

# THE Fine PRINT

Gokce  
Istanbul

April 2016  
43  
Special Issue



## Data Protection Law: Time to Take Measures



## Data Protection Law: Time to Take Measures

The Data Protection Law no. 6698 (Law) which has been expected for a long time was finally published in the Official Gazette and came into effect on 7 April 2016.

The terms of “personal data” and “processing personal data” are defined inclusively under the Law and legal and natural persons using, recording or processing data related customers, employees and other persons are included scope of the Law. Therefore it is expected that all business entities will be affected from the Law.

The Law sets forth heavy sanctions such as administrative fines up to TL 1.000.000 and, in some cases, imprisonment up to 6 years in case of violation.

Personal data which were processed before the effective date of this Law are also included within the scope of Law and a transition period is set forth for the same.

In order to ensure compliance with the Law, business entities are recommended to evaluate their current situations and then to carry out a compliance work with respect to past and future transactions.

## Personal Data

Under the Law, personal data is inclusively defined as “any information relating to an identified or identifiable real person”.

Personal data is any data which directly or indirectly makes a person identifiable such as name, surname, date of birth, place of birth, telephone number, vehicle registration plate number, passport number, curriculum vitae, photo, audio or video record, fingerprint, IP address, e-mail address, hobbies or preferences of person, people who are in contact with a person, group membership, information regarding a person’s family or health etc.

Any data, as described above, which:

- the employers collect from their employees; or
  - the sellers or service providers collect from their customers; or
  - the associations/foundations collect from their members
- may be given as examples for personal data.





## Processing Personal Data

Processing personal data means any operation performed on personal data, whether or not by automatic means, such as collection, recording, storage, retaining, adaptation or alteration, retrieval, disclosure by transmission, transfer, making available, alignment or blocking wholly or partly. It must be noted that the collection or storage of personal data shall be deemed as processing even the data is not used in any transaction or on any platform or disclosed to third parties.

## Conditions for processing Personal Data

According to basic principles set out in the Law, personal data must; (i) be processed lawfully and fairly, (ii) be accurate and where necessary kept up to date, (iii) be collected for specific, explicit and legitimate purposes, (iv) not be excessive in relation to the purpose of processing, and (v) not be kept for longer than necessary.

As the general principle, personal data can only be processed with an explicit consent of data subject provided that the principles listed above are met. On the other hand, personal data may be processed without obtaining explicit consent of a data subject (i.e. whose data is processed) provided that the exemptions listed under the Law.

Personal data shall be erased, destroyed or anonymized after disappearance of the reason for processing.

## Controller and Processor

The Law defines a data controller (Controller) as a “real” or “legal” person which is in charge of the establishment and management of the data filing system within a unit, institution or agency, and a data processor (Processor) as a real or legal person which is authorized by the Controller to process personal data on its behalf.

A Controller is obliged, under the Law, to take necessary measures in order to provide an adequate level of security for personal data. Controller and Processor are held liable jointly for security of the personal data they possess.

## Notification obligations for Personal Data

According to the Law, a Controller or a person authorized by a Controller shall inform data subjects regarding the following matters:

- the identity of Controller or Controller’s representative,
- the purpose of processing,
- to whom or for what purposes may the processed personal data be transferred to,
- the reason and method of collecting personal data,
- the rights of data subject stated in the Law.

The notification obligation is applicable even in the cases where explicit consent for processing of personal data is not required.



## **“Special Categories” of Personal Data**

The Law also describes certain “special categories” of personal data (Special Categories of Personal Data) such as racial or ethnic origin, political opinions, religious, denominational or other beliefs, appearance, health state, sexual life, data regarding a person’s criminal convictions or security measures, genetic and biometric data. Special Categories of Personal Data other than data regarding health state of sexual life of the data subject cannot be processed without explicit consent of data subject except where the laws explicitly permit so.

Data regarding health or sexual life may be processed without explicit consent of data subject, provided that it is processed by authorized institutions and organizations or individuals, who are under the oath to preserve secrets, for the purposes of protection of public health, preventive medicine, medical diagnosis, providing treatment and care services, planning, management and financing of health services.



## **Conditions of transferring of personal data to third parties**

The following can be given as examples for transferring personal data; (i) disclosing the information of customers or employees of a real or legal person to advertising agencies or marketing companies or (ii) disclosing such data to third parties in order to obtain statistical data.

As the general principle, personal data cannot be transferred to third parties without explicit consent of the data subject except for the exemptions listed under the Law.

## **Conditions for transferring personal data to a foreign country**

The most common example for the transferring personal data to a foreign country is transferring personal data regarding customers or employees of real or legal persons in order to host such data on servers located in such foreign country.

As the general principle, personal data shall not be transferred to foreign country without the explicit consent of the data subject except for the exemptions listed under the Law.

If the foreign country is not able to ensure an adequate level of protection, the data may be transferred without explicit consent of data subject, only if a written commitment regarding adequate protection is obtained from Controllers both in Turkey and the country to which the data is to be transferred and authorization of the Board is obtained. Board is authorized to determine and declare whether a foreign country provides an adequate level of protection.

## **Personal Data Protection Board and Registry of Data Controllers**

According to the Law, real or legal persons who process personal data are obliged to register with the Data Controllers Registry which will be maintained publicly under the supervision of the Personal Data Protection Board (Board) before processing personal data.



## Sanctions and penalties in case of breach of the Law

In case of a breach of the Law, administrative fines from TL 5,000 to 1,000,000 will be imposed. Also in case of breach of provisions of Turkish Criminal Code (TCC) with respect to personal data, imprisonment from one year to six years may be imposed depending on the type of the breach.

In this context, it is considered that the crimes and sanctions regarding personal data in the TCC which have been in effect before the effective date of the Law but have had no place to be applied due to lack of definition of personal data, will have a field of application after the Law comes into force.

## Situations where the Law is not applicable

Some of the examples to which the Law shall not be applied are as follows: (i) processing personal data by real persons within the scope of the activities related to themselves or family members living in the same residence, (ii) processing of personal data by means of anonymization for the purposes of research, planning and statistic etc., (iii) processing of personal data for artistic, historical, literary or scientific purposes only if they do not constitute a crime or they do not create a conflict with national defense, national security, public safety, public order, financial safety, right of privacy or personal rights.



## Principles regarding effectiveness and transition period

Provisions regarding transfer of personal data to third parties or foreign country, data subject's rights, application and complaints, sanctions and administrative fines shall enter into force after six months from the date of publication of the Law. The other provisions shall enter into force as of publication date of Law.

The Law also introduces a transition period of 2 years with respect to compliance for the personal data which were processed before publication date of the Law. On the other hand, consent which was legally obtained before publication date of the Law will be deemed valid unless the data subject revokes its consent within one year as of the publication date.

Secondary legislation with respect to Law will be published in one year from the publication of the Law.

## Compliance with the Law

In light of the information given above, it must be considered that real or legal persons subject to Law should determine the current situation and make a risk assessment regarding data processing. All the records regarding customers, employees and business partners should be analyzed and it should be determined for which purposes and by whom and what data is being processed.

After a thorough legal due diligence, (i) a document containing data subject's approval regarding processing of his/her personal data should be prepared; (ii) internal trainings should be provided to employees; (iii) agreements signed and/or to be signed with employees, customers and Processors as well as with any other real or legal persons who are subject to the Law should be revised. Having said that, it must be considered that under the Law, the sanctions for noncompliance shall be applied after 6 months as of the effective date.



# Answers. Not theories.

## Gokce Attorney Partnership

### Editors:



**Assoc. Prof. Dr. Ali Pasli**  
ali.pasli@gokce.av.tr



**Zeynep Ozsoy**  
zeynep.ozsoy@gokce.av.tr

### About our firm

Gokce Attorney Partnership is an Istanbul-based law firm offering legal services across a broad range of practice areas including mergers and acquisitions, joint ventures, private equity and venture capital transactions, banking and finance, capital markets, insurance, technology, media, telecoms and internet, e-commerce, data protection, intellectual property, regulatory, real property, and commercial litigation. Please visit our web site at [www.gokce.av.tr](http://www.gokce.av.tr) for further information on our legal staff and expertise.

**Please contact us at**  
**contact@gokce.av.tr**  
**0 212 352 88 33**

*The Fine Print is prepared and published for general informative purposes only and does not constitute legal advice or create an attorney-client relationship. Should you wish to receive further information, please contact Gokce Attorney Partnership. No content provided in The Fine Print can be reproduced or re-published without proper attribution or the express written permission of Gokce Attorney Partnership. While all efforts have been made to ensure the accuracy of the content, Gokce Attorney Partnership does not guarantee such accuracy and cannot be held liable for any errors in or reliance upon this information. The Fine Print was created for clients of Gokce Attorney Partnership and the possibility of circulation beyond the firm's clientele should not be construed as advertisement.*