the traffic data and location data.

In the Regulation on Protection and Sharing of the General Health Insurance Data, data regarding the health services provided to a general health insured and his/her dependents is defined as "medical data". Another type of data regulated under the Regulation on Bank Cards and Credit Cards is "sensitive data regarding cards", which is defined as the PIN information that is written on a bank card or credit card which enables financial transactions to be made when possessed. There are further examples of the types of data elsewhere in Turkish law, but the foregoing constitutes the most common.

1.3.3 Types of acts/operations

The Law is applicable to the data processed wholly or partly by automatic means or by non-automatic means, provided that the data is part of a data filing system. "Data filing system" means any system in which personal data is processed, being structured according to specific criteria.

The Law covers all kinds of personal data "processing", which is defined as any operation performed on personal data, wholly or partly, whether through automatic means, or, if the data is part of a data filing system, through non-automatic means, such as collection, recording, storage, preservation, alteration, retrieval, disclosure, transfer, acquisition, making available, categorising or blocking.

The Law requires erasure, destruction or anonymisation of personal data by the data controller either *ex officio* or upon the request of the data subject (even if such data is processed in line with the Law or other laws), when the reasons for the processing of personal data are no longer valid.

The Law regulates the transmission of personal data. As mentioned above, personal data cannot be transferred without the explicit consent of the data subject, subject to exceptions. For a more detailed explanations see *Section 3.2* above.

1.3.4 Exceptions

The Law is not applicable where personal data is processed:

By natural persons in the course of activities that are completely personal or relating to the family members living in the same household, provided that the personal data is not shared with third parties and the data security obligations are fulfilled and complied with.

For purposes of research, planning or statistical operations after being anonymised as official statistics, such as the statistics of Turkish Statistical Institute or the statistics kept by universities for research purposes.

For artistic, historical, literary or scientific purposes, or within the scope of the freedom of speech, provided that national defence, national security, public safety, public order, economic safety, the privacy of private life or personal rights are not violated and the processing does not constitute a crime.

By public institutions and organisations which are authorised by law within the scope of their preventive, protective and intelligence activities for national defence, national security, public safety, public order or economic safety.

With respect to investigation, prosecution, trial and execution procedures by judicial organs or law enforcement authorities.

On the other hand, article 24 of the Civil Code, which is also applicable to the protection of personal data, provides for an exception to the violation of personal rights where:

- The person whose personal rights are violated gives consent.
- There is a prevailing private or public benefit.
- The authority granted by the law is exercised.

The Criminal Code also provides for certain exceptions regarding the application of the penalties, which would also apply to data breaches, where the perpetrator is:

- Performing an obligation imposed by law.
- Performing a legal right.
- Subject to irresistible or unrecoverable force and violence.
- Under absolute and heavy intimidation and threat.
- Where the perpetrator makes an inevitable mistake regarding the wrongfulness of its actions.
- Under the age of 12, or between 12 and 15 but is not capable of understanding the legal consequences of his/her actions.
- Mentally handicapped.
- Temporarily under the effect of a drug, which he/she took involuntarily, rendering him/her incapable of understanding the consequences of his/her actions, while committing the crimes stipulated in the Criminal Code.

1.3.5 Geographical scope of application

The Law does not contain an explicit provision as to its geographical scope of application, but it should be applicable within the Turkish jurisdiction, as are the Civil Code and Criminal Code.

However, when there is a foreign element in a private law dispute regarding data protection, the applicability of the Civil Code and the Law will be determined according to the Turkish conflict of laws principles.

On the other hand, pursuant to article 8 of the Criminal Code, Turkish laws apply to crimes committed in Turkey. Moreover, if the act is partially or completely committed in Turkey or the consequences occur in Turkey, the crime is deemed to have been committed in Turkey.

1.3.6 Particularities

Online or other general terms and conditions relating to data processing might be deemed invalid if they include provisions to the detriment of the counterparty, which are aggravating the counterparty's contractual conditions, against good faith.

2. DATA PROTECTION AUTHORITY

Currently, there is no specific data protection authority in Turkey. However, the Law stipulates the establishment of a supervisory authority, called the Personal Data Protection Authority, which has the authority to supervise the compliance of the data processing systems with the Law. Any automatic and non-automatic system enabling processing of data would be considered to be a data processing system. The Personal Data Protection Authority will be an independent authority comprised of nine members.

Five members of the authority will be selected by the Turkish Grand National Assembly, two members will be selected by the Council of Ministers and two members will be elected by the President of Turkish Republic. The decision-making organ of the authority is the Board.

Turkish courts are also entitled to order seizure of unauthorised and/or unlawful processing of personal data in cases where there is a personal right violation, based on the claimant's application.

In addition, there is a specific authority for electronic communications in Turkey. Pursuant to the Electronic Communications Law, the Information and Communication Technologies Authority (ICTA) is responsible for making the necessary arrangements and supervisions pertaining to the rights of subscribers, users, consumers and end users, as well as the processing of personal data and the protection of privacy. ICTA exercises its authority through the Information Technologies and Communication Board. There are a significant number of Information Technologies and Communication Board decisions imposing general data protection principles on the operators in the electronic communications sector. Furthermore, ICTA determines the procedures and principles for the processing of personal data and the protection of privacy in the electronic communications sector.

The contact details for ICTA are:

Information and Communication Technologies Authority
Bilgi Teknolojileri ve İletişim Kurumu
Yeşilırmak Sokak No 16
Demirtepe 06430 Ankara
Turkey
t +90 312 294 72 00
f +90 312 294 71 45
w www.eng.btk.gov.tr

2.1 Role and tasks

The Personal Data Protection Authority has an obligation to pursue the duties stipulated by the Law, including, but not limited to, preparing an annual report on its activities, ensuring all register entries on data processing are complete, cooperating with domestic and foreign authorities with respect to the protection of personal data, following the developments in data protection laws and taking the necessary measures to ensure they are applied, preparing, developing and conducting technical assistance projects and research in the necessary fields in cooperation with the national and international authorities, and performing other duties assigned by laws, such as the legislation establishing the Personal Data Protection Authority (which has not been prepared at the time of writing).

Currently, ICTA is responsible for making the necessary arrangements and supervisions pertaining to the rights of subscribers, users, consumers and end users, as well as the processing of personal data and the protection of privacy in the electronic communications sector (*see Section 2 above*).

2.2 Powers

The Personal Data Protection Authority will be vested with the following powers:

- Deciding on applications regarding violations of personal rights.
- Taking interim measures in order to prevent the possibility of damages being incurred by the data subject.
- Preparing regulatory actions regarding the processing of personal data.
- Rendering a decision if there are concerns regarding the transfer of data abroad (if the applicable legislation does not provide a clear authorisation).
- Deciding on the President's proposals with regard to measures to be taken regarding the protection of personal data.
- Enactment of the secondary legislation regarding implementation of the Law.

ICTA is entitled to determine the procedures and principles for the processing of personal data and the protection of privacy in the electronic communications sector.

2.3 Priorities

Not applicable.

3. LEGAL BASIS FOR DATA PROCESSING

Article 20 of the Constitution constitutes the main legal basis for the processing of personal data. Personal data may only be processed in cases where it is stipulated by law or with the data subject's explicit consent. Similar to the Constitution, the prior consent of the data owner is also considered to be a justifying element under the Civil Code, except where there is a higher private or public interest, or in case of the exercise of a legal right under the Civil Code.

On the other hand, the Law includes "clear, certain and legitimate purpose" as one of the general principles for processing personal data. The personal data must be processed to achieve the relevant purpose and be limited to this purpose. Therefore, the personal data may not be processed if the relevant processing is not related to the purpose. Personal data can only be processed in accordance with the provisions of the Law and other laws. Data processing must be lawful and in line with good faith, and the personal data must be precise and up to date where necessary, and the data processed must be preserved for the period of time determined by the relevant legislation or the period deemed necessary for the purpose of the processing.

3.1 Consent

3.1.1 Definition

Article 20 of the Constitution requires the explicit consent of the data subject in order to be able to process his/her personal data, as meaning that nobody can have any doubt as to the data subject's will.

The Law also requires explicit consent of the data subject for processing of his/her personal data. The Law provides exceptions for the explicit consent requirement, and states that if one of the relevant exceptions listed under the Law exists, the personal data can be processed without obtaining the data subject's explicit consent.

3.1.2 Form

Neither the Constitution nor the Law specifies the form in which the consent must be given. However, for evidential purposes, it is recommendable that it is obtained in writing.

3.2 Other legal grounds for data processing

Pursuant to the Law, personal data cannot be processed without the explicit consent of the data subject, except where one of the conditions below applies:

- It is explicitly foreseen by law.
- Processing is necessary to protect the vital interests or the bodily integrity of the data subject, or of another person, where the data subject is physically or legally incapable of giving his/her consent.
- Processing personal data of the parties of a contract is necessary, on condition that the processing is directly related to the execution or performance of such contract.
- Processing is necessary for compliance with a legal obligation to which the data controller is subject.
- The data has already been made public by the data subject.
- Processing is necessary for the establishment, exercise or defence of a legal claim.
- Processing is necessary for the purposes of the legitimate interests of the data controller, provided that such interests do not violate the fundamental rights and freedoms of the data subject.

In parallel, special categories of personal data are prohibited from being processed without the data subject's explicit consent. Special categories of personal data, other than those relating to health and sex life, may be processed without the explicit consent of the data subject if the processing is explicitly allowed by law. Personal data relating

to health and sex life may be processed without the explicit consent of the data subject only if the data is processed by authorised entities and institutions or by persons who are under an obligation of confidentiality for the purposes of protecting public health, preventive medicine, medical diagnosis, planning, managing and financing of treatment and maintenance services.

3.3 Codes of conduct

Not applicable.

4. SPECIAL RULES

4.1 Employment

There are no specific laws governing the processing of personal data in the employment relationship. However, there is a particular provision imposing certain obligations on employers with respect to their employees' personal information. Pursuant to article 75 of the Turkish Labour Law, employers are obliged to keep personnel files on their employees but are obliged to use this information in good faith, and in accordance with the law.

4.2 Health

As per article 78 of the Law on Social Security and General Health Insurance, in principle the health information of the insured person and the persons that the insured person is obliged to look after is confidential.

The Medical Deontology Bylaw and the Patient Rights Regulation stipulate that information obtained during medical procedures cannot be disclosed unless required by law.

4.3 Finance

Article 73 of the Banking Law stipulates that personal information must not be disclosed by banks and persons who have acquired such information because of their role or duties, even after they leave their role or duties, except when requested by the competent authorities. In addition to the authorisation of public prosecutors and courts, the Banking Law also entitles the Banking Regulation and Supervision Agency to audit banks and request any information (including that classified as confidential). The banks, their subsidiaries, associations, branches, representative offices and outsourcing institutions, as well as any other natural or legal persons related to those banks, are obliged to provide any and all necessary systems, passwords, documents, records and information upon such request.

Under the Bank Cards and Credit Cards Law, member enterprises cannot disclose, keep or copy the information they acquired from consumers without their consent, except for requests by authorised authorities. Member enterprises cannot share, sell, buy or trade such information, and may only do so with the affiliated bank-card issuer.

4.4 Telecommunications

The Electronic Communications Law is the primary law applicable to the telecommunications and telecoms companies. The Regulation on Processing and Protection of Privacy of Personal Data in the Electronic Communications Sector (Regulation on Electronic Communications), which is based on the Electronic Communications Law, sets out the procedures and principles to be followed by operators (namely any legal entity

authorised to provide electronic communications services and/or to provide an electronic communications network and operate the infrastructure) active in the electronic communications sector with respect to the processing and retention of personal data and the protection of privacy in the electronic communications sector.

The main principles for processing personal data, stipulated under the Regulation on Electronic Communications, are quite similar to the principles set out in Convention No 108. The Regulation on Electronic Communications encompasses the retention of data, including personal data, traffic data and location data. However, retention of the communication's content is not included in the scope of the regulation and, in fact, is expressly excluded.

4.5 Historical, statistical and scientific research purposes

The Law provides an exception for personal data processed for scientific and statistical purposes. In particular, if personal data is processed for purposes of research, planning or statistical operations after being anonymised as official statistics, the Law will not apply. Moreover, if personal data is processed for artistic, historical, literary or scientific purposes or within the scope of freedom of speech, provided that national defence, national security, public safety, public order, economical safety, the privacy of private life or personal rights are not violated and the processing does not constitute a crime, the Law will not apply either.

The Regulation on Data Privacy and Principles and Procedures Regarding Security of Confidential Data in the Official Statistics sets out the principles and procedures with respect to data privacy and the maintenance of security of confidential information in official statistics.

4.6 Children

Not applicable.

4.7 Whistleblowing

Not applicable.

4.8 Email, internet and video monitoring

Although there are no specific regulations as to email, internet and video monitoring with respect to data protection, article 20 of the Constitution provides that personal data may only be processed if it is allowed by the laws or by the data subject's explicit consent. Therefore, for example, it is important to indicate when there are surveillance cameras and to inform persons subject to surveillance.

As for the monitoring of email and the internet in the scope of an employment relationship, an employer should obtain the explicit consent of its employees for such monitoring, except for certain instances, such as if the employee uses business computers for business correspondence and the employer has notified the employees that the computers and internet should not be used for personal purposes.

4.9 Direct marketing and cookies

The Law on Regulation of Electronic Commerce (E-Commerce Law) aims to regulate the principles and procedures regarding commercial electronic communications, especially the information obligation. The scope of the regulation covers all kinds of communication sent by electronic means to promote goods and services or brands of natural or

legal persons, directly or indirectly. The E-Commerce Law requires prior opt-in consent before sending electronic commercial communications.

There are no special rules regarding cookies under Turkish law. However, the Constitution and the Law require the data subject's explicit consent to process personal data, confirmed by the applicable laws with respect to data protection and High Court of Appeals' precedents. Therefore, cookies may only be legitimately used once the data subject's explicit consent has been obtained.

4.10 Big data

Not applicable.

4.11 Mobile apps

Not applicable.

5. DATA QUALITY REQUIREMENTS

The general preamble of the Law adopts the principle of data quality. This principle stands for the actuality, completeness and correctness of personal data and purpose limitation. The personal data should be adequate, relevant and not excessive in relation to the purposes for which it is processed. It must also be accurate and, where necessary, kept up to date. These requirements are also applied in the Regulation on Electronic Communications.

6. OUTSOURCING AND DUE DILIGENCE

6.1 Outsourcing

Not applicable.

6.2 Due diligence

Not applicable.

7. INTERNATIONAL DATA TRANSFERS

7.1 Applicable rules

The Law regulates the transfer of personal data abroad. In principle, personal data cannot be transferred abroad without the explicit consent of the data subject, except in specific circumstances.

7.2 Legal basis for international data transfers

The exceptions where personal data can be transferred abroad without the explicit consent of the data subject are: if the country to which the personal data is to be transferred provides an adequate level of protection; or, if the protection is not adequate in such country, then the data controllers in Turkey and in such country may provide a written undertaking guaranteeing an adequate level of protection, which should be authorised by the Board.

The Board determines which countries have an adequate level of protection and announces them publicly. The Board determines whether a foreign country can afford an adequate level of protection and whether data transfers will be authorised after consulting with the relevant public administrations and agencies, if necessary, and by evaluating:

- The international agreements to which Turkey is a party.
- The reciprocity relating to data transfers between Turkey and the country to which the personal data will be transferred.
- The category of the personal data, as well as the purpose and period of processing for each specific data transfer.
- The relevant legislation and practice in the foreign country to which the data will be transferred.
- The measures that the controller in the foreign country to which the data will be transferred commits to provide.

Without prejudice to the provisions of international treaties, if the interests of Turkey or the data subject will be seriously undermined, personal data may only be transferred abroad upon the authorisation of the Board, having ascertained the relevant public institution's or authority's opinion.

7.2.1 Data transfer agreements

Turkey does not have specific rules for data transfer agreements. Therefore, the general provisions of the Law and Turkish Code of Obligations are applicable to data transfer agreements. However, data transfer agreements may be regulated once the Law enters into force and the Personal Data Protection Authority has taken up its duty.

Currently, the data protection provisions and principles found in various laws may be taken into account, along with the specifics of the EU legislation, while applying the general provisions to data transfer agreements. The Turkish courts take these provisions and principles into account, and the data transfer agreements which are not compliant with them can be deemed void by the courts. Furthermore, the Law is expected to enter into force soon, and it would be prudent for the parties of a data transfer agreement to act in accordance with the Law to avoid any disputes with respect to validity of the agreement in the future.

7.2.2 Binding corporate rules

Not applicable.

7.2.3 Safe Harbour and Privacy Shield

Not applicable.

7.2.4 Other legal bases

Not applicable.

7.3 E-discovery and law enforcement requests

Not applicable.

7.4 Representative

Not applicable.

8. INFORMATION OBLIGATIONS

8.1 Who

The data controller, or any person authorised by the data controller, is obliged to provide the relevant data subjects with information.

Pursuant to the Regulation on Processing and Protection of Privacy of Personal Data in the Electronic Communications Sector, operators providing electronic communications also have certain obligations for informing the subscribers/users.

8.2 What

The data controller, or any person authorised by the data controller, is obliged to provide the data subjects with the following information:

- The identity of the data controller and of his/her representative, if any.
- The purposes of the processing.
- To whom and for what purpose the processed personal data can be transferred.
- The method and legal ground of the collection.
- Data subject's rights.

8.3 Exceptions

See *Section 1.3.4* above.

8.4 When

The data subject should be informed during the collection of the personal data.

8.5 How

Not applicable. However, it is recommended that the data subjects are informed in writing.

9. RIGHTS OF INDIVIDUALS

Data subjects have the rights to:

- Apply to the data controller in order to learn whether or not any data relating to him/her is being processed.
- Request relevant information, if personal data relating to him/her is being processed.
- Obtain information as to the purpose of the processing and whether or not the personal data has been processed accordingly.

- Obtain information as to any third persons within or outside the country to whom personal data is being transferred.
- Ask for the correction of any incomplete or inaccurate processing of personal data.
- Ask for the erasure or destruction of personal data.
- Request the notification to third parties to whom the data has been transferred of corrections relating to any inaccurate or incomplete personal data processing or any erasure, destruction or anonymisation of personal data.
- Object to any negative consequences which might occur to him/her pursuant to the analysis of the processed personal data exclusively by means of automated systems.
- Demand compensation for the damages suffered as a result of an unlawful processing operation.

9.1 Who

Any natural person whose personal data is processed may exercise these rights.

9.2 What

See *Section 9* above.

9.3 Exceptions

The rights listed in *Section 9* above may be restricted – as long as such restriction is in accordance with the purpose of the Law and its principles, and is proportionate – if:

- Processing of personal data is necessary for the prevention of a crime or for a criminal investigation.
- The personal data processed has already been made public by the data subject.
- The processing of the personal data is necessary for the performance of supervisory or regulatory duties, along with disciplinary investigation or prosecution by the assigned and authorised public institutions and agencies, or professional organisations carrying the nature of public institutions (such as labour unions and bar associations), based on an authorisation by law.
- The processing of personal data for the protection of the state's economic and financial interests with respect to the budget, tax and financial matters.

9.4 When

Not applicable.

9.5 How

The Law, the requests should be made in writing or by other means to be determined by the Personal Data Protection Authority.

9.6 Charges

Not applicable.

10. SECURITY OF DATA PROCESSING

10.1 Confidentiality

In principle, personal data may not be disclosed to a third party without the explicit consent of the data subject.

10.2 Security requirements

According to the Law, the data controller is obliged to take the appropriate technical and administrative measures to protect the personal data. There are no specific technical requirements described under the Law yet. However, the International Organization for Standardization (ISO) already has a set of standards with respect to technical data security measures entitled ISO/IEC 27000, though it is not clear whether these ISO standards are sufficient to comply with the information security requirement set forth under the Law.

10.3 Data security breach notification obligation

10.3.1 Who

The breach notification obligation is incumbent on the data controller, the data processor and operators.

10.3.2 What

In the event that the processed personal data is unlawfully obtained by others, the data controller shall notify the issue to the data subject and the Board. If necessary, the Board may announce the issue on its own website or via any other means it deems appropriate.

The Regulation on Processing and Protection of Privacy of Personal Data in the Electronic Communications Sector obliges the operators to effectively inform their subscribers/users of risks violating the security of personal data and the network, and/or of the existing violations of personal data protection, provided that ICTA and the Board deem it necessary.

10.3.3 Exceptions

Not applicable.

10.3.4 When

The notification must be done as soon as possible or, in case of the Regulation on Processing and Protection of Privacy of Personal Data in the Electronic Communications Sector swiftly.

10.3.5 How

Not applicable.

10.4 Cybersecurity

Cybersecurity is not regulated by any specific legislation in Turkey, but cybersecurity provisions are found in separate regulations. As a governmental step for maintaining cybersecurity in Turkey, a decision regarding conducting,

managing and coordinating national cybersecurity activities came into force on 20 October 2012. On 20 June 2013, another decision on the national cybersecurity strategy and action plan for the years 2013–2014 came into force. The action plan aimed to protect public IT systems and critical IT infrastructures (such as national security-related military infrastructures) operated by both the government and the private sector. One of the key actions under the action plan was specified as amending primary legislation by considering the needs of cybersecurity in Turkey. There is already an established Cyber Security Board in Turkey, which is entitled to determine governmental precautions regarding cybersecurity, to approve national cybersecurity strategies and procedures and principles, and to maintain national cybersecurity and coordination. Preparation of the action plan for 2015–2016 continues as of April 2016. Currently there are no specific obligations that apply to companies or private organisations specifically with respect to cybersecurity. However, the Law introduced data security obligations for data processors and data controllers (*see the first part of this section*).

11. DATA PROTECTION IMPACT ASSESSMENTS, AUDITS AND SEALS

Not applicable.

12. REGISTRATION OBLIGATIONS

Persons or legal entities processing personal data should register with the Data File Registry before processing personal data. The Board may grant exemptions based on certain objective criteria, such as the type of personal data, the amount of data and that the processing is based on a specific law.

12.1 Notification requirements

12.1.1 Who

Persons or legal entities processing personal data are required to register with the Data File Registry by notification.

12.1.2 What

The following information should be provided by the applicant:

- Identity and address of the data file owner or its representative, if any.
- Purpose for the processing of the data.
- Explanations pertaining to the (categories of) data subjects and relevant personal data.
- Recipients or categories of recipients to whom the personal data may be disclosed.
- Type of personal data expected to be transferred to third countries.
- Measures taken with respect to data security.
- Maximum period of time needed for the purposes of processing personal data.

12.1.3 Exceptions

The registration obligation will not apply – as long as such restriction is in line with the purpose of the Law and its principles, and is proportionate – if:

- The processing of personal data is necessary for the prevention of a crime or for a criminal investigation.
- The personal data processed has already been made public by the data subject.
- The processing of personal data is necessary for the performance of supervisory or regulatory duties, along with disciplinary investigation or prosecution by the assigned and authorised public institutions and agencies, or professional organisations carrying the nature of public institutions, based on an authorisation by law.
- The processing of personal data for the protection of the state's economic and financial interests with respect to the budget, tax and financial matters.

Also, the Board may provide an exemption for the obligation to register in accordance with objective criteria to be determined by the Board, such as the nature and the number of the processed data, whether or not data processing is required by law, or whether or not data will be transferred to third parties. As the Board is not yet established, specific exceptions are not yet clear.

12.1.4 When

The registration notification should be made prior to processing personal data and changes should be notified immediately.

12.1.5 How

The Law does not stipulate the form of the notification. A preliminary examination is conducted by the Data File Registry at the latest within a month after the submission of the notification.

12.1.6 Charges

Not applicable.

12.2 Authorisation requirements

Not applicable.

12.3 Other registration requirements

Not applicable.

12.4 Register

The Personal Data Protection Authority is obliged to keep a public Data File Registry. The data file owners are obliged to register with this Data File Registry, which contains the information indicated in *Section 12.1.2* above. The Data File Registry must be maintained publicly under the supervision of the Board. Accordingly, natural and legal persons who process personal data should be registered with this Registry prior to begin data processing.

13. DATA PROTECTION OFFICER

13.1 Function recognised by law

Not applicable.

13.2 Tasks and powers

Not applicable.

14. ENFORCEMENT AND SANCTIONS

14.1 Enforcement action

The Personal Data Protection Authority may evaluate complaints regarding the application of data protection provisions and send instructions to the data file owners, or may decide to cease the processing of personal data and impose administrative fines.

14.2 Sanctions

The Law on Data Protection refers to the existing sanctions for data breaches under the Criminal Code. The criminal sanctions stipulated under the Criminal Code are as follows:

- Whoever unjustly records personal data shall be imprisoned for six months to three years.
- Whoever unjustly acquires or disseminates personal data or gives personal data to somebody else shall be imprisoned for one to four years.
- Whoever fails to destroy any personal data after the retention period set forth in the law has been passed shall be imprisoned for six months to one year.
- Whoever produces, imports, dispatches, transports, stores, accepts, sells, exposes for sale, buys, supplies and keeps equipment, a computer program, a password or other security code which is specifically used as a tool for the aforementioned cybercrimes set forth under the Criminal Code or used as a tool for any other crimes committed by electronic means shall be imprisoned for one year to three years and be subject to a punitive fine up to 5,000 days.

The aforementioned crimes mainly concern unlawful processing of personal data. In addition, article 18 of the Law regulates minor offences, and envisages administrative fines ranging from Turkish Lira 5,000 to 1,000,000 (approximately EUR 1,500 to EUR 300,000) for breaches of certain provisions of the Law.

14.3 Examples of recent enforcement of data protection rules

Not applicable.

15. REMEDIES AND LIABILITY

15.1 Judicial remedies

Complainants who claim that there is a violation of the data protection rules and that the violation constitutes a crime may apply to the public prosecutors for prosecution under the Criminal Code or under the Law, when it comes into effect.

In addition, pursuant to article 24 of the Civil Code, a civil action can be initiated before the general courts due to a violation of personal rights.

15.2 Class actions

Not applicable.

15.3 Liability

Under Turkish law, individuals may claim damages arising from data breaches. The person who caused such a data breach would liable according to the general provisions of Turkish law.