TURUNÇ

15 April 2016

TURKISH DATA PROTECTION LAW ENTERS INTO FORCE

Many years in the making, the Turkish Data Protection Law (*Kişisel Verilerin Korunması Hakkında Kanun*), Law No. 6698 (the **"Data Protection Law"** or the **"Law"**), Turkey's first data protection and privacy law, was passed by the Turkish parliament on 24 March 2016 and published in the Official Gazette on 7 April 2016.[1]

The aim of the Data Protection Law is to safeguard the fundamental rights and freedoms of individuals, in particular their right to privacy, with respect to the processing of their personal data. Accordingly, the Law sets forth the principles that apply to the processing, use and transfer of personal data. Any legal or natural person who processes the personal data of others in whole or in part by automatic means, or non-automatic means which form part of a data recording/filing system, are subject to these principles.

Under the Law, the processing of personal data includes a wide range of actions including the collection, recording, storage, alteration, reorganization, disclosure, transfer, classification, and restriction of the use of such data, or making such data retrievable.

1. Basis and Origins of the Law

The Law enacts Turkey's undertakings under the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of the Council of Europe (Convention 108), which Turkey signed on 28 January 1981 and ratified on 30 January 2016. In terms of drafting and specific provisions, the Law is modeled after the Data Protection Directive (95/46/EC) (the **"Directive"**) with certain differences.[2]

2. General Principles Relating to the Processing of Personal Data

Under the Data Protection Law, personal data must:

- be processed lawfully and fairly;
- be accurate and, where necessary, kept up to date;
- be collected for specified, explicit and legitimate purposes; and
- not be excessive in relation to the purposes for which they are collected.

Furthermore, such data must be kept no longer than is necessary for the purpose for which they were collected or processed.

[1] Certain provisions of the Data Protection Law entered into force as of the Law's publication date while others will enter into force six months from the date of publication.

[2] For example, a person's clothing (choices/habits) is considered personal data under the Law (but not the Directive), presumably because it may reflect or be indicative of other protected data such as religious beliefs.

Processing of the personal data requires the explicit[3] consent of the data subject. Having said that, such consent will not be required if:

- the processing is permitted by law;
- the processing is necessary to protect the life or bodily integrity of a person who is unable to give consent due to actual impossibility or whose consent is not legally recognized, or the life or bodily integrity of another person;
- the processing is necessary for the formation or performance of a legal contract to which the data subject is party;
- the processing is necessary in order to comply with a legal obligation to which the data controller is subject;
- the data have been made public by the data subject;
- the processing is necessary in order to establish, use or protect a legal right; or
- the processing is necessary for the purposes of legitimate interests pursued by the controller; *provided* that fundamental rights and freedoms of the data subject are not harmed.

Under the Law, personal data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, clothing choices/habits, trade-union membership, health or sex life, criminal conviction and security measures, biometric or genetic information are defined as sensitive personal data. These categories of data cannot be processed without the consent of the data subject except where required by applicable law.

Any personal data processed prior to the publication of the Law must be made compliant with the Law within two years of the publication. Furthermore, any personal data in violation of the Law must immediately be deleted or anonymized. Having said that, any consent received legally prior to the publication of the Law will be deemed to have been obtained properly under the Law unless the data subject retracts such consent within a year of the publication of the Law.

The Law has also established a new independent public authority called the Personal Data Protection Authority (the **"Authority"**), which is tasked with supervision and enforcement of the Law.

3. Transfer of Personal Data

The Law prohibits the transfer the personal data to third parties in Turkey or abroad without the consent of the data subject. Having said that, transfer without consent is permitted pursuant to certain exceptions (including as described above). Furthermore, the transfer of personal data abroad is permitted without explicit consent if the relevant foreign jurisdiction:

- provides adequate protection[4]; or

[3] "Unambiguous" under the Directive.
[4] The Authority has the power to determine the list of jurisdictions with adequate protection based on the principles set forth in the Law.

- in the absence of adequate protection, with the permission of the Authority; *provided* that the relevant domestic and foreign data controllers undertake in writing to accord adequate protection.

Notwithstanding the foregoing and without prejudice to international treaty obligations, personal data may be transferred abroad only with the permission of the Authority in consultation with any other relevant institutions if such transfer will materially damage national interests or the interests of the data subject.

4. Rights of the Data Subject

Data controllers have the responsibility to comply with the provisions of the Law. Data subjects, on the other hand, have the right to apply to data controllers in order to (a) obtain information on whether and how their personal data are being processed, (b) correct or destroy any incomplete or inaccurately processed data, and (c) object to the results obtained by analyzing the processed data.

Misdemeanor violations of the Law are subject to administrative fines ranging from TRY 5,000 to TRY 1,000,000 (approx. EUR 1,500 to EUR 310,000). Certain provisions of the Turkish Criminal Code also apply to some violations of the Data Protection Law.

Ms. Esin Çamlıbel (ecamlibel@turunc.av.tr) would be happy to answer any questions you have about the Data Protection Law.