MOROĞLU ARSEVEN

Multilaw - Global Data Protection Law Guide Turkey 2021

9 Dec 2021

The following law(s) specifically govern personal data / information:

Personal Data Protection Law No. 6698 ("**Law** ") is the main law governing personal data. Other than that, Electronic Communication Law No. 5809, The Law on Regulation of Electronic Commerce No. 6563 ("**eCommerce Law** ") Turkish Law of Obligations No. 6098, Turkish Penal Law No. 5237, Health Services Fundamental Law 3359 and their secondary legislation are some other laws that contain specific provisions for governance of personal data.

Key secondary legislation guiding the implementation of the DP Law can be outlined as follows:

28 October 2017: Regulation on Erasure, Destruction or Anonymization of Personal Data (entered into force on 1 January 2018)

30 December 2017: Regulation on the Data Controllers Registry (Amendment to the Regulation on the Data Controller Registry has been published in the Official Gazette on 28 April 2019)

16 November 2017: Regulation on Working Procedures and Principles of the Personal Data Protection Board

9 February 2018: Regulation on Personal Data Protection Expertise

26 April 2018: Regulation on Organization of the Personal Data Protection Authority

5 May 2018: Regulation on Promoting and Change of Title of the Data Protection Authority Personnel

17 May 2019: Regulation on Disciplinary Supervisors of Personal Data Protection Authority

21 June 2019: Regulation on Personal Health Data

10 March 2018: Communiqué on Principles and Procedures for Application to Data Controller

10 March 2018: Communiqué on Procedures and Principles Regarding the Data Controller's Obligation to Inform Data Subjects.

The key data protection principles in this jurisdiction are:

The following key principles need to be followed in all personal data processing activities (Article 4 of the DP Law) performed by data controllers. Personal data must be:

- Processed lawfully and fairly.

- Accurate and, where necessary, kept up to date.
- Processed for specified, explicit, and legitimate purposes.
- Relevant, limited, and proportionate to the purposes for which they are processed.
- Retained for the period determined by relevant legislation, or as deemed necessary for the purpose of the data processing

The supervisory authority / regulator in charge of data protection is:

In order to ensure proper implementation of the data protection rules, the Personal Data Protection Authority ("Authority") was established as an independent regulatory authority, with organisational and financial autonomy, charged with ensuring fulfilment by market players of all provisions of the DP Law. The Authority is composed of the Personal Data Protection Board ("Board") and the Presidency.

The Board is the Authority's decision making body, consisting of nine members, five of which are appointed by the Grand National Assembly of Turkey, and the remaining four by the President of the Republic. The Board has been active in Turkey since January 2017.

Is there a requirement to register with a supervisory authority / regulator?

In principle, all data controllers are required to register with Data Controllers Registry System ("VERBİS") before processing personal data (see, Article 16 of the DP Law), however, the Board may, in its discretion, grant exemptions.

In this regard, the Board issued decisions granting exemptions from the VERBIS registration requirement to certain professional groups, associations, and political parties. The Board has also granted a general exemption to local data controllers whose:

- Annual number of employees is less than 50, OR
- Annual balance is less than TRY 25 million.

A local data controller with employees or revenue in excess of the foregoing must register with VERBİS unless they fall within another exception, or an exception is granted by the Board on other grounds.

Notably, overseas data controllers processing data from Turkey must register with VERBİS without exception.

Is it possible to register with / notify the supervisory authority / regulator online?

Registration to VERBİS can be carried out online through the official VERBİS website.

DP Law requires all local data controllers exceeding the thresholds to register with the VERBİS which is an online registration system where data controllers shall record their data processing activities. The thresholds are as follows:

- more than 50 employees;
- total annual balance sheet of more than TL 25 million; OR
- overseas data controllers processing Turkey originated data (regardless of their balance sheet amount or employee number).

Below is an outline of the steps for the registration with VERBİS for overseas data controllers:

1. Creating VERBİS User Account

For creating the VERBİS user account, the application form on VERBİS must be completed and sent to the Board's attention. Then the account name and password will be sent to the data controller's e-mail address, which is the corporate e-mail address notified to the Board during the creation of the application form.

1. Appointment of a Contact Person

The data controllers are obliged to appoint a contact person responsible for communication with the Board. The relevant contact person will be notified to VERBİS and notifications about VERBİS will be made by the data controller through the e-government account of the appointed contact person.

The contact person will then submit the data inventory, as explained below, and complete registration with VERBİS.

1. Preparation of a data inventory for the personal data processed in Turkey

Data controllers must prepare a data inventory and upload it to VERBİS. Please note that since the registration scope will be limited to the processing channels including Turkey originated data; the data controller will only prepare a data inventory for such processes.

It should be kept in mind that data the registration process for overseas data controllers is more complex as it requires the appointment of both a data controller representative (Turkish legal entity or natural person) and contact person (Turkish natural person).

The data controller representative will then complete the VERBİS application form and appoint a contact person. All data controllers must inform a contact person to VERBİS. The contact person needs to be a Turkish citizen and a person can only be appointed as the contact person for one legal entity.

Is there a requirement to notify the supervisory authority / regulator?

The requirement to notify the Board applies for data breaches. Please see the answer of the **"Does this jurisdiction have any specific data breach notification requirements?" question** below for more detailed information.

The key data subject rights under the data protection laws of this jurisdiction are:

As per Article 11 of the DP Law, data subjects are entitled to request the following from data controllers:

- information about whether their personal data has been processed;
- if their personal data has been processed including information about such data and processing;
- information about the purpose of the data processing and whether the data was used for that purpose;
- information about the identities of the natural or legal persons to whom the data was transferred;

- correction, erasure, or removal of the personal data;
- that the data controller advises the recipient about correction, erasure, or removal of the personal data if data is transferred;
- there is no negative consequence of their data being analyzed exclusively through automated systems; and
- compensation where a data subject suffers any damage due to the illegal processing of their data.

Is there a requirement to appoint a data protection officer (or equivalent)?

No. However, as explained above, data controllers must appoint a contact person to carry out the correspondences with the Board; but the scope of the authority of the contact person is limited with communication with the Board.

Do data protection/ privacy impact assessments need to be carried out in certain circumstances?

No specific data protection/privacy impact assessment is regulated under Turkish law, however, data controllers are obliged to assess the impact of the data processing or data transfer each time they process or transfer personal data.

Does this jurisdiction have any specific data breach notification requirements?

Yes, data breaches must be notified to the Board. No statutory details have been provided for the data breach notification process; however, the Board determined the required procedures applicable to breach notification in its decision dated 24 January 2019, (2019/10). The requirements can be summarized as follows:

- Data controllers shall notify the Board within seventy-two (72) hours, at the latest, from the date he/she learns of a breach, and shall promptly notify the data subject(s) affected by the breach using appropriate methods after identifying;
- If the data controller cannot, with good cause, notify the Board within seventy-two (72) hours, it must notify the Board and also state the reasons for the breach;
- Data breach notifications must be made through the standard form (Data Breach Notification Form) announced by the Board;
- If all of the information requested in the Data Breach Notification Form cannot be provided by the data controller as specified, it can provide the information to the Board in phases, without delay;
- The data controller must record the information, effects, and measures taken in relation to the data breach, and, if requested, make this available for the Board's review.
- If a data breach occurred in the processing activities of a data processor, the data processor must notify the data controller(s) immediately that data breaches have occurred within their organisation;
- In case a data breach occurs within an overseas data controller, it must notify the Board if the breach meets the following conditions: (i) the consequences of the breach affect data subjects residing in Turkey, and (ii) data subjects in Turkey benefit from the products and services provided by the data controller; and
- Data controllers are obliged to prepare a formal data breach response plan and review it periodically. This plan should include information including who a data breach should be reported to within the organisation, who will be held accountable after an assessment of the potential consequences, and who will be charged with providing notice of the breach in accordance with the DP Law.

The following restrictions apply to the international transfer of personal data / information:

Yes. As per Article 9 of the DP Law, cross border data transfers shall be based upon one of the following legal grounds:

- the data subject has given his/her explicit consent, OR
- the crossborder transfer is based on grounds set forth in the DP Law, including:

-The receiving country must be determined by the Board to be safe and to provide adequate data protection; OR

-If the level of data security is not adequate, then the data transferor in Turkey and the data receiver overseas (data controller or processor) must execute a written letter of undertaking (containing the minimum which has been determined by the Board), and then seek the Board's approval to perform the data transfer.

The Board has not yet published a comprehensive list of countries providing adequate data protection. It is therefore sensible to consider all countries outside of Turkey as countries without adequate protection for data transfers. Currently, there are two statutory ways for a data controller to transfer personal data overseas:

1. obtaining explicit consent of the data subject; OR
2. approval of the Board upon a written undertaking executed by the data transferor and data receiver. The Board published standard terms for data transfers on it's website, including the requirement that a written undertaking executed by the data transferor and the data transferee must, at a minimum, recite standard terms. These standard terms are essential clauses that must be included in agreements for transferring personal data to countries without an adequate level of protection and include separate provisions for transfers to data controllers and data processors. The minimum content required by the Board is similar to the European Union Standard Contractual Clauses.

When granting permissions, the Board must evaluate international treaties, reciprocity of countries, measures taken by the data controller as well as the period and purpose of the data processing. This requirement is particularly relevant, both for multinationals and local companies with cross border operations, or data servers maintained outside of Turkey. The Board can limit cross border data transfers if they determine the transfer to be against the public interest or personal interests. It is not yet clear how the Board will determine violations.

Do the data protection laws in this jurisdiction have "extra-territorial effect" (i.e. do they apply to organisations outside this jurisdiction)?

Unlike the General Data Protection Regulation of the European Union ("GDPR")., the DP Law does not have a territorial scope. However, in line with the principle of territoriality applicable under the Turkish Law, the DP Law shall apply to all natural and legal persons who process Turkish originated data, regardless of whether they are located in Turkey or overseas.

The following rules specifically deal with marketing:

As per e-Commerce Law, personal data collected from a data subject can only be used and shared with third parties with the data subject's consent. Therefore, customer consent must be obtained to use personal data for marketing purposes, such as online mailing or online behavioural advertising as well as other electronic

commercial communication. Also, the receiver's consent is required for sending electronic commercial messages. Please see answer of **"Does your jurisdiction have any rules specially dealing with electronic marketing (for example, by email, text, WhatsApp message, online ads etc)?"question** below for more detailed information regarding commercial electronic messages.

Do different rules apply to business-to-business and business-to-consumer marketing?

Yes, no prior consent is required for sending electronic commercial messages to merchants; however, if they choose to opt-out, no commercial electronic messages can be sent until they opt-in. However, with respect to personal data, there is no distinction between business-to-business and business-to-consumer marketing.

Does your jurisdiction have any rules specially dealing with electronic marketing (for example, by email, text, WhatsApp message, online ads etc?

Yes. The electronic commercial communication has been regulated under the Regulation on Commercial Electronic Communication ("e-Communication Regulation"), published in the Official Gazette numbered 29417 on 15 July 2015.

As per e-Communication Regulation, the receiver's consent is required for sending electronic commercial messages.

The Regulation Amending the Regulation on Commercial Communication and Electronic Commercial Messages sets forth the establishment of a central and singular platform, with the purpose of conducting transactions that involve obtaining prior consent from recipients in order to send electronic commercial messages. On 4 January 2020, the Official Gazette (30998) published information on the recipient's right of rejection and complaint procedures.

The Commercial Electronic Messages Management System ("**MMS** ") Registry was established to conduct transactions that involve obtaining prior consent from recipients in order to send electronic commercial messages. The right of rejection by the recipient and complaint procedures are mandatory for the real or legal persons aiming to send commercial messages. Electronic messages cannot be sent to the recipients whose approval are not on the MMS.

The following rules specifically deal with cookies:

No specific rules apply to cookies. General rules for marketing and data protection apply.

The consequences of non compliance with data protections laws (including marketing laws) are:

Non-compliance with certain DP Law requirements will trigger administrative sanctions (see. Article 18 of the DP Law). Accordingly, for:

- Violation of the obligation to inform will be imposed with an administrative fine between TRY 9.384,00 - TRY 196.689,00;
- Violation of the obligation with data security will be imposed with an administrative fine between TRY 29.503,00 - TRY 1.966.862,00;
- Violation of the compliance with the Board's decision will be imposed with an administrative fine between TRY 49.172,00 - TRY 1.966.862,00; OR
- Violation of the registration obligation to VERBİS will be imposed with an administrative fine between TRY 39.337,00 - TRY 1.966.862,00.

Also, Under Turkish Criminal Law:

- Unlawful recording of personal data is punishable by imprisonment for 1 to 3 years. If the personal data unlawfully recorded relates to race, ethnic origin, political and philosophical views, sexual orientation, health or tradeunion membership is punishable by imprisonment for up to 4 to5 years.
- Illegally obtaining, transferring, and disseminating personal data is punishable by imprisonment for 2 to 4 years. However, if committed (i) by a public official in misuse of power, or (ii) by an individual misusing benefits or privileges of a profession or trade, then it is punishable by up to 6 years imprisonment.
- Failure to destroy personal data after expiration of the applicable statutory retention period is punishable by imprisonment for 1 to 2 years. However, where such failure is due to the nature of the data, within the purview of Turkish criminal law, then it is punishable by up to 4 years imprisonment.

Sending unsolicited commercial messages requires an administrative fine between TRY 2,071 to TRY 10,381. However, the fine can be increased up to 10 times if the messages are sent to multiple receivers.

In broad terms, multinational organisations should be aware of the following key factors if they process personal data / information from individuals within this jurisdiction, without being located there:

The knot of cross border data transfer has yet to be untied. Currently, as the board have not yet declared the list of countries with adequate protection, an undertaking is the only way for the transfer of personal data of data subjects who do not provide their explicit consent. However, only 4 undertakings have been approved by the Board so far. Therefore, explicit consent is the most favoured tool for cross border data transfers. However, as the consent must be based free will, it cannot be compulsory. Therefore, an alternative way must be presented to data subjects who do not consent to a cross border data transfer.

Multinational organisations should be aware of the following upcoming data protection developments:

In the near future, the Turkish Parliament is expected to take a step to align the DP Law with the GDPR. This intention has already been clearly addressed in the 11th Development Plan of Turkey for 2019-2023. In the Human Rights Action Plan, published in April 2021, the timeline prediction for the alignment was one year. Therefore, the Turkish DP Law is expected to be amended to align with the GDPR. This should also resolve the cross border transfer issue with an aligned law with the GDPR, which allows standard contractual clauses and the method of notification.

**The content was originally published in Multilaw's website*

Related Practices

- Privacy and Data Protection

Related Attorneys

- BURCU TUZCU ERSİN, LL.M.
- BURCU GÜRAY