MEMORANDUM ON PERSONAL DATA PROTECTION LAW

July 13, 2016

IŞIKTAÇ & ATABAY
HUKUK BÜROSU

MEMORANDUM ON PERSONAL DATA PROTECTION LAW

1. General

The Personal Data Protection Law numbered 6698 ("the Law") has been accepted at the Turkish Parliament General Assembly on 24 March 2016 and has been enforced on 7 April 2016 upon being published in the Official Gazette numbered 29677.

The provisions on the transfer of personal data to third parties or abroad, the data subject's rights, application and complaint, violations and administrative monetary penalties will be enforced within 6 months following the publication of the Law. The provisions except above specified ones these have been enforced on the same date of the publication date of the Law (i.e. 7 April 2016).

For the personal data that has been processed before the publication of the Law, a transition period of two years (starting from publication date of the Law) has been given for adaptation. Therefore, there exists a time limitation for adaptation (until 7 April 2018) for the personal data that has been processed before 7 April 2016 against provisions of the Law. The consents that have been lawfully obtained before the publication of law will be accepted to be in accordance with the Law provided that no objections have been made within one year. Therefore, the consents that have been lawfully obtained before 7 April 2016 will be accepted to be in accordance with the Law in the event that no objections have been made.

As for the other detailed regulations in Law, it is foreseen that necessary secondary regulations will be published within one year following the publication of the Law.

2. Definition and Processing of Personal Data

2.1 Definition of Personal Data

Personal data has been defined under Article 3 of the Law titled "Definitions" as "any information related to real persons of whom identity is identified or identifiable". According to the legal ground of the Law; name, last name, birth date and place, telephone number, motor vehicle plate, social security number, passport number, resume, photograph, video and voice records, fingerprints, genetic information are accepted as personal data due to the fact that such information enables persons identified or identifiable.

2.2 Processing of Personal Data

Processing of personal data means any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

Article 4 of the Law sets out core principles that need to be applied while processing personal data. Such principles foresee that personal data must be (i) lawful and fair (ii) accurate and, where necessary, kept up to date; (iii) processed for specified, explicit and legitimate purposes (iv) adequate, relevant and not excessive in relation to the purposes for which they are processed; and (v) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data for which they are processed.

Explicit Consent

Article 5 of the Law foresees that for personal data processing explicit consent of the data subject shall be sought. However, there are several exceptional cases where explicit consent is not sought for processing of personal data. Below are such cases:

- it has been explicitly foreseen in the laws
- processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving his consent; or
- processing is necessary provided that it is directly linked to the establishment or execution of a contract
- processing is necessary for the purposes of carrying out the legal obligations of Data Responsible
- the processing relates to data which are manifestly made public by the data subject
- processing is necessary for the purposes of establishment, exercise or defence of a right
- the processing is necessary for the legitimate benefits of the data subject provided that data subject's rights and freedoms are not harmed.

Pursuant to Article 7 of the Law, in the event that the situations where explicit consent is given or the reasons (where explicit consent is not required) that require processing of personal data are eliminated, personal data shall be erased, eliminated or made anonymous. The persons who do not carry out their duty of elimination will be sentenced to prison from one to two years according to Article 138 of Turkish Penalty Code.

The Law brings "qualified personal data" concept. According to Article 6 of the Law; data related to race, ethnical roots, political beliefs, philosophical beliefs, religious beliefs, fashion style, membership of an association, health, sexual life, criminal record, security precautions and biometric data are deemed as qualified personal data. Such data will only be processed with the explicit consent of the data subject. There is a particular situation in the data related to health and sexual life. Such data can only be processed for the purposes of protecting public health, preventive healthcare, medical diagnosis, treatment and care services and planning of financing of health services without seeking explicit consent of the data subject.

3. Data Responsible, Data Processor and Their Liabilities

The concepts of Data Responsible and Data Processor have been set out in the Law. Data Responsible has been defined as the real or legal person who is responsible for the establishment and management of a data registry system before a unit, an institution or a representative. Data Processor shall mean a real or legal person who processes personal data on behalf of the Data Responsible.

Data Responsible or its representative has a duty of informing. The matters for which informing is required have been set out under Article 10 of the Law. According to the said Article, Data Responsible or its representative is obliged to inform the data subjects on below specified subjects:

- the identity of the Data Responsible and its representative if any

- the purpose of processing of personal data
- to whom and for what purpose the transfer of processed personal data can be realized
- the method of collecting personal data and its legal reasoning
- legal rights of the data subject

Pursuant to Article 18 of the Law the violators of informing obligations shall be subject to an administrative fine of minimum 5.000 Turkish Lira up to 100.000 Turkish Lira.

Data Responsible has obligations related to data security as well as informing obligation. According to the relevant Article 12, Data Responsible is obliged to (i) prevent the illegal processing of personal data, (ii) prevent illegal access to personal data and (iii) take all sorts of technical and administrative measures as to provide an appropriate level of security for restoring personal data. In the event that Data Responsible violates above specified obligations, it will be subject to administrative fine of minimum 15.000 Turkish Lira up to 1.000.000 Turkish Lira.

The establishment of Personal Data Protection Authority is planned for the purposes of protecting personal data and applying the Law. Additionally, it is foreseen that Personal Data Protection Committee ("Committee") is established within 6 months following the publication of the Law. Article 16 of the Law brings an obligation for Data Responsible to be registered at the Data Responsible Registry ("Registry") before starting to process personal data. Violators will be subject to an administrative fine of minimum 20.000 Turkish Lira up to 1.000.000 Turkish Lira.

Registry will start to carry out its activities following the establishment of the Authority (within 6 months starting from the enforcement of the Law). Within the same Article it is foreseen that exceptions can be made to the registry rule. The criteria to be taken into account for exceptions are such as "the characteristics and number of the processed personal data, lawfulness of the data processing or transfer of personal data to third party".

4. Transfer of Personal Data

4.1 Transfer of Personal Data Domestically

The explicit consent of data subject that is sought in the processing of personal data is sought for transfer of personal data domestically as well. However, the exceptional situations where explicit consent is not sought for personal data processing is applicable in transfer as well. Therefore, personal data can be transferred without seeking explicit consent of the data subject provided that one of the conditions in the relevant articles exists in the event of exceptional situations in second paragraph of Article 5 and third paragraph of Article 6. Such situations are specified in above specified section 2.2.

4.2 Transfer of Personal Data Abroad

Explicit consent is sought in transfer of personal data abroad as in processing of personal data and transfer of personal data domestically. However, in the event of exceptional situations in second paragraph of Article 5 and third paragraph of Article 6, in addition to the existence of one of the conditions in the relevant articles; adequate protection in the country of transfer (i.e. country to which transfer will be made) is sought. According to the relevant Article 9, if there is no adequate protection in the country of transfer, personal data can be transferred abroad even if the data subject does not give explicit consent provided that (i) Data Responsible both in

Turkey and country of transfer undertake the protection in written form and (ii) Committee authorizes the transfer.

Adequate Protection

According to third paragraph of Article 6, the countries where adequate protection exists are determined and announced by the Committee. Under fourth paragraph of the same article several criteria are foreseen for the Committee to decide to permit the transfer and whether or not adequate protection exists in the country of transfer. The Committee evaluates such criteria and if it deems necessary asks for the relevant authorities' opinion. The criteria are as follows:

- International treaties and conventions to which Turkey is a party
- Reciprocity between the country of transfer and Turkey regarding data transfer
- For each specific personal data transfer, characteristic of the personal data and purpose and term of processing
- The legislation and application of the country of transfer on the subject
- The measures that have been undertaken by the Data Responsible that is in the country of transfer

The Foreign Element in the Processing of Personal Data

Article 35 of Turkish Private International Law numbered 5718 is applied in the claims that involve foreign element and where such claims arise from processing of personal data or violation of personality rights by way of limiting right to information on personal data. The law to be applied in such claims can be chosen by the damaged party. The damaged party has the right to choose between the below specified law systems:

- The law of the habitual residence of the damaged party if the damaging party should have expected that the damage would occur in this country
- The law of the country where the place of business or the habitual residence of the damaging party is situated or
- The law where the damage has occurred if the damaging party should have expected that the damage would occur in this country

Findings and Recommendations on the Obligations of the Data Responsible

Our recommendations for the Data Responsible to be in compliance with the Law are as follows:

- For the Data Responsible to be in compliance with the rules of data processing, it needs to arrange their systems in accordance with the Law and prepare a strategy for the processing of personal data. Such strategy will cover all channels of data collection such as internet, call centre and contract
- For the Data Responsible to fulfil the obligations under the Law, the Data Responsible needs to determine the incompliance by analysing the internal procedures and politics and eliminate such incompliances
- The determination of obligations of Data Responsible in terms of data protection by

making a gap analysis comparing the current situation and targeted situation

- Evaluation of explicit consent and obtaining statements for this purpose if necessary
- Training of the employees for data protection purposes and keeping these records for this purpose
- Review and update of the internal registry system of the Data Responsible's employees and update of the personal data protection policies of the employees accordingly
- Informing the customers regularly on personal data processing methods and informing the customers in written form in case of change
- Collaboration and communication of the relevant departments of the Data Responsible on data processing matters
- Carrying out studies to minimize the risk by making evaluations on personal data secrecy, processing of personal data and supporting information technologies
- Updating of the existing of the existing contracts by reviewing the obligations related to personal data protection
- Follow up of the registration at the Registry
- Follow up of the above specified arrangements and announcements that will be done by the Authority

In compliance with the current legislation, the information and material contained in this memorandum is for general information purposes only. It is not intended to constitute an advertisement, a contractual offer of service, legal or other professional advice, and should not be relied on or treated as a substitute for professional counselling. Isiktac & Atabay Law Firm declines all responsibility for any loss which may arise from reliance on the herein information.