LBF PARTNERS
Law & Consultancy

DATA PROTECTION LAW IN TURKEY

Law No:6698 on the Protection of Personal Data (**"PPD Law**"), published in the Official Gazette on 7 April 2016, has established the legal framework for the protection of personal data in Turkey. This Law is generally inspired by the European Union's Directive No: 95/46 on Data Protection ("**Directive No:95/46**"), although its differs from the latter on some aspects.

PPD Law mainly sets out the conditions that personal data may be processed, stored and transferred, and the obligations of data controllers and data processors for ensuring the security of personal data. The Law also provides the formation of the Data Protection Authority of Turkey, which is responsible for monitoring compliance with the rules and procedures laid down in the Law and imposing fines on persons breaching those rules or procedures.

The important aspects of the legal framework established by PPD Law may be summarised as below:

I. The Term "Personal Data"

The term "personal data" is at the centre of the legal framework set out under PPD Law. Article 3/I(d) defines personal data as "*any information relating to an identified or identifiable natural person*". This definition is almost the same as the definition for personal data provided for under Directive No:95/46.

According to this definition, data relating to legal persons or anonymous or any other data that cannot be associated with an identifiable person may not qualify as personal data and therefore the processing of those data falls outside PPD Law. As "*all information relating to an identifiable natural person*" constitutes personal data, any information does not have to have any kind of sensitive to fall under PPD Law. That said, Article 6 of PPD Law provides more strict conditions for the processing of the special categories of personal data, including *data concerning a person's race, ethnic origin, political opinions, philosophical belief, religion, sect or other faith, attire and clothing, membership to associations, unions or trusts, health, sex life, criminal record and biometric and genetic data.*

II. Data Processing

PPD Law essentially regulates the "processing" of personal data. Therefore, the term "processing of personal data" is another central concept of the Turkish data protection framework. According to Article 3/I(e) of PPD Law, "processing of person data" means "*any operation performed upon personal data, such as collection, recording, storage, maintenance, alteration, rearrangement, disclosure, transfer, acquisition, dissemination or otherwise making available, classification or blocking of personal data wholly or*

partially, by automatic means or non-automatic means, where it is part of a filling system." The concept of data processing has been broadly defined so that PPD Law may catch any breach committed by using unforeseen methods and technologies.

Article 4 of PPD Law sets forth the general principles that must be complied in processing personal data. Those principles are:

(i) to be compatible with law and rules of good faith,

(ii) to be accurate and, where necessary, up-to-date,

(iii) to process for specific, explicit and legitimate purposes,

(iv) to be relevant, limited and proportionate to the purpose underlying the processing,

(v) to store for such duration which is specified in the relevant legislation or is necessary for the fulfilment of the purpose of processing.

III. Data Controller and Data Processor

The responsibility for processing personal data in compliance with PPD Law principally belongs to data controllers. Article 3/I(ı) defines data controller as "*any natural or legal person who determines the purposes and means of the processing of personal data, and who is responsible for the establishment and management of the filing system under the Law*." In this regard, data controllers may be natural persons, public institutions, business entities or foundations.

A data controller may utilise the services of data processors in processing personal data. The term "data processor" is defined in Article 3/I(ğ), as "*any natural or legal person who processes personal data based on the authority granted by and on behalf of the data controller*." Data controllers are jointly and severally responsible for the breaches by data processors of PPD Law. Data processors are also under obligation to take necessary measures to ensure the security of personal data and prevent unlawful access thereto.

IV. Obligations of Data Controllers

1. Obtaining the Consent of the Data Subject

a) General

Article 5.1 of PPD Law states that in principle personal data may not be processed without the explicit consent of the data subject. However, in any of the exceptional cases provided for under Article 5.2, the data controller may be entitled to process *personal data which do not fall under the special category specified in Article 6*, without the explicit consent of the data subject. These exceptional situations are as below:

(i) if the processing of data is expressly provided for under any law,

(ii) if it is necessary for protecting the life or physical integrity of the data subject who is physically or legally incapable of giving his/her consent, or of another person,

(iii) if it is necessary for the execution or performance of a contract,

(iv) if it is necessary for compliance with a legal obligation,

(v) if the data is made public by the data subject herself/himself,

(vi) if it is necessary for the establishment, exercise or protection of a right and

(vii) if it is required for the legitimate interests of the data controller, provided that the fundamental rights and freedoms of the data subject are not harmed.

Article 6 of the Law provides more restrictive conditions for processing of sensitive personal data. Accordingly, *sensitive personal data other than to health and sexual life* may be processed without the explicit consent of the data subject, only if such processing is explicitly provided for by any law. *Personal data relating to health and sexual life* may however be processed, without obtaining the explicit consent of the data subject, only by persons under confidentiality obligation or competent institutions and organizations for purposes of the protection of public health, the operation of preventive medicine, medical diagnosis, treatment and care services and planning and management of health services and financing.

b) Transfer of Personal Data

Although the transfer of personal data is also a sort of data processing, it is separately regulated under Article 8 and 9 of PPD Law. Pursuant to Article 8, the data controller may transfer personal data to third parties either upon the explicit consent of the data subject or where one of the exceptions provided for under Article 5 or 6 for processing of general or special personal data without explicit consent is present.

Article 9, however, sets forth additional conditions for transferring personal data abroad. Personal data may be transferred abroad without obtaining the explicit consent of the data subject, if one of the conditions set forth in the Article 5 or Article 6, if applicable, is present and

- if the foreign country to whom personal data will be transferred provides adequate level of data protection or
- in case there is no adequate level of data protection, if the data controllers in Turkey and abroad commit, in writing, to provide an adequate level of protection and take the permission of the Data Protection Board of Turkey.

Which countries are considered to provide adequate level of data protection will be declared by the Data Protection Board.

2. Informing the Data Subject on the Protection of Personal Data

Article 10 of PPD Law requires data controllers to inform data subjects, at latest when collecting the personal data, of: (i) the identity of the data controller and if any, its representative, (ii) purposes for which personal data will be processed; (iii) persons to whom processed personal data might be transferred and purposes for such transfer, (iv), the method and legal reason of collection of personal data and (v) the rights of data subjects set forth under Article 11.

Exceptions for the information requirement set forth in the second paragraph of Article 28 of PPD Law is more limited than those for the consent requirement. Only situation in which a private data controller is not under the duty to provide information is where personal data are made public by the data subject himself/herself. Other than this exception, private data controllers must make information notice, even if obtaining explicit consent is not compulsory under Articles 5 or 6 of PPD Law.

3. Deletion, Destruction or Anonymization of Personal Data

The fact that personal data has been legally processed in the first place does not entitle the data controller to store such data forever. According to the first paragraph of Article 7 of PPD Law, personal data legally processed must be deleted, destroyed or anonymized, ex officio or upon the request of the data subject, by the data controller, once the reason for processing such data in the first place disappears. On 29th of May 2017, the Data Protection Board published a draft Regulation on the Deletion, Destruction and Anonymization of Personal Data and opened it to public consultation. It is expected that the Board will adopt the Regulation within the year 2017.

4. Data Security and Data Inspection

Another obligation of data controllers arising after personal data is legally processed is set forth under Article 12 of PPD Law. Accordingly, the data controller must take all necessary technical and organizational measures for providing an appropriate level of security to prevent unlawful processing of, and access to, personal data, and safeguard them. In case personal data are processed on behalf of the data controller by a data processor, the data controller will be jointly and severally liable with such person for providing such data protection.

The data controller is also obliged to carry out necessary inspection to ensure compliance with the provisions of PPD Law within its institution or organization.

Finally, if processed personal data are acquired or accessed by others through unlawful means, the data controller must notify the data subject and the Data Protection Board of such situation as soon as possible.

5. Responding to the Data Subject's Requests and Complying with the Board Decisions

Pursuant to Article 13 of PPD Law, data controllers must respond to requests made by data subjects, at latest within 30 days. In case responding to the request results in additional cost or charge, the data subject may be charged with a fee in such amount that will be specified by the Data Protection Board, provided that the application of the data subject is not made due to the fault of the data controller.

If the data controller considers the request justified, it must take necessary actions to satisfy the request. If the data controller refuses to respond or does not respond within the time limit, then the data subject will be entitled to make complaint to the Data Protection Board, within 30 days from the day he/she receives the response from the data controller and in any case at latest within 60 days from the date of the request.

When the Board takes a decision upon the application of the data subject or its ex officio examination, the data controller must comply with such a decision at latest within 30 days from the receipt of the decision.

6. Registering in the Data Controllers Registry

According to Article 16 of PPD Law, data controllers that will be specified by the Data Protection Board will be required to register in the Data Controllers Registry to be held by the Board. On 5th of May 2017, the Board published a draft Regulation on the Data Controllers Registry and opened it public consultation. The draft Regulation regulates how the registration will be made in the Registry. However, it does not specify which data controllers will be subject to the registration requirement and when such obligation must be fulfilled. Pursuant to the draft Regulation, these matters will be addressed by the Board later in a resolution.

V. Sanctions

The breach of obligations set out under PPD Law may result in criminal, administrative or civil liability of the persons concerned. First of all, persons who illegally record, collect or transfer personal data or fail to destroy or delete them may be sentenced to imprisonment between one and six years. In addition, pursuant article 18 of PPD Law, in the event of a breach of obligations provided for thereunder, the Data Protection Board of Turkey may impose an administrative fine up to 1,000,000 Turkish Liras. Finally, data subjects whose personal rights over their personal data are violated, and competitors claiming unfair competition may bring damages actions against the breaching data controller. Considering all these outcomes, it is highly important particularly for companies to ensure compliance with PPD Law.

LBF PARTNERS
Law & Consultancy

LEGAL SERVICES WE OFFER TO OUR CLIENTS

As LBF Partners, we offer legal services to our clients on all aspects of data protection law, including but not limited to:

- preparing data maps of the client, identifying data subjects whose consent must be obtained for processing his/her personal data, and drafting necessary documents for obtaining consent from data subjects and informing them about the protection of their personal data;
- reviewing and updating all agreements executed with customers, employees, suppliers and other third parties whose personal data is processed or to or by whom personal data is transferred or accessed, in order to ensure compliance with PPD Law and other data protection legislations;
- drafting internal policies, regulations, layouts and notification documents relating to collection, process, storage of and access to personal data,
- providing all necessary legal assistance for registration in the Data Controllers Registry,
- providing in-company trainings on data protection law.

If you need any legal assistance in this matter, please contact us via info@lbfpartners.com.