KOLCUOĞLU DEMİRKAN KOÇAKLI
HUKUK BÜROSU • ATTORNEYS AT LAW

TURKISH LAW BULLETIN April 2016

New Era in Protection Of Personal Data

As information systems and technological developments continue to prevail, almost every operation in modern daily life is carried out electronically. As a result, individuals, companies and governmental authorities can now easily access personal data. Although this may sometimes seem like an advantage, one must consider that, as more and more information is gathered electronically, the abuse of personal data becomes more likely, and the risk of collecting an individual's personal data without his or her consent increases significantly.

1- Legislation on Data Protection

In Turkey, work on personal data protection actually began in the 1980s. Initially, "The Principles for Protection of Personal Space and Cross Border Personal Data Traffic" were accepted in Turkey on 23 September 1980. Later on, Article 10 of Turkish Constitution was amended by a referendum on 12 September 2010. With this amendment, protection of personal data was secured as a fundamental right in the country. The same article also anticipated the drafting and entry into force of a special law governing data protection.

Apart from the Constitution, the protection, processing and storage of personal data are dealt with under various national laws, such as the Labor Law, the Turkish Code of Obligations, the Turkish Penal Code, and the Law on Electronic Commerce. However, in practice, the absence of an overarching framework law and supervisory institution to oversee the application of legislation has caused numerous problems.

Turkey signed the European Council's "Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data" (the "**Convention**"), which regulates the protection and transmission of personal data, on 28 January 1981. However, the approval procedures required for the Convention to enter into force in Turkey were not completed until very recently. The Law on Approval of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data No. 6669 was published in the Official Gazette on 17 March 2016, and the Convention finally entered into force in Turkey.

Thanks to this progress, the Grand National Assembly of Turkey has been able to speed up enactment of the Law on Protection of Personal Data[1] (the "**Law**"), which (i) governs the details of protection, processing and storage of personal data, and (ii) establishes a supervisory body to inspect the application of the law. The Law was finally published in the Official Gazette on 7 April 2016.

According to the Law, the provisions regarding (i) transmission of personal data to third persons and foreign countries; (ii) the rights of the data owner; (iii) the complaint mechanism; and (iv) criminal acts and actions giving rise to liability will enter into force six months after the publication date of the Law. The remaining provisions will enter into force on the publication date.

[1] Numbered 6698, published in the Official Gazette dated 7 April 2016 numbered 29677.

The personal data which were processed before the publication date of the Law must be synchronized with the Law within two years from the publication date. Otherwise, the related personal data must be deleted, destroyed or anonymized. However, if the consent is provided from the related personal data owner with legal grounds and the related personal data owner does not make any statements on the contrary, this consent will be deemed in accordance with the law.

The Law stipulates establishment of a "Data Protection Institution" (the "**Institution**") in Ankara, responsible for (among other duties) researching, investigating and making recommendations regarding personal data processing. The Institution is directly related to the Prime Ministry, and consists of (i) the Data Protection Board (the "**Board**") and (ii) a president.

2- Processing and Transmission of Personal Data

Both under the Convention and the Law, "personal data" is defined as any type of information related to an individual whose identity is identified or identifiable. However, personal data is not limited to information providing definite identification information, such as name, surname, date of birth and birthplace. As explained under the preamble of the Law, data concerning physical, familial, economic, social and other features of an individual is also classified as "personal data".

The term "processing of personal data" includes operations such as acquisition, recording, storage, maintenance, alteration, reorganization, explanation, transmission, transfer, classification or bringing into or prevention of use of data, wholly or partially, within a data record system[2], either through automated or non-automated means.

Both the Law and the Convention stipulate common principles on protection and processing of personal data. Accordingly, personal data should be processed: (i) in accordance with the law, (ii) in good faith, (iii) for definite, clear and legitimate purposes, and (iv) in an appropriate and measured manner. The processing should be carried out accurately and should be up-to-date. Personal data must also be stored only for the statutorily permissible period of time (as determined under the applicable legislation), and for a proper purpose.

As per the Law and the Convention, personal data cannot be processed without the explicit consent of the related individual. Personal data may only be processed without explicit consent under certain circumstances stipulated under the Law.

According to the Law, data regarding an individual's race, ethnic origin, philosophical beliefs, religion, sect, other beliefs, clothing, membership in any association, foundation or union, health, sex life, criminal history, and security and biometric and genetic data are classified as "special category personal data". Processing this type of data without the relevant individual's explicit consent is prohibited. Furthermore, according to the Convention, this type of data cannot be subject to automatic processing.

Any personal data processed in accordance with the Law must be deleted, destroyed or anonymized automatically or upon the relevant individual's request, if the original grounds for processing cease to exist. The Law states that details of these precautionary requirements will be laid out in a regulation. As the date of our bulletin, such regulation has not yet been presented to the public's attention.

[2] Within the scope of the Law, the data record system means a record system where the personal data is processed by way of structuring in line with specific criteria.

3- Transmission of Personal Data to Foreign Countries

Personal data cannot be transmitted to foreign countries without the explicit consent of the relevant individual. However, if any of the exceptions brought by the law exist and adequate protection is provided in the foreign country, to which the data will be transferred, the relevant individual's explicit consent is not required. A list of the foreign countries which have adequate levels of data protection will be announced by the Board.

4- The Data Responsible

Under the Law, the "data responsible" is an individual or a legal entity that determines the purposes and means of processing personal data. The data responsible is responsible for establishment and administration of the data recording system. As per Article 18 of the Law, if the data responsible does not fulfill his/her obligations under the Law (i.e., preventing unlawful processing of personal data), he/she will be subject to an administrative fine of TRY 15,000 to TRY 1,000,000.

The data responsible must be registered with the Data Responsible Registry, which will be made available to the public by the presidency (under the supervision of the Board). As per Article 18 of the Law, if the data responsible does not register with the Data Responsible Registry, he/she will be subject to an administrative fine of TRY 20,000 to TRY 1,000,000.

The relevant person is entitled to submit his/her requests to the data responsible in writing or by other means determined by the Board. The data responsible is obligated to carry out these requests free of charge as soon as possible and in any case, within thirty days. If the data responsible rejects the request, he/she is obligated to submit the grounds for rejection in writing or electronically.

5- Data Protection Board

The Board is the Institution's decision-making body. The Board's main function is to ensure that personal data processing occurs in accordance with the fundamental rights and freedoms of the individual.

The Board consists of seven members (four members selected by the cabinet and three members selected by the President). The Board exercises its duties and powers independently and autonomously. When carrying out its duties, the Board will not consider any order, instruction, recommendation or suggestion from any organ, office, authority or person.

6- Sanctions

The penalties regarding personal data are regulated under the "Crimes" and "Faults" sections of the Law. Accordingly, the provisions of the Turkish Penal Code will be applied to the persons or entities committed the crimes relating to personal data; also administrative fine will be applied to the persons and entities breaching the obligations stipulated under the Law. However, as mentioned in the first section of our bulletin, the provisions relating to crimes and faults will be entered into force six months after the publication date of the Law.

Pınar Bülent (pbulent@kolcuoglu.av.tr) & Melis Özenbaş (mozenbas@kolcuoglu.av.tr)