Turkey

ELIG Attorneys at Law
Gönenç Gürkaynak, Ilay Yılmaz & Ceren Yıldız

1. LEGISLATION

1.1 Name/title of the law

Turkey has no specific fully-fledged law governing the privacy of personal data. The applicable legislation in this respect is:

- Articles 20 and 22 of the Turkish Constitution of 1982, which generally protect privacy of personal life and communication, respectively;
- Article 24 of the Turkish Civil Code, which entitles individuals whose personal rights are unjustly violated to file a civil action; and
- Articles 135, 136 and 138 of the Turkish Criminal Code, which regulate unlawful storage of, transmission or reception of, and failure to destroy personal data, respectively.

1.2 Pending legislation

There is a draft law on the protection of personal data (Draft Law), which has been submitted to the General Assembly of the Turkish law-making parliament for ratification, however, no progress has been made since the Draft Law was put on the agenda in 2006 and the Draft Law is declared as being void in the Turkish parliament's online records.

1.3 Scope of the law

1.3.1 The main players

Due to the lack of a comprehensive law on the issue, the players are not explicitly defined under the legislation. Having said that, the Turkish Criminal Code imposes sanctions on persons who unjustly: (i) record or (ii) acquire or disseminate personal data, or give personal data to third persons.

1.3.2 Types of data

The Turkish Civil Code does not provide a comprehensive list in respect of personal rights and leaves the matter to the discretion of the judge. Therefore, the question of whether the data that will be collected qualify as a personal right within the meaning of Article 24 of the Turkish Civil Code will depend on the judicial precedents on the matter. In this respect, the relevant jurisprudence and the scholarly writings give weight to the will of the data owner, ie, the fact of whether the data owner considers the collected data to be personal.

Unlike the Turkish Civil Code, the Turkish Criminal Code adopts a definition of 'personal data', which does not fall far from the definition provided in the Council of Europe's Convention of 28 January 1981 for the

Protection of Individuals with regard to Automatic Processing of Personal Data. On this basis, the rationale of the Turkish Criminal Code makes reference to the penal code of France and states that '*information relating to and sufficient enough to identify an individual*' would qualify as 'personal data' within the meaning of Article 9 of the Turkish Criminal Code. Nevertheless, the question of whether any given data would qualify as 'personal data' will ultimately be assessed by the criminal judge on a case-by-case basis.

1.3.3 Types of acts/operations

Article 20 of the Turkish Constitution of 1982 regulates the act of processing – without any definitions – and states that personal data may only be processed in cases where it is stipulated by law or with the owner's explicit consent.

Article 22 of the Turkish Constitution of 1982 regulates the privacy of communication and states that communication cannot be hindered and its privacy cannot be violated.

Article 24 of the Turkish Civil Code addresses 'violation' and entitles individuals whose personal rights are unjustly violated to file a civil action. The Turkish Criminal Code regulates the acts of:

(i) unlawful storage of personal data;
(ii) unlawful transmission or reception of personal data; and
(iii) failure to destroy any personal data even after the waiting periods set forth in the law have passed.

The Turkish Criminal Code addresses the unlawful storage of, transmission or reception of, and failure to destroy personal data. However, the Turkish Criminal Code (or any other statute) does not define the phrase 'unlawful'. The term unlawful in this context may be interpreted as storage or transmission of personal data without consent from the relevant individuals.

1.3.4 Exceptions

Article 24 of the Turkish Civil Code stipulates that all violations addressed to personal rights are deemed unlawful except where:

(i) the person whose rights are violated gives his/her consent;
(ii) there is a higher private or public benefit; or
(iii) authorisation which has arisen from law is exercised.

1.3.5 Geographical scope of application

The legislation currently in force applies to the territory of Turkey.

1.3.6 Particularities

As per the Turkish Criminal Code, if the person who unlawfully stores, transmits or receives personal data is a public officer and is committing these crimes by misusing its public authority, or benefits the facilities of a particular profession and art, the punishment shall be increased by 50 per cent.

2. DATA PROTECTION AUTHORITY

There is no specific data protection authority in Turkey.

Pursuant to Article 24 of the Turkish Civil Code, an individual whose personal rights are violated unjustly is entitled to file a civil action before the general courts.

As per Article 139 of the Turkish Criminal Code, the data privacy crimes stipulated thereunder are *ex officio* investigated by the public prosecutor and are not subject to complaint by the injured party. In this respect, Turkish public prosecutors and courts are authorised to protect data privacy.

2.1 Role and tasks

Not applicable.

2.2 Powers

Turkish courts are authorised to impose criminal and legal sanctions.

2.3 Priorities

Not applicable.

3. LEGAL BASIS FOR DATA PROCESSING

3.1 Consent

3.1.1 Definition

Article 20 of the Turkish Constitution of 1982 states that personal data may be processed with the owner's explicit consent. 'Consent' regarding data privacy is not defined in any relevant legislation or case law.

By virtue of Article 24/II of the Turkish Civil Code, prior consent of the data owner is considered to be a legitimising factor.

The term 'unlawful' in Articles 135 and 136 of the Turkish Criminal Code may be interpreted to mean lack of consent from the relevant individuals for storage, transmission or receipt of the personal data.

3.1.2 Form

Not applicable.

3.1.3 In an employment relationship

The Turkish Employment Law provides that the employer is obliged to use the personal data of its employees in accordance with the law and the principle of good faith.

3.2 Other legal grounds for data processing

Other legal grounds include cases where there is a higher private or public benefit or authorisation which has arisen from law is exercised.

3.3 Direct marketing and cookies

Not applicable.

3.4 Data quality requirements

Not applicable.

3.5 Outsourcing
Not applicable.

3.6 Email, internet and video monitoring
3.6.1 General rules
Not applicable.

3.6.2 Employment relationship
Personal data should be used in accordance with the laws and the principle of good faith. There are no legal obstacles against the employee granting consent to his/her employer for the use of its personal data.

4. INFORMATION OBLIGATIONS
There is no obligation to provide any information to data subjects in Turkey.

5. RIGHTS OF INDIVIDUALS
5.1 Access
5.1.1 Right
Under Article 20 of the Turkish Constitution of 1982, everyone has the right to request the protection of their personal data. This right covers providing information to the relevant person about their personal data; access to their personal data; the right to request the rectification or erasure of their personal data; or the right to know whether their data are being used lawfully and in accordance with proper purposes.

5.1.2 Exceptions
Not applicable.

5.1.3 Deadline
Not applicable.

5.1.4 Charges
Not applicable.

5.2 Rectification
5.2.1 Right
Article 20 of the Turkish Constitution of 1982 provides the right to request the rectification of incorrect personal data.

5.2.2 Exceptions
Not applicable.

5.2.3 Deadline
Not applicable.

5.2.4 Charges
Not applicable.

5.3 Erasure

5.3.1 Right

Article 20 of the Turkish Constitution of 1982 provides the right to request the erasure of personal data.

5.3.2 Exceptions

Not applicable.

5.3.3 Deadline

Not applicable.

5.3.4 Charges

Not applicable.

5.4 Blocking

Not applicable.

5.5 Objection

Not applicable.

5.6 Automated individual decisions

Not applicable.

5.7 Other rights

5.7.1 Right

Article 20 of the Turkish Constitution of 1982 provides the right to find out if personal data are being used in accordance with proper purposes.

5.7.2 Exceptions

Not applicable.

5.7.3 Deadline

Not applicable.

5.7.4 Charges

Not applicable.

6. REGISTRATION OBLIGATIONS

Not applicable.

7. DATA PROTECTION OFFICER

7.1 Function recognised by law

It is not mandatory to appoint a data protection officer and this role is not recognised by law.

Appointing data protection officers in organisations is not very common in Turkey.

7.2 Tasks and powers
Not applicable.

8. INTERNATIONAL DATA TRANSFERS
8.1 Applicable rules
Article 136 of the Turkish Criminal Code, without making a distinction between international and domestic data transfers, states that anyone who unlawfully transfers personal data shall be sentenced.

8.2 Legal basis for international data transfers
Not applicable.

9. SECURITY OF DATA PROCESSING
There is no specific obligation with regard to the confidentiality or the security of personal data in the data protection provisions. The general provisions, ie Articles 20 and 22 of the Turkish Constitution of 1982, Article 24 of the Turkish Civil Code, and Articles 135, 136 and 138 of the Turkish Criminal Code, as stipulated above apply.

9.1 Confidentiality
Not applicable.

9.2 Security requirements
Not applicable.

9.3 Data security breach notification obligation
There exists no obligation to notify individuals or any authority about any data breaches. Such notifications are not common in practice in Turkey. However, under general provisions that apply to personal data, anyone whose rights with respect to his/her personal data are breached, might sue the breaching party or might notify the suspect to the competent authorities for criminal investigation if the breach constitutes a crime.

9.4 Data protection impact assessments and audits
Not applicable.

10. ENFORCEMENT, SANCTIONS, REMEDIES AND LIABILITY
10.1 Enforcement actions
As per Article 139 of the Turkish Criminal Code, the data privacy crimes stipulated under the Turkish Criminal Code are *ex officio* investigated by the public prosecutor.

In this respect, public prosecutors and consequently courts can take enforcement actions.

10.2 Sanctions
Sanctions under the Turkish Criminal Code include:

- Article 135/I: Unlawful storage of personal data may trigger

imprisonment from six months to three years.

- Article 136/I: In the case of unlawful transmission or receipt of personal data, the penalty is increased to imprisonment from one year to four years.
- Article 138: Any person who fails to destroy any personal data, even after the waiting periods set forth in the law have passed, may face imprisonment from six months to one year. If such crimes are committed by a legal entity, the entity will be subject to the security measures set forth under Article 60 of the Turkish Criminal Code. Such security measures are, as the case may be: (i) if the entity carries out its commercial activities by virtue of a permit granted by a public institution, cancellation of such permit of activity; and (ii) seizure of the relevant goods and objects that were used in committing the crime.

There are no administrative offences and penalties stipulated by law, however, persons whose personal rights are violated might apply to general courts and request pecuniary and non-pecuniary damages.

10.3 Examples of recent enforcement of data protection rules

We are not aware of any precedents regarding the enforcement of the foregoing rules.

10.4 Judicial remedies

Pursuant to Article 24 of the Turkish Civil Code, an individual whose personal rights are violated unjustly is entitled to file a civil action before the general courts. Personal rights capture the personal data as well.

Courts are entitled to stop the distribution, publication etc of any personal data which are used without the owner's permission and/or against the law. For example, in a precedent of the Supreme Court Assembly of Chambers (2001/4-926E and 2001/742K) dated 17 October 2001, a photograph of a person was published without permission, and the court of first instance decided to stop the publication and distribution of the photograph as injunctive relief.

10.5 Class actions

Not applicable.

10.6 Liability

Individuals can claim damages before the general courts. The precedents in general capture the privacy of communication and private life.

In one instance of the Supreme Court for the 4th Circuit (2009/8119E, 2010/7573K) dated 23 June 2010, whereby the correspondence between two persons was secretly recorded, the court decided that the audio record was obtained against the law and that secrecy and recording of audio in a secret manner constitutes a violation of personal rights and that the defendant should pay a certain amount of compensation for non-pecuniary damages. However, the amount of compensation was not indicated in the decision.

In another instance, the Supreme Court for the 4th Circuit (2009/14515E,

2011/1353K) dated 16 February 2011, the court granted non-pecuniary damages to the plaintiff, whose private phone conversations were disclosed. There is no information as to the amount of compensation awarded.