Turkish Data Protection Law

Further to its accession negotiations with the European Union (the "EU"), Turkey is currently in the process of aligning its legislation with the EU acquis communitairé, to meet the accession criteria, including data protection legislation.

Although data protection rules did previously exist under the Turkish Criminal Code (No.5837), more extensive and comprehensive regulations are seen necessary to ensure the adequate protection of the personal data in line with European standards.

After lengthy discussions on the draft data protection law for nearly two years, Turkey finally enacted the Law on the Protection of Personal Data (No. 6698) (the "Law") on 7 April 2016, in accordance with the EU Directive 95/46/EC (the "Directive"). The Regulation regarding the Processing of Personal Health Data and the Protection of Privacy (the "Health Data Regulation") also been enacted recently.

This briefing provides an overview of the: (i) definition of personal and sensitive personal data; (ii) legitimate processing; (iii) right to be forgotten; (iv) rules on transparency; (v) transfer of personal data; (vi) supervisory board's role and (vii) sanctions.

Personal Data and Sensitive Personal Data

The Law introduced separate definitions for personal and sensitive personal data. Personal data is defined as any information regarding an individual (not a legal entity) who is identified or identifiable. Accordingly, any information that may be able to be associated with an individual is likely to be treated as personal data, and might fall within the scope of the Law.

Sensitive personal data is defined as a subset of personal data about an individual's race, ethnical origin, political ideology, philosophical believes, religion, sect or other beliefs, appearance, membership to an association, foundation or trade union, health, sexual life, criminal convictions, information regarding other security measures and biometrical and genetic data.

Although the general principles on restriction of personal and sensitive data processing are similar, there are differences in areas such as the conditions for the legitimate processing of data (*i.e.* processing data regarding health and sexual life).

Legitimate Processing

General Principles

The Law sets out the general principles applicable to personal and sensitive data processing. Any kind of personal and sensitive data processing must be: **(i)** in compliance with the law and good faith; **(ii)** accurate and up to date when necessary; **(iii)** must have a specific, clear and legitimate purpose; **(iv)** limited, moderate and relevant with the purpose; and **(v)** preserved for the time necessary for the purpose and required under the relevant legislation.

Personal Data

The approach set out under the Law is in parallel with the approach under the Directive. Subject to certain carve outs primary rule is that personal data cannot be processed without the express consent of the respective individual. However, personal data can be processed without the express consent of the respective individual, if;

(i) it is expressly permitted under the laws;

(ii) it is imperative for protecting the life or physical integrity of the subject or another person where the data subject is physically or legally incapable of providing its consent;

(iii) it is necessary to process data of the parties to a contract, provided that such processing is directly related to the execution or performance of the contract;

(iv) it is imperative for the data controller[1] to fulfil its legal obligations;

(v) the relevant data has been publicised by the individuals themselves;

(vi) it is imperative for the establishment, usage or protection of a right;

(vii) it is imperative for the legitimate interests of the data controller, provided that such processing does not violate the fundamental rights and freedoms of the individuals.

Sensitive Personal Data and the Health Data Regulation

The Law further prohibits sensitive personal data processing without the express consent of the individual. However, the Law makes a distinction between the data concerning the health or sexual life of an individual and other sensitive personal data.

Accordingly, sensitive personal data other than the data concerning health and sexual life can be processed if it is permitted by law. Sensitive personal data concerning health or sexual life, can only be processed, by the people who are under confidentiality obligation or by the authorised institutions, for the purposes of: **(i)** protection of public health; **(ii)** execution of preventive medicine, medical diagnosis, treatment and care services; **(iii)** planning and management of healthcare services and finance.

The Health Data Regulation restates and expands the exceptions to the prohibition of processing and transferring personal health data. The regulation underlines that, individuals who are subject to processing must be informed in detail and must give explicit written consent for processing personal health data in a non-anonymous manner for the purposes other than above.

The Health Data Regulation further provides that personal health data may also be published or transferred for the purposes of determining health policies, calculating health expenses, developing health services etc provided that such personal health data is kept anonymous.

The Health Data Regulation further requires the Ministry of Health to establish a central data system in which all the personal health data will be archived for the establishment, execution or protection of rights or for assisting the judicial authorities when required. Access to such data will be prohibited for any other reason.

The Scope of the Law

The Law also sets out further circumstances where the Law will not be applicable and the express consent of the respective individual will not be required for processing their personal data (even for data regarding their health and sexual life). Similarly to the Directive, these circumstances include national, public and economic security, intelligence and protective operations conducted by authorised institutions.

Right to be Forgotten

The Law introduced the right to be forgotten, giving individuals a right to require the data controller to erase, destroy or make the data (that has already been processed) anonymous if grounds for the legitimate processing of such data no longer exist (such as the withdrawal of the express consent that had initially justified the processing).

Where such circumstances exist, the data controller is also under an obligation to erase, destroy and make the data anonymous, irrespective of so individual's request. The Law imposes a censure sanction of up to 4 year imprisonment on data controllers (or data processors that are under this obligation) that fail to comply with the right to be forgotten rules.

Transparency

The Law also introduces provisions to ensure the transparency of the data processing. The data controller (or the individual authorised by the data controller) must inform the individuals about: **(i)** the identity of the data controller and its representative (if any); **(ii)** the purpose of the data processing; **(iii)** to whom and for what purposes the processed data is transferred to; **(iv)** the methods and the legal grounds for the data processing; and **(v)** the individual's rights regarding data process.

[1] Data controller is defined as an individual or legal entity which determines the purposes and means of personal data processing and is responsible for establishing and managing the data registration system.

The individuals are also entitled to request information from the data controller regarding the data processing regarding whether their personal data have been processed, whether they has been transferred to third parties and etc.

Transfer of Personal Data

The Law's approach to the transfer of personal data is similar to the legitimate processing regulations, starting from absolute prohibition without the express consent of the respective individual, then moving on to setting out the circumstances where express consent is not necessary. The circumstances, in which express consent is not necessary, are similar to the grounds for legitimate processing of personal and sensitive personal data, and again reflecting the position under the Directive.

The Law also includes additional conditions for cross-border transfers of personal data. Accordingly even if the circumstances for the transfer of personal data exist, the following rules must be considered before a cross-border data transfer:

(i) whether the recipient country has adequate data protection measures;

(ii) whether the data controller in the recipient country gives a written undertaking to provide adequate data protection (if adequate legal measures do not exist); and

(iii) whether the Board has approved such transfer.

Sanctions

Administrative Sanctions

The persons or authorities who:

(i) do not fulfil transparency obligation will be subject to administrative fine from TRY 5,000 to TRY 100,000;

(ii) do not fulfil data safety obligation will be subject to administrative fine from TRY 15,000 to TRY 1,000,000;

(iii) do not comply with the Board's decisions in respect to the complaints will be subject to administrative fine from TRY 25,000 to TRY 1,000,000; and

(iv) violate the obligations pertaining to data controllers registry will be subject to administrative fine from TRY 20,000 to TRY 1,000,000.

Criminal Sanctions

According to the Law (by reference to the Turkish Criminal Code (Law No. 5237)), persons who:

(i) records personal data illegally will be subject to imprisonment from one to three years;

(ii) who obtains, transfers, circulates personal data illegally will be subject to imprisonment from two to four years; and

(iii) who do not erase, destroy or anonymise personal data after the terms envisaged by the laws have expired will be subject to imprisonment from one to two years.

The Turkish Criminal Code also sets forth aggravating circumstances for the foregoing criminal offences.

The Supervisory Board

The Law established the Personal Data Protection Authority (the "**Authority**") which will act as an independent supervisory body to ensure compliance with the data protection rules that are envisaged in the Law and other secondary legislation. The Authority will act through the Personal Data Protection Board (the "**Board**") as its main decision making body, which will be comprised of 9 independent members appointed by the Turkish Parliament (5 members); the Council of Ministers (2 members); and the President (2 members).

Interim Period

The Law has become fully effective on 7 October 2016.

The Law also requires any type of personal data that has been processed before the Law's effective date to be aligned with the relevant requirements within two years from the Law's effective date and any personal data that has been processed in violation of the Law must promptly be erased, destroyed or made anonymous.

Authors

Itır Çiftçi
Partner
T: +90 212 339 0077
E: itir.ciftci@yeginciftci.av.tr

Kemal Aksel
Counsel
T: +90 212 339 0064
E: kemal.aksel@yeginciftci.av.tr

Aras Görkem
Associate
T: +90 212 339 0062
E:aras.gorkem@yeginciftci.av.tr

Yegin Çiftçi Attorney Partnership, Kanyon Ofis Binasi Kat 10, Büyükdere Cad. No. 185, 34394 Levent, Istanbul, Turkey

Yegin Çiftçi Attorney Partnership is registered with the Istanbul Bar.
Registered office: Kanyon Ofis Binasi Kat 10, Büyükdere Cad. No. 185, 34394 Levent, Istanbul, Turkey