Law on Protection of Personal Data is Effective Now: ***Are We Ready?***

07.04.2016

ÇİĞDEMTEKİN·DORA·ARANCI
HUKUK BÜROSU *LAW OFFICE*

Law on Protection of Personal Data is Effective Now: ***Are We Ready?***

Introduction

Law on Protection of Personal Data (the "Law") has come into force following its publication in the Official Gazette of Turkey on 7th of April 2016. The Law sets forth important rules applicable to real persons and legal entities handling personal information.

Please find below a Q&A document, which aims to inform you on the rules adopted by the Law, the penalties and fines for non-compliance with the Law, and the necessary steps towards getting your organization compliant with the Law.

About CDA

CDA Law Firm, provides services to companies active in Technology, Media and Telecommunication sectors for many years. CDA's expertise in these fields has been recognized by prestigious legal directories such as Legal500, Chambers and Partners and Clients' Choice. CDA offers compliance due diligences on personal data regulations, and provides customised solutions for its clients depending on the individual needs and sector requirements. Our team includes Certified Information Privacy Professionals, and experienced lawyers who have a sound capability to deliver large and customized projects.

Please contact us at the below details for more information about CDA and personal data.

Kağan Dora
Managing Partner
kdora@cdahukuk.com
+905323557103
www.linkedin.com/in/kagan-dora-0372707

Background

Turkish Constitution and certain laws, such as Turkish Criminal Code, included certain general rules about personal data and its process before the adoption of the Law.

Also certain sector specific regulations such as Law on Electronic Communications, Banking Law and E-Commerce Law included rules on protection of personal data. However, there was not a detailed framework law governing personal data.

This was deemed necessary for Turkey's EU accession process as well as for operations of Turkish companies which were harmed by the blacklist status of Turkey with respect to personal data protection.

There was also a strong public opinion and pressure as to imposition of a regulation area on personal data due to the developments in the technology, and increased use of internet and e-commerce.

*What is **personal data?***

Any information relating to an identified or identifiable real person is considered personal data under the Law.

Information relating to legal persons are not included in this definition provided that such information does not related to a real person.

Personal data relating to religion, ethnicity, association, foundation and union membership, health and dressing preferences are considered special categories of personal data and process of the these data will be subject to requirements that will be provided by Data Protection Commission.

In addition to the information which in itself is enough to identify a real person (e.g. name-surname, identity number, passport number, IP address, telephone number, photos, video and audio records, fingerprints and e-mail address, information such as a person's hobies, preferances, physical attribitutes, browsing habits) are considered as personal data as well.

*What is **processing of personal data?***

Processing of personal data includes operations such as collection, recording, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction of personal data. This is a definition mirroring the provisions in the Directive 95/46/EC.

*Who falls **under the scope of the Law?***

In general, **any natural or legal person** processing personal data falls within scope of the Law.

*What are **exempt from the scope of the Law?***

Personal data which are processed in relation to activities such as national intelligence, freedom of expression, academic freedom or public security fall outside the scope of certain provisions of the Law. Also personal data that is anonymised falls outside of the scope of the Law, but the process of anonymizing personal data is subject to the rules under the Law. Anonymizing personal data is defined as processing personal data in a way that it could no longer be related to an identifiable person in any manner.

*Who is **Data Controller and Data Processor?***

Data controller is any legal or real person who determines the purposes and means of processing of personal data and is responsible for establishment and management of data registry (e.g. employers in respect to their employees' personal data, websites in respect to the data they obtain from their users).

Data processor is any person processing personal data under the authority granted by and on behalf of the data controller (e.g. Cloud IT service providers, payroll companies). Accordingly with these definitions; it is possible for a company to be both a data controller and a data processor with respect to its different activities.

*What makes **data processing legitimate?***

Personal data may be legitimately processed if:

- explicit consent of the data subject is obtained. Explicit consent requires the data subject to be informed beforehand and the consent should be based on the data subject's free will, and should be unambiguously clear and be limited with the purposes for which it is obtained;
- the personal data is publicized by the data subject
- processing is necessary for compliance with a legal obligation, or is obligatory for performance of a right;
- processing is necessary for the conclusion or performance of a contract, to which the data subject is a party, personal data may be processed only for the purposes relating to such performance;
- processing is necessary for the legitimate interests pursued by the controller unless such interests are overridden by the interests of the data subject with respect to fundamental rights and freedoms;
- the data subject is unable to express his consent; personal data relating to him can only be processed for protecting vital interests of such data subject.

*What other rules **apply to processing?***

Following rules apply to processing of personal data:

- Personal data should be accurate, and, if necessary, up to date.
- Personal data should be kept no longer than is necessary for the purposes it has been collected.
- Processing should be for legitimate and specified purposes in accordance with law and good faith.
- Personal data may be transferred to third parties only upon explicit consent of the data subject, or if the transfer is required by law.
- Personal data may be transferred abroad upon data subject's explicit consent. When the processing is based on other legitimate grounds, the country to where personal data is transferred should be regarded to be safe in protecting personal data, by Personal Data Protection Authority, or the tranferee should be providing adequate safeguards.
- Measures to prevent unlawful access to and processing of personal data should be taken.
- Data subject should be informed on the identity of data controller, purposes and means of processing and conditions under which the personal data may be transferred to third parties.
- Data subject's requests for information on and erasure or rectification of their personal data should be met.
- Data processors and controllers should be register with the Personal Data Protection Authority before they start processing.
- Processing should be compliant with other regulations such as the Banking Law and the Law on Electronic Communications.

As of December 2015, there are 400.000 organizations registered with United Kingdom Information Commisioner's Office.

Çiğdemtekin Dora Arancı Law Office
Akçam Sokak No: 22, 4. Levent, Beşiktaş, Istanbul / Turkey.
T: +90 212 227 00 61 F: +90 212 227 00 63
www.cdahukuk.com

*When will **the Law's provisions come into force?***

7 April 2016	*7 October 2016*	*Within 1 year*	*Within 2 years*
The Law entered into force.	Provisions regarding (i) data transfers to third parties or abroad, (ii) data subjects' right to access and complain, (iii) data controllers' registry and sanctions will become effective.	The secondary legislation envisaged in the Law will be enacted.	Each real person or legal entity that process personal data must become compliant with the Law.

*What sanctions will be **applicable for incompliance with the Law?***

The crimes punishable by imprisonment as listed below are set forth under the Turkish Criminal Code.

The monetary fines provided in the Law as listed below, will become effective on 7 October 2016.

Crime or Offence	*Sanction*
Unlawful recording of personal data	*1 to 3 years of imprisonment*
Unlawful transfer, transmission and collection of personal data	*2 to 4 years of imprisonment*
Failure to destroy the personal data which was required to be destroyed	*1 to 2 years of imprisonment*
Incompliance with the obligation to inform the data subject	*Monetary fine between 5.000 TRY and 100.000 TRY (app. 30.000 EUR) to be issued by Personal Data Protection Authority.*
Not registering with or notifying the data processors registry	*Monetary fine between 20.000 TRY and 1.000.000 TRY (app. 300.000 EUR) to be issued by Personal Data Protection Authority.*
Breach of data security obligations	*Monetary fine between 15.000 TRY and 1.000.000 TRY (app. 300.000 EUR) to be issued by Personal Data Protection Authority.*
Non-compliance with the decisions of Personal Data Protection Board	*Monetary fine between 25.000 TRY and 1.000.000 TRY (app. 300.000 EUR) to be issued by Personal Data Protection Authority.*

*What impact will **the Law have on our business?***

Today personal data has a continuously increasing effect on how we operate our businesses. Considering the value it adds to businesses, it is clear that personal data is a valuable asset for companies especially with regard to its know-how and competitiveness.

With the ever-increasing usage of technology and internet, personal data requires protection and regulation. Also a large number of customer surveys demonstrate that customers are more sensitive about the privacy of the personal data.

For all these reasons, we believe that compliance with data protection should not be considered as a one-time project. Instead, it should be incorporated into the way we think of our businesses and should be conducted as an ongoing process.

Below are a few questions which could constitute a good starting point for a compliance process and which also provide a valuable benchmark to assess the awareness of a business with respect to protection of personal data.

- What personal data do we get?
- From which resources do we collect the personal data?
- Which personal data do we need? For what purposes? Are there any personal data that we do not need but collect anyway?
- How do we categorize those personal data with respect to its collection, storage, use and destruction?
- Are we compliant with the current regulations with respect to such processes?
- How will we be effected with the Law and the future secondary regulations?

For evaluation of the answers to these questions and management of the risks associated with personal data regulations please do not hesitate to contact us.

Çiğdemtekin Dora Arancı Law Office
Akçam Sokak No: 22, 4. Levent, Beşiktaş, Istanbul / Turkey.
T: +90 212 227 00 61 F: +90 212 227 00 63
www.cdahukuk.com