

DATA PROTECTION LAWS OF THE WORLD

Turkey



Downloaded: 11 July 2017

TURKEY



Last modified 26 January 2017

LAW

The Turkish Data Protection Law No. 6698 ('DP Law'), which is based on EU Directive 95/46/EC, came into force on 7 April 2016.

DEFINITIONS

Definition of personal data

In the DP Law, personal data was described as *"Any information relating to an identified or identifiable natural person"*.

Definition of sensitive personal data

Sensitive personal data (Special Categories of Personal Data as mentioned in the DP Law) is defined as *"...data revealing data subject's ethnicity, political views, philosophical beliefs, religion, sect or other beliefs, appearance, membership to associations, foundations or unions, information related to health, sex life, previous criminal convictions and biometric data..."*

NATIONAL DATA PROTECTION AUTHORITY

The new DP Law introduces two bodies to watch over and regulate data processing and transfer activities. These are the Data Protection Board and the Data Protection Authority.

In accordance with the decision which was published in the Official Gazette dated 30 December 2016, the last two members were appointed to the Data Protection Board bringing this to a total of nine members, which means that the establishment of the Data Protection Board is now complete.

The Data Protection Board is an independent decision making body.

REGISTRATION

As of October 7, 2016, all data controllers are required to enlist with the Data Protection Registry to be held under the Data Protection Authority and under supervision of the Data Protection Board.

DATA PROTECTION OFFICERS

There is not yet a requirement in Turkey to appoint a data protection officer.

COLLECTION & PROCESSING

Pursuant to the DP Law, it is mandatory to comply with certain principles to collect and process personal data. In light of such principles personal data must be:

- processed fairly and lawfully
- accurate and up to date
- processed for specific, explicit and legitimate purposes
- relevant, adequate and not excessive
- kept for a term necessary for purposes for which the data have been processed.

Further, in principle, personal data cannot be processed without being collected and processed with explicit consent of the data subject. However the DP Law stipulates certain exceptions where consent is not required. These are:

- processing is expressly permitted in the law
- processing is necessary for protection of data subject's, who is not in a situation to give consent due to an actual impossibility or a person whose consent is not legally recognized, or third parties' life or physical integrity
- processing personal data of contractual parties is necessary for forming or the performance of a contract
- processing is mandatory for the data controller to perform his/her legal obligation
- personal data has been opened to the public by data subject
- processing is mandatory for assigning, using or protecting a right
- processing is mandatory for legitimate interest of data processor and without damaging rights of data subject.

As part of the collection of data from the data subject the controller is obliged to provide the data subject with the following information:

- the identity of the controller and of his representative, if any
- the purposes of the processing for which the data is intended
- the recipients of the data and the reasons for transfer
- the process of collecting data and the legal grounds, and
- the rights of the data subject.

Where the data has not been obtained from the data subject, the controller shall provide the data subject with the above stated information as well as details of the categories of data concerned.

Processing of sensitive personal data without explicit consent of the data subject is forbidden. However sensitive data other than health and sex life data can be processed without explicit consent of data subject only if a law/legislation permits such processing. Further, health data and sex life data can only be processed by natural persons who are under oath of secrecy or by authorities for the purposes of protecting public health, preventive medicine, medical diagnosis, the provision of care and treatment services or planning, management and financing of health-care services.

TRANSFER

The DP Law distinguishes transfer of personal data to third parties in Turkey and transfer of personal data to third countries.

Transfer of personal data to third parties

In principle, personal data can be transferred to third parties with explicit consent of data subject. The conditions and exemptions

applied to collection and processing of personal data are applied for transfer of personal data to third parties.

Transfer of personal data to parties in third countries

In addition to conditions and exemptions applied for transfer of personal data to third parties, either of the following conditions shall exist for transfer of data to parties in third countries:

- The country to which personal data will be sent shall have sufficient level of protection
- The data controller in Turkey and target country shall undertake protection in writing and obtain the Data Protection Board's permission.

SECURITY

In light of the provisions of the DP Law and consistent with the principles of good faith those entrusted with personal data are expected to ensure protection of such data. Under the DP Law, the data controller is required to ensure that appropriate technical and organisational measures are taken to prevent all illegal processing and to ensure the data is not destroyed, lost, amended, disclosed or transferred without authority. Such measures must ensure an appropriate level of security, taking into account the state of the art and the costs of their implementation in relation to the risks inherent in the processing and the nature of the data to be protected.

BREACH NOTIFICATION

There is no breach notification requirement; nonetheless, in the event that data is inadvertently or erroneously lost, transferred, destroyed etc., notification should be made to the data subjects in accordance with the principles of good faith. Furthermore, each situation should be evaluated in accordance with provisions of the applicable specific law, if any, as more strict procedures may apply.

ENFORCEMENT

The DP Law and the Turkish Criminal Code No. 5237 imposes custodial sentences for the unlawful processing of data. The Turkish Civil Law No. 4721 affords the right to claim compensation for the unjust use of data and a number of other laws impose administrative fines.

Furthermore, the DP Law introduces administrative fines up to TRY 1.000.000 (€247.000) for those who act against the requirements or rules in the DP Law.

ELECTRONIC MARKETING

The Law on Regulation of Electronic Trade was published in the Official Gazette on 5 November 2014 ("**Electronic Trade Law**"). The Electronic Trade Law came into force on 1 May 2015. Further, secondary legislation (The Regulation on Electronic Trade) was published in the Official Gazette on 26 August 2015 and came into force on the same date.

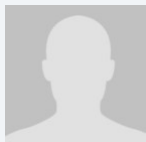
Pursuant to the Electronic Trade Law, commercial electronic communication (electronic marketing) can only be sent by obtaining prior consent (opt-in) from recipients. Such consent can be obtained in writing or through means of electronic communication. It is required that the commercial electronic communication is in compliance with the consent obtained from recipients. Further, the identity of the service provider, contact information (such as e-mail, sms, telephone number, fax number (depending on the type of commercial electronic communication) and if made on behalf of a third party information the third party must be present.

Pursuant to the Electronic Trade Law, consumers have the right to refuse commercial electronic communication. The service provider is obliged to allow the free transmission of the refusal. Commercial electronic communications to recipient must be ceased within 3 business days from the receipt of refusal. Non-compliance with the above obligations stated is subject to administrative fines between 1.000 TRY to 15.000 TRY (approx. 247 - 3.706 EUR).

ONLINE PRIVACY

There is no legislation in Turkey which specifically regulates privacy on Cookies and Location Data. However, Law No. 5651 on Regulating Broadcasting in the Internet and Fighting against Crimes Committed through Internet Broadcasting enables internet users to initiate prosecution in case of infringements of their personal rights.

KEY CONTACTS



Baak Kartal

Associate

[Gokce Yarat Attorney Partnership](#)

T +90 212 352 88 33

basak.kartal@gokce.av.tr

DATA PRIVACY TOOL

You may also be interested in our [Data Privacy Scorebox](#) to assess your organisation's level of data protection maturity.

Disclaimer

DLA Piper is a global law firm operating through various separate and distinct legal entities. Further details of these entities can be found at www.dlapiper.com.

This publication is intended as a general overview and discussion of the subjects dealt with, and does not create a lawyer-client relationship. It is not intended to be, and should not be used as, a substitute for taking legal advice in any specific situation. DLA Piper will accept no responsibility for any actions taken or not taken on the basis of this publication.

This may qualify as 'Lawyer Advertising' requiring notice in some jurisdictions. Prior results do not guarantee a similar outcome.

Copyright © 2017 DLA Piper. All rights reserved.