Practical Law™
GLOBAL GUIDE 2018
DATA PROTECTION

The New Personal Data Protection Law in Turkey

Ozan Karaduman, Partner, Gün + Partners

global.practicallaw.com/w-014-3014

On 7 April 2016, a new law on the protection of personal data came into force in Turkey, Data Protection Law 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 persons or entities dealing with personal data (data controllers) must comply with.

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. In comparison to the previous applicable legislation, the Data Protection Law is a modern law aiming to respond to the requirements of the constantly increasing volume of personal data that is collected and processed.

The Data Protection Law is a step towards harmonising the Turkish legislation with EU legislation, and it 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, in relation to the Turkish Data Protection Law, the differences between them may be seen as deficiencies rather than improvements.

Furthermore, the EU has introduced new legislation on the protection of personal data in the form of Regulation (EU) 679/2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation (GDPR)), and is 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.

In 2017, Turkey saw a lot of important activities in terms of personal data:

- The Personal Data Protection Board (Board) was established.
- A number of guidelines were issued in relation to the various concepts set out in the Data Protection Law.
- Three regulations (that is, secondary legislation under Turkish law) were prepared by the Board and came into force in 2017. The regulations issued so far are as follows:
  - Regulation on Data Controllers' Registry;
  - Regulation on Erasure, Destruction and Anonymisation of Personal Data; and
  - Regulation on Working Principles of the Data Protection Board.

This article intends to provide a brief overview of the relatively new legislation on the protection of personal data in Turkey. The obligations discussed apply to both data controllers inside and outside of Turkey when processing the personal data of the residents in Turkey.

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. The concepts and their related 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.

PROCESSING PERSONAL DATA

Processing non-sensitive personal data

The Data Protection Law provides that the general rule for the processing of 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.

After setting out that obtaining consent is the general rule for processing of personal data, the Data Protection Law provides additional legal grounds that allow the data controller to process personal data without the explicit consent of the data subject. This raises doubts as to whether the explicit consent is the preferred legal ground for processing personal data. However, taking into consideration the fact that the Turkish Constitution does not discriminate between explicit consent and any other legal ground for processing personal data, the structure adopted by the Data Protection Law must be accepted.

ADDITIONAL LEGAL GROUNDS THAT DO NOT REQUIRE EXPLICIT CONSENT

Personal data can be processed without the explicit consent of the data subject in the following circumstances:

- If clearly proposed under laws.
- If mandatory 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 for and directly related to the establishment or performance of a contract, and limited with the personal data related to the parties to the contract.
- If mandatory in order for a data controller to fulfil its legal obligations.
- If the data is made manifestly public by the data subject.
- If mandatory for the establishment, exercise or protection of certain rights.
- If processing the data is mandatory for 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.

PROCESSING OF SENSITIVE PERSONAL DATA

All sensitive personal data can only be processed with the explicit consent of the data subject. In terms of additional legal grounds for processing, the Data Protection Law divides sensitive personal data into two categories:

- Personal data on health or sexual life.
- "Other" sensitive personal data.

Personal data related to health or sexual life is protected more strictly than other sensitive data, as the scope of the additional legal grounds for processing is very limited. In addition to the requirement to obtain the explicit consent of the data subject, personal data related to health or sexual data can only be processed by persons under an obligation of confidentiality, or by authorised institutions and establishments, for the purposes of:

- Protection of public health.
- Protective medicine.
- Medical diagnosis.
- Treatment and care services.

For other types of sensitive personal data, these can only be processed if such processing is allowed under Turkish laws.

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

The strict limitations on processing health data can create a problem for many businesses. The Data Protection Law does not recognise the employment requirements as a legal ground for processing health data. This means businesses would be required to either:

- Obtain consent from their employees for the processing of such health data.
- Make amendments to their operation structures (such as including a medical doctor during the processing of health data).

Neither of the above solutions is ideal. Obtaining consent is problematic as the validity of consent in an employment relationship is questionable and consent can be withdrawn at any time. Similarly a business making changes to their operational structure is also problematic as including a third party medical doctor in all of the operations related to healthcare is not always easy.

TRANSFER OF PERSONAL DATA

Transfer to a third party. Sensitive and non-sensitive personal data can be transferred to third parties if the explicit consent of the data subject is obtained or if one of the additional legal grounds mentioned above is applicable for such transfer (see above, Additional legal grounds that do not require consent).

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. This creates a problem, especially in relation to transfers between data controllers and data processors, as there is no explicit provision in relation to data transfers between data controllers and data processors. As a result, any transfer of personal data from a data controller to a data processor must be considered a transfer to a third party. This means that any such transfer would need to be made either:

- With the explicit consent of the data subject.
- Where an additional legal ground exists.

It is possible to think that in most cases, such a transfer would fall under the scope of the legal ground of legitimate interest. However, it is necessary to consider the differences between the Data Protection Directive and the Data Protection Law in this regard. Where the Data Protection Directive uses the expression "necessary" for the legitimate interests, the Data Protection Law uses the expression "mandatory" for legitimate interests. It is clear that the word "mandatory" has a stricter scope than the word "necessary". It is not easy to respond to the question whether a transfer of personal data to a data processor is mandatory. For example, would a company be unable to operate without using a human resources application provided by a third party? It would be able to operate but in a less efficient manner and generally with more costs. The increase in efficiency and the decrease in costs may make such a transfer necessary for that company but it is doubtful that it would make it mandatory. As there is no precedent in this regard, it is not yet clear how the Board will interpret the word mandatory in this context. From a practical point of view, the Board should give a broader meaning to the word than its current use in the Turkish language. This is in order to not frequently block transfers of personal data to data processors. However, it is possible that a broader interpretation may be considered to be contrary to the intentions of the law maker.

Another solution may be found in the interpretation of the definition of "data processor" under the Data Protection Law. As the data processor is an individual or a legal entity processing personal data "on behalf of" the data controller, it can be stated that the data processor is different to an ordinary third party. It acts under the

authority of the data controller, making the data processor a part of the data controllers organisation. As the transfer of personal data between the employees of a data controller cannot be considered a transfer to a third party (although the data controller and each employee is a separate entity), perhaps the transfer to the data processor should not be considered as a transfer to a third party. This is a far reaching interpretation but if the Board adopts a decision in this respect, such an interpretation would get stronger and its chances of holding out against the test of a court would be higher.

Transfer to a foreign country. Sensitive and non-sensitive personal data can be transferred abroad if the explicit consent of the data subject is obtained.

If explicit consent is not obtained, one of the additional legal grounds must apply to the transfer of personal data to the foreign country (see above, Additional legal grounds that do not require explicit consent). Furthermore, the destination country must have "sufficient protection" in order to conclude the transfer abroad without having obtained explicit consent. Data processed within the framework of such additional legal grounds, 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, both:

- The data controller in Turkey and in the foreign country must provide a written commitment, stating that sufficient data protection will be provided.
- The transfer must be authorised by the Personal Data Protection Board.

A list of jurisdictions that provide sufficient protection will be determined by the Board. However, it is currently not possible to list the countries that provide sufficient protection, as this list is yet to be issued by the Board.

RESPONSIBILITIES OF DATA CONTROLLERS RELATED TO PERSONAL DATA

Obligation to erase, destroy or anonymise the data

If the reason(s) for processing the data are eliminated, any 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 establish an infrastructure where the reasons for processing data can be monitored and assessed regularly.

To address this, the Board has issued Regulation on Erasure, Destruction and Anonymisation of Personal Data. Under the Regulation, every data controller must prepare and put into force an internal policy for the erasure, destruction and anonymisation of personal data. This internal policy should create a regular monitoring system of all of the personal data kept by the data controller. The regular monitoring should be made at intervals of six months or less. At each monitoring session, the data controller must determine whether the legal grounds for keeping the personal data still exist. If there is any personal data for which there is no legal ground for keeping, the relevant personal data must be erased, destroyed or anonymised.

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 of data subjects provided under Article 11 of the Data Protection Law (see below).

Data controllers who do not fulfil the obligation to inform data subjects can be subject to an administrative fine of between TRY5,000 and TRY100,000.

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.

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.

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, the data controllers will be liable for an administrative fine of between TRY15,000 and TRY1 million.

In the case of a data breach, the data controller 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 and to compel them to carry out their obligations under 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. 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.

Data Officers Registry

An obligation to register in the Data Controllers Registry has been introduced for data controllers (Article 16, Data Protection Law). However, although the Data Protection Law has introduced this new obligation, the details of how this obligation will be implemented were not clear until the end of 2017. On 30 December 2017, the Board issued a Regulation on Data Controllers' Registry, which provided the details of the obligations that the data controllers must comply with in terms of the Data Controllers' Registry. With this Regulation, it became apparent that the obligation to register with the Data Controllers' Registry was not a simple notification to an online registrar but a set of obligations with a detailed preparation process.

Data inventory. The most important obligation regarding the Data Controllers' Registry is that a data controller must prepare a personal data inventory before registering. The inventory will then be accessible online through the website of the Data Controllers' Registry.

Every data controller must make a thorough review on its activities, determine where it uses personal data in any way and make a list of the following issues for each personal data process:

- The purpose of processing activity.
- The category of the personal data.
- The recipient group.
- The data subject group.
- The maximum retention period.

- Whether or not the personal data is to be transferred abroad.
- The precautions taken for data security.

Contact/representative. The second important obligation related to the Data Controllers' registry is that the data controllers must appoint either a contact person or an authorised representative based on whether the data controller is based inside or outside of Turkey.

The data controllers' residing in Turkey must appoint an individual as a contact person. It is important to note that the Turkish subsidiaries of foreign companies fall under this category, if such subsidiaries process personal data (however minimal their workforce in Turkey is). This individual's name and contact details will be published online and they will be responsible for establishing the communication between the data subjects and the data controllers.

The data controllers residing outside Turkey must appoint a representative. The representative can be either a legal entity or an individual. The appointment of the representative must be made with a resolution of the data controller, which needs to be notarised and apostilled (or otherwise legalised). The representative will act as a point of contact for the data controller in relation to its dealings with the Board, the Data Protection Authority (Authority) and the data subjects.

Data controllers that do not fulfil the obligation to register with the Data Controllers Registry will be sentenced to an administrative fine of between TRY20, 000 and TRY1 million.

RIGHTS OF THE DATA SUBJECTS

Article 11 of the Data Protection Law provides certain rights to data subjects, which data controllers must abide by. A data subject has the following rights:

- To know whether or not their personal data is processed.
- To know how their data is processed.
- To know what the purpose of the processing is, and whether or not the data is being processed in accordance with these purposes.
- To know of any third parties located inside or outside Turkey to whom their personal data is transferred.
- To request the correction of incomplete or inaccurate information.
- To request erasure of their personal data in case the legal ground for processing the relevant personal data does not exist anymore.
- To ensure that their request for the correction and erasure of their personal data are notified to the third parties to whom their personal data has been transferred (see above, Responsibilities of data controllers related to personal data, Obligation to erase, destroy or anonymise the data).
- To object to any negative results produced through a fully automated processing of their personal data.
- To request compensation if they suffer damage due to processing of their personal data that is contrary to the law.

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 still parts of the Data Protection Law that need improvement. Data controllers that are used to the EU legislation on personal data protection will need to pay careful attention to the differences between the EU legislation and the Data Protection Law and the implications that these differences will bear in practice. Data controllers that reside outside of Turkey but process the personal data of Turkish residents must be aware that the obligations of the Data Protection Law will apply to them as well as to the data controllers within Turkey. Despite its 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.

Practical Law **Contributor profiles**

Ozan Karaduman, Partner

Gün + Partners

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

Professional qualifications. Turkey, Lawyer

Areas of practice. Technology, media and telecommunications; corporate and M&A; finance; energy and natural resources.

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, Turkish

Professional associations/memberships. International Bar Association (IBA); International Association of Privacy Professionals Turkey (IAPP), Co-chair of Turkey KnowledgeNet; Galatasaray University Alumni Association, President; Galatasaray Education Foundation, Board Member.

Publications

- *Regulation on Health Data – Stay of Execution, Gün + Partners (Co-Author) 28 September 2017.*
- *The General Data Protection Regulation: Achieving Compliance for EU and non-EU Companies, IBA-Business Law International Vol 18 No 3 (Author) 26 September 2017.*
- *Telecoms and Media 2017, Turkey Chapter, GTDT (Co-Author) 15 September, 2017.*
- *Data Protection & Privacy 2018, Turkey Chapter, GTDT, (Co-Author), 11 September 2017.*
- *Turkey: Draft Regulation on Data Controllers' Registry, Gün + Partners, (Co-Author), 1 June, 2017.*