The New Personal Data Protection Law in Turkey

- **Resource type: Article**
- **Status: Law stated as at 01-Jul-2016**
- **Jurisdiction: Turkey**

This analysis article gives an overview of the new law on the protection of personal data that has recently entered into force in Turkey. It analyses the most important points under the new law and the many obligations that data controllers must now comply with when dealing with personal data.

This article is part of the Global Guide to data protection. For a full list of contents, please visit *www.practicallaw.com/dataprotection-guide*

Hande Hançar Çelik and Ozan Karaduman, Gün + Partners

Contents

On 7 April 2016, a new law on the protection of personal data has come into force in Turkey, Data Protection Law No. 6698 (Data Protection Law). It is the first law of its kind, regulating the protection of personal data, and also introducing many new obligations that the persons or entities dealing with personal data (data controllers) must comply with.

The Data Protection Law was recently enacted in Turkey, but the Law has been in planning for a long time. The first draft of the Law was prepared in 2003 and a second draft was submitted to the Turkish Parliament in 2008, although the drafts were not enacted. The third and the final draft was prepared and submitted to Parliament in 2015 and enacted in 2016. Until 2016, the protection of personal data, except for certain regulated sectors, was regulated by a single provision in the Turkish Constitution and a few provisions in the Turkish Penal Code. None of those provisions were adequate in responding to the needs of increasingly complex technology and the amount of personal data processed and transferred each day.

A law on the protection of personal data was a step taken towards harmonising the Turkish legislation with EU legislation. The Data Protection Law was prepared based on Directive 95/46/EC on data protection (Data Protection Directive). The Data Protection Law is very similar to the Data Protection Directive, but it is not a complete replica and the differences in the Data Protection Law are deficiencies rather than improvements.

Furthermore the EU has now introduced new legislation on the protection of personal data; Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of such Data, and repealing the Data Protection Directive. As a result, the Data Protection Law is now further away from its EU counterpart, yet still closer than where Turkey would have been had it not introduced a law on the protection of personal data.

Important concepts

One of the most important developments brought about by the Data Protection Law is that it provides official and generally applicable definitions for some of the most important concepts related to the protection of personal data. Those concepts and their definitions are as follows:

- **Personal data.** This is defined as any type of information that relates to an identified or identifiable individual. Before the Data Protection Law was enacted, there was discussion as to whether information related to legal entities can be categorised as personal data. The new definition of personal data put an end to that discussion by stating that only individuals (natural persons) can have personal data.
- **Sensitive personal data.** This is limited to only the types of data as listed in the definition. Sensitive data has been defined as data relating to:
  - race;
  - ethnic origin;
  - political beliefs;
  - philosophical beliefs;
  - religion, denomination or other faiths;
  - clothing and attire;
  - membership of an association, charity or union;
  - health;
  - sexual life;
  - criminal convictions and security measures; and
  - biometric and genetic data.
- **Explicit consent.** This is defined as consent that relates to a specified issue, declared by free will and based on information.
- **Processing of personal data.** This is defined as any type of action made using personal data.
- **Data controller.** This is defined as the real or legal person that determines the objectives and tools of processing of the personal data, and is responsible for the establishment and management of a data recording system.
- **Data processor.** This is the real or legal entity that processes the personal data, with the authority bestowed by the data controller, and in the name of the data controller.

Obtaining consent

The general rule for the processing of personal data and sensitive personal data is that such data can only be processed with the explicit consent of the data subject. Explicit consent has been defined as consent that relates to a specified issue, declared by free will and based on information. The definition provides that not all kinds of consent will suffice under the Data Protection Law. The data subject must know what he is providing consent for, and must clearly express his consent. For example, consent obtained in English from non-English speakers in Turkey would not be considered to be explicit consent.

Exceptions for obtaining consent

Personal data. The Data Protection Law provides that obtaining the consent of the data subject is the main rule with regards to processing personal data. However, certain exceptions have been introduced to this rule. Data can be processed without the explicit consent of the data subject in the following circumstances:

- If clearly proposed under certain laws.
- If necessary for the protection of life or to prevent the physical injury of a person, in cases where that person cannot express consent or whose consent is legally invalid due to physical disabilities.
- If necessary to process personal data that is related to the parties of the contract, provided that it is directly related to the establishment or performance of a contract.
- If required in order for a data controller to fulfill its legal obligations.
- If the data is made manifestly public by the data subject.
- If necessary for the establishment, exercise or protection of certain rights.
- If processing the data is required to satisfy the legitimate interests of the data controller, provided that the fundamental rights and freedoms of the data subject or any related person are not compromised.

Sensitive data. The exceptions related to obtaining consent for the processing of sensitive personal data are more limited and generally permitted if provided for by law (with the exception of health and sexual life). For data related to health and sexual life, the exception to the requirement of consent is that the processing of such data must only be conducted by:

- Persons under the obligation of confidentiality.
- Authorised institutions and establishments for the purposes of protection of public health, protective medicine, medical diagnosis, treatment and care services.

Additionally, the Data Protection Law provides that for the processing of sensitive personal data, "sufficient measures" as determined by the Data Protection Board (Board) must be adopted. However, this additional condition is not currently applicable, as the Board has not yet been established and the additional measures have not been determined. Once the Board has been properly established and the "sufficient measures" determined, necessary systems must be created by data controllers to apply these measures.

Transfer of personal data

The Data Protection Law has regulated the transfer of personal data to third parties and foreign countries. The general rule is that the transfer can only be made if the data subject's explicit consent has been obtained (*see above, Exceptions for obtaining consent*). Certain exceptions apply in relation to consent for the transfer of personal data.

Transfer to a third party. For the transfer of personal data to third parties, if the data to be transferred falls within the explicit consent exceptions, explicit consent will not be sought for the transfer. The Data Protection Law does not provide a definition for a third party, therefore any individual or entity (other than the data controller and the data subject) can be considered a third party. Additionally, the Data Protection Law does not provide any privilege or exception for intra-group transfers of data or transfers of data to outsourcing companies, such as cloud service companies.

Transfer to a foreign country. For the transfer of personal data to foreign countries, if the data to be transferred is included within the exceptions to explicit consent (*see above*) consideration must be given as to whether the destination country has "sufficient protection" in order to conclude the transfer abroad without having obtained explicit consent. Data processed within the framework of such exceptions, can only be transferred if there is sufficient protection in the destination country. If there is no sufficient protection in the destination country, for realisation of the data transfer, the data controller in the foreign country must provide a written commitment, stating that sufficient data protection will be provided and such transfer must be authorised by the Personal Data Protection Board.

The following are subject to this provision:

- Companies that store data in servers abroad.
- Companies that use cloud services abroad.
- Companies sending data to parent companies abroad.

Countries providing sufficient protection will be determined by the Personal Data Protection Board (Board). It is currently not possible to list the countries that provide sufficient protection, because as of the date of the article, the Board is not yet fully established.

Responsibilities of data controllers related to personal data

Obligation to delete, destroy or anonymise the data

If the reason(s) for processing the data are eliminated, related personal data must be deleted, destroyed or anonymised automatically by the data controller or on request by a related person (*Article 7, Data Protection Law*). Therefore, data controllers must use an infrastructure where the reasons for processing data can be monitored and assessed regularly.

Obligation to inform

Under the Data Protection Law, data controllers are obliged to inform the data subject when they process their personal data. Within the framework of this obligation, the data controller must inform the data subject of the:

- Identity of the data controller and its representative (if any).
- Purpose of processing the data.
- Legal grounds for collecting and processing the personal data.
- Method for collecting the personal data.
- Rights provided under Article 11 of the Data Protection Law.

Data controllers who do not fulfill the obligation to inform data subjects can be subject to an administrative fine of between TL5,000 and TL100,000. The obligation to inform will also occur if the personal data is processed within the framework of the exceptions to the explicit consent requirement (*see above*).

Additionally, data controllers must establish necessary communication and monitoring systems for the exercise of rights granted to related persons in accordance with Article 11 of the Data Protection Law. Particularly in relation to whether the data will be processed or not, and requesting the revision or deletion of the data.

Data safety obligations

Data controllers are obliged to adopt all kinds of technical and administrative measures to (*Article 12, Data Protection Law*):

- Prevent the illegal processing of data.
- Prevent unauthorised access to data.

- Provide safekeeping of personal data.

Details of the technical and administrative measures are not yet known, but it is expected that it will be clarified through the regulations to be prepared in accordance with the Data Protection Law.

A data controller that authorises a third party to process personal data will be jointly responsible together with the data processor in relation to the adoption of these administrative and safety measures. If the measures are not adopted, it is anticipated that the data controllers will be liable to an administrative fine of between TL15,000 and TL1 million.

A data controller that is responsible for the processing of data, and allows illegitimate access to that data, must notify the unauthorised access to both the related data subject and the Institution of Protection of Personal Data (Institution) as soon as possible.

Obligations related to complaint applications

Under the Data Protection Law, data subjects can file complaint applications in relation to data controllers. Data subjects will be able to file applications for execution of the provisions of the Data Protection Law. The application must be in writing or in any other means, as to be determined by the Institution, to the data controller (*Article 13, Data Protection Law*).

The Data Protection Law states that these applications must be concluded within a maximum period of 30 days. The applications must be concluded by the data controllers free of charge. If the process does involve a cost, a fee will be charged according to the tariff to be determined by the Institution. Following the assessment of the application by the data controller, the response (whether positive or negative) will be delivered in writing or through electronic medium. If the reason for the application is due to an error by the data controller and if a fee was charged within the framework of the application, it will be returned to the related person.

The execution of Article 13 of the Data Protection Law (which regulates the application process) has been delayed until 7 October 2016, six months after the publication date of the Data Protection Law. Therefore, data controllers will need to have established a method for properly handling the applications, by no later than 7 October 2016.

Data Officers Registry

An obligation to register in the Data Controllers Registry has been introduced for data controllers (*Article 16, Data Protection Law*). The Data Controllers Registry will be a record system, containing:

- Contact details of the data controllers.
- Information concerning the processed data.
- Information about third parties who are due to receive transferred data (within the framework of the data processing procedures and arrangements concerning the safety and storage of the data).

In accordance with the sanction provisions of the law, data controllers that do not fulfill the obligation to register with the Data Controllers Registry and/or who do not provide the required information, will be sentenced to an administrative fine of between TL20, 000 and TL1 million.

However, the provision regarding the Data Controllers Registry has also been delayed until 7 October 2016, which is six months after the publication date of the Data Protection Law. Therefore, data controllers do not currently have to comply with any obligations regarding registry procedures. Additionally, it has been stated that the rules and procedures related to the Data Controllers Registry will be provided in a regulation, and exceptions may be introduced to the obligation to register. Therefore, no action related to the Data Controllers Registry should be taken until the Data Protection Board and the determination of any exceptions to the obligation to register are established.

Conclusion

Turkey is a large country with a population of 78 million and high internet usage. As a result, large amounts of personal data are being processed in Turkey every day. Before the Data Protection Law was enacted, the processing of personal data was regulated by a single provision under the Turkish Constitution and a few provisions under the Turkish Penal Code. This was insufficient and did not

fully respond to the current needs of both data subjects and data controllers in Turkey. The Data Protection Law introduced detailed provisions in an attempt to respond to those needs. There are parts of the Data Protection Law that need improvement and that it is based on the former EU Data Protection Directive, rather than the current EU General Data Protection Regulation. Despite these deficiencies, the introduction of the Data Protection Law is a big development for Turkey and can be viewed as a starting point for future areas of improvement in the country's data protection laws.

Contributor profiles

Hande Hançar Çelik, Partner

Gün + Partners

T +00 90 212 354 00 00
E hande.hancer@gun.av.tr
W www.gun.av.tr

Professional qualifications. Attorney at law, İstanbul Bar Association, 2007

Areas of practice. Life sciences; technology; media; telecommunications.

Recent transactions

- Advising many pharmaceutical companies aligning their operations in compliance with the Data Protection Law.
- Training programmes and presentations with regards to the Data Protection Law for some clients.
- Providing legal assistance with regards to data transfer, security and data interception by local authorities to software and telecommunication companies.
- Providing legal assistance for the implementation of electronic commercial websites of clients, prepared privacy policies, distance sale contracts, informative notices and assisting in the process of order acceptance.
- Advising an online sales website about their project to supply the government with cloud technology along with private enterprises.

Languages. French, English

Professional associations/memberships. International Association of Privacy Professionals (IAPP)

Publications. *"The Bliss of Forgetting – An Analysis of the Right to be Forgotten under Turkish Law Perspective", published on Media Law International.*

Ozan Karaduman, Managing Associate

Gün + Partners

T +00 90 212 354 00 00
E ozan.karaduman@gun.av.tr
W www.gun.av.tr

Professional qualifications. Attorney at law, İstanbul Bar Association, 2008

Areas of practice. Finance; energy; technology; media; telecommunications.

Recent transactions

- Advising many pharmaceutical companies aligning their operations in compliance with the Data Protection Law.
- Training programmes and presentations with regards to the Data Protection Law for some clients.
- Providing legal assistance with regards to data transfer, security and data interception by local authorities to software and telecommunication companies.
- Providing legal assistance for the implementation of electronic commercial websites of clients, prepared privacy policies, distance sale contracts, informative notices and assisting in the process of order acceptance.
- Advising an online sales website about their project to supply the government with cloud technology along with private enterprises.

Languages. French, English

Professional associations/memberships. International Association of Privacy Professionals (IAPP)

Publications. *" The Bliss of Forgetting – An Analysis of the Right to be Forgotten under Turkish Law Perspective" , published on Media Law International.*

Resource information

Resource ID: 4-631-1678

Law stated date: 01-Jul-2016

Products: Data Protection Global Guide, IP&IT, PLC Cross-border, PLC UK Commercial, PLC UK Corporate, PLC UK Employment, PLC UK Financial Services, PLC UK Law Department, PLC UK Public Sector, PLC US Intellectual Property & Technology, PLC US Law Department

Series: Cross-border chapters

Related content

Topics

Cross-border: IP&IT (http://uk.practicallaw.com/topic3-200-1614)

Data Protection (http://uk.practicallaw.com/topic8-103-1271)

Financial Crime (http://uk.practicallaw.com/topic7-103-1182)

Privacy (http://uk.practicallaw.com/topic6-383-8687)