GEDİK & ERAKSOY

November 2016

The Law on Protection of Personal Data has entered into force as of April 2016

The Law on Protection of Personal Data finally entered into force on 7 April 2016, following a lengthy adaptation process, providing Turkey with comprehensive legislation codified under a single law.

Background

As per the consequence of technologic developments and globalization of the world, it has become considerably easy to access and process all kinds of data, where, it has become increasingly harder to protect personal data. Although there were a limited number of provisions regarding personal data protection in place within the Constitution of the Republic of Turkey and other several legislation, those provisions did unfortunately not adequate to provide significant protection for personal data.

Due to rising needs regarding personal data protection and EU harmonization, Turkey has entered into an adaptation process with regards to protection of personal data. It is worth mentioning that EU harmonization has been one of the triggering factors throughout this process. The first step taken by Turkey was accepting the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (the **Convention**) on 18 February 2016. Since Article 4 of the Convention states that "each party shall take necessary measures in its domestic law to give effect to the basic principles for data protection", Turkey needed to enact the Draft Law on Personal Data Protection (**Draft Law**). The Draft Law has been heavily negotiated and worked on at the Parliament level and finally, on 7 April 2016, Turkey's Law on Protection of Personal Data (the **Law**) has entered into force. Note that the provisions relating to local and international transmission of personal data, processes relating to application to the data registry and complaints and personal data crimes and misdemeanours will enter into force following a grace period of 6 months from the general enforcement date (i.e., 7 April 2016) of the Law. The importance of this Law is that this is the first time Turkey has a comprehensive data protection measures provided under a single law.

Law on Protection of Personal Data

The Law is mainly based on EU Directive 95/46/EC (the **Directive**) on the protection of individuals with regard to the processing of personal data and on the free movement of such data, which also attests to the fact that data protection is a global concern and EU harmonization is a major triggering factor. Nevertheless, the Directive and the Law are not identical.

The purpose of this Law is to protect the fundamental rights and freedoms of individuals, primarily the right to privacy in processing personal data and to regulate the obligations of real persons and legal entities that process personal data and the procedures and principals to be followed by the same. Accordingly, the Law provides definitions of fundamental terms, and the scope of basic principles and sanctions for misconduct, including administrative fines, with regard to data protection. All individuals, whose personal data is

processed and all real persons and legal entities that process personal data wholly or partially by automatic medium, or by non- automatic means, provided that the latter is part of a data storage system, are subject to the Law.

Fundamental Terms

The importance of definitions provided under the Law arises from the fact that comprehending the scope of the fundamental definitions is the key to a comprehensive understanding of the subject matter. There are several main terms within the Law, which are worth mentioning. In this regard, the first term is personal data. Personal data is defined under the Law as "any information relating to an identified or identifiable individual". The Law also provides the term "sensitive personal data". In accordance with the Law, sensitive personal data is any personal data regarding race, ethnicity, political views, philosophical beliefs, religion, religious sect or other beliefs, appearance and dressing, foundation or union membership, health, sexual life, penal convictions and security measures as well as biometric and genetic data of a person. On this point, it is noted that while determining the scope of personal data, the Law differs from the Directive by adding "appearance and clothing", "data relating to penal convictions and security measures" and "biometric and genetic data" as categories of sensitive personal data. According to the Law, both sensitive personal data and personal data may only be processed upon the receipt of explicit consent of the data provider. The Law, nevertheless, provides certain exceptions, where the explicit consent of the data provider may not be sought. The term "data processing", is defined as any operation or set of operations fully or partially through automatic medium, or by non- automatic means provided to be a part of any data storage system used for the collection, recording, organization, storage, adaptation or alteration, retrieval, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking the use of the personal data. The Law also stipulates fundamental principles regarding data processing and draws the legal framework of the term.

Fundamental Principles of Data Processing

There are several fundamental principles under the Law regarding data processing, which mainly determine the legal scope and constitute the legal grounds thereof. Main principles of data processing are as follows;

1. The data shall be processed fairly and lawfully; in compliance with legal requirements and good faith,

2. The data shall be accurate and up to date,

3. The data shall be processed for certain, explicit and legitimate purposes,

4. The data processing shall be relevant, limited and measured in line with the processing purposes.

5. Personal data shall be kept for the time stipulated by law or for a period no longer than the processing purpose requires.

Transfer of Personal Data

Transfer of personal data is one of the significant matters within the Law. Transfer of personal data is also linked with EU harmonization process, since the relevant country, to which data is transferred, shall provide competent and adequate protection of personal data according to its legislation. In this regard, by enacting a certain and comprehensive Law, Turkey has taken a step to ease the transfer of data from abroad as well as protecting both the data owner and personal data transmitted. Note that, as per the Law, the provisions regulating transfer of personal data will enter into force on 7 October 2016.

As a general principle, the explicit consent of the data provider must be obtained in order to transfer personal data. However, there are exceptions stipulated by the Law, where the consent of the data provider may not be sought. On this point, the Law makes a distinction between transferring data within Turkey and transferring

data abroad. In order to transfer personal data abroad without obtaining the explicit consent of the data provider, the Law requires, in order to protect personal data and data owner during data transfer, the relevant country to provide adequate personal data protection rules or the officials in the relevant country to undertake the provision of adequate protection regarding the transferred data in writing which must be accepted by the board of protection of personal data, composed under the Law. In light of the above, the Law is intended to satisfy mainly the growing need for the protection of personal data in the age of technology as well as meeting the emerging global standards regarding data protection. The introduction of the Law is a clear step forward in the EU harmonization process and will have resonating effects on personal data processing practices currently in place in Turkey.

*Note: The State of Emergency (**SoE**) Decree on the Precautions to be taken within the scope of SoE numbered 670 which was published in the Official Gazette on 17 August 2016 (the **SoE Decree no.670**) sets out provisions in relation to the protection of personal data. Pursuant to Article 3 of the SoE Decree no. 670, except for the information, which is deemed as customer secret as per the Banking Law numbered 5411, any and all information and documents including communication via telecommunication required by authorized boards, commissions and other authorities pertaining to judicial and public officers against whom an investigation has been initiated as per the SoE Decree no.667 and children and spouses thereof, shall immediately be submitted to the competent authorities.*

*Moreover, as per SoE Decree no.670, any and all information held in (i) Asya Katılım Bankası A.Ş. (**Bank Asya**) operation license of which has been revoked and transferred to Saving Deposit Insurance Fund, (ii) Saving Deposit Insurance Fund relating to Bank Asya, (iii) Banking Regulation and Supervision Agency and (iv) Financial Crimes Investigation Board, pertaining to public officers and their children and spouses shall immediately be submitted to the relevant public authorities where such officers are employed, upon request thereof.*

Gedik & Eraksoy Avukatlık Ortaklığı

Büyükdere Caddesi, River Plaza
Bahar Sokak, No: 13 Kat: 17
Levent, Istanbul
Turkey

Tel +90 212 371 2950
Fax +90 212 371 2955

www.gedikeraksoy.com

Hakkı Gedik
Partner, Gedik & Eraksoy

Contact
Tel +90 212 371 2953
hakki.gedik@gedikeraksoy.com

Gökhan Eraksoy
Partner, Gedik & Eraksoy

Contact
Tel +90 212 371 2952
gokhan.eraksoy@gedikeraksoy.com