central & eastern europe
legal insights
schönherr

02.05.2016

Turkey: First Personal Data Protection Act in force

Arzu-Sema Cakmak
Associate
T: +43 1 53437 50761
E: a.cakmak@schoenherr.eu

*The long-awaited Personal Data Protection Act no. 6698 (Kişisel Verilerin Korunması Kanunu) (the "**DPA**" or "**Law**") was approved by the Turkish Parliament on 24 March 2016, was published in the Official Gazette on 7 April 2016, and hence came into force. Although various acts include provisions for the protection of personal data (eg the Turkish Code of Obligations, the Turkish Penal Code, the Turkish E-Commerce Act), the DPA is the first comprehensive act regulating data protection in Turkey. The DPA reflects the EU's Data Protection Directive (95/46/EC) ("**Directive**") and thus, Turkey continues adjusting its legislation to EU standards since enacting the Turkish E-Commerce Act on 1 May 2015.*[1]

1. Purpose and scope of the DPA

Pursuant to Art (1) (1) DPA, the object of the Law is (i) to protect the fundamental rights and freedoms of natural persons with respect to the processing of personal data, furthermore it regulates (ii) the liabilities of natural persons and legal entities processing personal data, and the procedures and principles related to same.

The DPA applies to all natural persons whose personal data (defined as any information relating to an identified or identifiable natural person- "**Personal Data**") is processed, and to all natural persons and legal entities processing personal data wholly or partly, whether or not by automatic means ("**Data Subject**"). Pursuant to Art (28) (1) DPA, the Law shall not apply to processing of Personal Data:

- by a natural person in the course of a purely personal or household activity;
- for the purpose of creating scientific research, planning and government statistics, provided that the data is anonymised;
- in the course of processing operations concerning art, history, literature, scientific purposes, and freedom of speech, provided that such processing does not violate national defence, national security, public safety, public order, economic well-being of the country, personal rights or the right to privacy;
- in the interests of national defence, national security, public safety, public order, economic well-being of the country within the scope of preventive, protective and intelligence-related activities by official authorities;
- in the course of activities of judicial authorities in areas of criminal law.

2. Processing and transfer of general data: general principles and criteria

[1] [1] For further information on the Turkish E-Commerce Act please see Schönherr's Roadmap16 http://roadmap2016.schoenherr.eu/new-e-commerce-legislation-in-turkey/

Processing of Personal Data means any operation which is performed upon such data wholly or partly, whether or not by automatic means, such as collection, recording, adaption or alteration, retrieval, storage or transfer to third parties or abroad ("**Processing**").

Schoenherr named Leading Law Firm in Austria and Romania by Chambers

2.1. Processing of Personal Data

Art 4 the DPA sets forth the general principles to be complied with when processing personal data, which must be:

- processed fairly and must be lawful;
- accurate and, where necessary, kept up to date;
- collected for specified, explicit and legitimate purposes;
- adequate, relevant and not excessive in relation to the purposes for which they are processed;
- stored for no longer than is necessary for the purposes for which the data was collected or the time designated by relevant law.

Furthermore, pursuant to Art 5 the key criterion for Processing is the Data Subject's explicit consent, which is defined as any freely given informed and specific consent. However, this provision can be departed from if:

A. it is permitted by any law;

B. it is necessary in order to protect the life and physical integrity of the data subject or another person where the data subject is physically or legally incapable to give its consent;

C. processing is necessary for the performance of a contract to which the data subject is party;

D. processing is necessary for compliance with a legal obligation to which the controller (definition below) is subject;

E. data is revealed by the Data Subject itself;

F. processing is necessary for the institution, usage or protection of a right;

G. processing is necessary for the purposes of legitimate interests of the controller, provided that fundamental rights and freedoms of Data Subjects are not violated.

The processing of special categories of data, which reveals the racial or ethnic origin, political opinions, religious or other beliefs, appearance (which is also categorised as such data in contrast to the Directive), trade-union and other memberships, health and sex life, criminal convictions and biometric or biological data ("**Sensitive Personal Data**"), is subject to stricter rules: It requires not only the Data Subject's explicit consent, but also adequate measures by the supervisory board of the data protection authority in Turkey ("**Authority**"). However, this regulation shall not apply, if (i) processing of Sensitive Personal Data, except concerning health and sexual life, is expressly permitted by any law, and if (ii) processing of Sensitive Personal Data concerning health and sexual life is necessary for the purposes of protection of public health, protective medicine, medical diagnosis, provision of care or treatment or the management of health-care services by an authorised body or persons who are under the obligation of confidentiality.

2.2. Cross-border transfer of Personal Data

Pursuant to Art 9, Personal Data may only be transferred abroad after obtaining a Data Subject's explicit consent. The aforementioned exceptions in relation to processing of such data also apply to transfers outside of Turkey. However, the Law sets forth further safety measures relating to cross-border transfers in accordance with such exceptional cases: The destination country must have any adequate level of protection, which is to be determined by the Authority, otherwise the Data Controller in Turkey and the data importer abroad have to commit in writing to provide an adequate level of protection, which is to be approved by the board of the Authority.

3. Controllers and processors

The DPA distinguishes between controller and processor. Controller ("**Data Controller**") shall mean the natural or legal person which determines the purposes and means of Processing and which implements and manages a personal data filing system. Data processor shall mean a natural or legal person, which processes Personal Data on behalf of the Data Controller. Since data processors are subject to the DPA and thus to Data Controllers' obligations, they must comply with the principles relating to Processing and respectively share responsibility with Data Controllers.

3.1 Data Controllers' obligations

Information to be given to the Data Subject

According to Art 10, the Controller or his representative must provide the Data Subject, from whom related data is collected with the following information:

- the identity of the Data Controller and of his representative, if any;
- the purposes of processing for which the data is intended;
- the recipients of the data;
- the means and legal basis for the data collection.

Consequently Data Subjects have (i) the right to obtain information relating to their personal data (eg whether or not the data relating to them is being processed, and information as to the purposes of processing; rectification, erasure or blocking of personal data etc), (ii) the right to object in cases of decisions which produce effects to the detriment of the Data Subject, and (iii) the right to claim compensation for damages as a result of unlawful processing.

Hence the Data Controller is subject to the obligation to implement appropriate technical and organisational measures necessary for the protection and security of personal data against unlawful processing and unauthorised access.

Obligation to register with the Data Controllers' registry

Prior to the commencement of Processing, Data Controllers must register with the data controllers' registry, unless they can rely on exemptions provided by the Authority.

Sanctions

For breaches of law the DPA imposes administrative fines between TL 5,000 and TL 1,000,000 (approx between EUR 1,500 and EUR 310,000) or imprisonment of one to four years pursuant to the Turkish Penal Code.

4 Transitional provisions

The DPA stipulates a gradual entry into force, thus regulations relating to the transfer of Personal Data, rights of Data Subjects, registry and sanctions will enter into force after six months.