DATA PROTECTION LAWS OF THE WORLD

Turkey

TURKEY

Last modified 22 January 2024

LAW

The main piece of legislation covering data protection in Turkey is the Law on the Protection of Personal Data No. 6698 dated April 7, 2016 (LPPD). The LPPD is primarily based on EU Directive 95/46/EC.

To date, the legislature has enacted several regulations to implement various aspects of the LPPD. The notable ones are mentioned below:

- Regulation on the Erasure, Destruction and Anonymizing of Personal Data (published in the Official Gazette dated October 28, 2017, numbered 30224);
- Regulation on the Working Procedures and Principles of Personal Data Protection Board (published in the Official Gazette dated November 16, 2017, numbered 30242);
- Regulation on the Registry of Data Controllers (published in the Official Gazette dated December 30, 2017, numbered 30286);
- Regulation on the Organization of Personal Data Protection Authority (published in the Official Gazette dated April 26, 2018, numbered 30403);
- The *Communiqué* on Procedures and Principles for Compliance with the Obligation to Inform (published in the Official Gazette dated March 10, 2018, numbered 30356);
- The *Communiqué* On The Principles And Procedures For The Request To Data Controller (published in the Official Gazette dated March 10, 2018, numbered 30356);
- The Decision of Data Protection Board, dated January 31, 2018, numbered 2018/10 on Adequate Measures to be taken by Data Controllers in Processing the Special Categories of Personal Data.

Certain general laws such as the Turkish Criminal Code no. 5237 and sector specific laws such as Electronic Communications Law No. 5809 also touch upon data protection and are mentioned below when relevant.

DEFINITIONS

Definition of personal data

In the LLPD, personal data is defined as “Any information relating to an identified or identifiable natural person.”

Definition of sensitive personal data

Sensitive personal data (Special Categories of Personal Data under the LPPD) is defined as "personal data relating to race, ethnic origin, political opinions, philosophical beliefs, religion, sect or other beliefs, clothing, membership of associations, foundations or trade unions, information related to health, sex life, previous criminal convictions and security measures, and biometric and genetic data.”

NATIONAL DATA PROTECTION AUTHORITY

The national data protection authority is the Kisisel Verileri Koruma Kurumu (Personal Data Protection Authority). The Personal Data Protection Authority’s decision-making body is Kisisel Verileri Koruma Kurulu (Personal Data Protection Board). The organizational structure of the Authority and the duties and powers of its bodies are regulated under the Regulation on the Organization of Personal Data Protection Authority and the Regulation on the Working Procedures and Principles of Personal Data Protection Board.

Kisisel Verileri Koruma Kurumu
Nasuh Akar Mah. Ziyabey Cad. 1407. Sok. No: 4
06520 Balgat-Çankaya / Ankara

T +90 312 216 5050

Website

kvkk.gov.tr

REGISTRATION

Pursuant to the LPPD and the Regulation on the Registry of Data Controllers, data controllers are required to enroll in the Registry of Data Controllers before proceeding with data processing.

The Regulation on the Registry of Data Controllers was published in the Official Gazette dated December 30, 2017, and entered into force on January 1, 2018. It regulates the establishment of a publicly accessible registry, which is to be held by the Personal Data Protection Authority and the procedures and principles concerning enrollment in the registry.

Under this Regulation, all data controllers are required to enroll in the Registry of Data Controllers before proceeding with data processing. However, the Personal Data Protection Board may bring an exception to the obligation of enrollment by taking into account the nature and number of personal data, purpose of processing personal data, and other objective criteria. Data controllers are not required to enroll in the Registry of Data Controllers in the following circumstances:

- The processing of personal data is required for criminal investigation or for prevention of a criminal offense;
- If the personal data being processed is already publicized by the data subject;
- If, based on the authority given by Law, personal data processing is required for disciplinary investigation or prosecution and execution of the supervision or regulation duties to be conducted by public institutions and organizations and professional organizations with public institution status; or
- If processing of personal data is required to protect the economic and financial interests of the State in relation to budget, tax and financial matters.

Over the past year, the Personal Data Protection Board has enumerated additional exceptions to enrollment obligation:

- Data controllers who process personal data by non-automatic means as a part of a filing system, lawyers, independent accountants and financial advisors;
- Natural or legal persons having less than 50 employees per annum and annual balance less than 25 million Liras and whose main field of activity is not processing special categories of personal data.

Data controllers who are non-resident in Turkey shall enroll in the registry through a representative they assign in Turkey. Legal persons in Turkey or Turkish citizens may be assigned as representatives for this purpose.

In addition, both legal entities resident in Turkey and the above-mentioned representatives of non-resident data controllers shall, as part of the enrollment procedure, appoint an individual to act as “contact person” for both the Personal Data Protection Authority and for data subjects.

Operations related to the Registry of Data Controllers shall be carried out through VERBIS (Data Controllers Registry Information System) by data controllers. The Personal Data Protection Authority, with its decision dated March 11, 2021, numbered 2021/238, had extended the dates for the registration through VERBIS until December 31, 2021.

Although the deadline has passed, it is still possible for local and foreign data controllers to register with VERBIS if the obligation arises or if the controller failed to register in time.

On August 15, 2022, the Data Protection Authority has started enforcement against foreign controllers that did not register within the deadline. Within the context of such enforcement the Data Protection Authority sent out letters to foreign controllers to request information as to reasons why the registration was not completed together with information on the number of users and global turnover to calculate the administrative fine.

Administrative fines of between TRY 189.245 - TRY 9.463.213 (approx. € 3.738 - € 296,245) may be imposed on data controllers breaching obligations regarding the Registry of Data Controllers.

Further, the DPA has the right to restrict the data processing activities of a data controller in cases of clear unlawfulness operation by a data controller and in theory, processing personal data without registering with the Registry of Data Controllers may lead to such restriction.

DATA PROTECTION OFFICERS

There is not yet a requirement in Turkey to appoint a data protection officer in the sense of GDPR. However, there is a requirement to appoint a local Representative for foreign controllers.

COLLECTION & PROCESSING

Pursuant to the LPPD, it is mandatory to comply with certain principles while collecting and processing personal data. In light of such principles collected personal data must be all of the following:

- 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 or for a term prescribed in relevant laws 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 LPPD stipulates certain exceptions where consent is not required. These are:

- Processing is expressly permitted by law;
- Processing is necessary for protection of the life or physical integrity of the data subject or a third party, where the data subject is not physically or legally capable of giving consent;
- Processing personal data of the contractual parties is necessary for the conclusion or the performance of a contract;
- Processing is mandatory for the data controller to perform his / her legal obligation(s);
- Personal data has been made public by the data subject;
- Processing is necessary in order to assign, use or protect a right;
- Processing is necessary for the legitimate interests of data processor and this does not damage the rights of the data subject.

Pursuant to Article 10 of the LPPD, data controllers or their authorized persons have an obligation to inform data subjects during the collection of the personal data. The Communiqué on Procedures and Principles for Compliance with the Obligation to Inform published in the Official Gazette dated March 10, 2018, numbered 30356 sets forth the principles and procedures on the obligation to inform. As part of the collection of data from the data subject the controller is obliged to provide the data subject with the following information:

- Identity of the controller and of its representative, if any;

- Purposes of the processing for which the data is intended;
- Recipients of the data and the reasons for transfer;
- Process of collecting data and the legal grounds; and
- 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. According to the relevant *Communiqué*, the obligation to inform should be fulfilled within a reasonable time after collecting the personal data, or during the first contact if the personal data is obtained for communication purposes with the relevant persons, or at the very latest the time of the initial transfer if the personal data is to be transferred.

Processing of sensitive personal data without explicit consent of the data subject is generally forbidden, although sensitive data other than health and sexual life data can be processed without explicit consent of data subject if a law / legislation permits such processing. Under the LPPD, data controllers need to take adequate measures required for the processing of sensitive personal data and comply with the decisions and guides of the Personal Data Protection Board designating such adequate measures. See also Personal Data Protection Board Decision dated January 31, 2018, numbered 2018/10 on Adequate Measures to be taken by Data Controllers in Processing the Special Categories of Personal Data.

Health data and sexual life data can only be processed by natural persons who are under an 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, and the management and financing of healthcare services.

Deletion, destruction or anonymization of personal data

The Regulation on Deletion, Destruction or Anonymization of Personal Data ("Regulation on Deletion of Personal Data") was published in the Official Gazette dated October 28, 2017, and entered into force on January 1, 2018. This Regulation is crucially important for data controllers in terms of time limitations regarding deletion, destruction or anonymization of personal data.

Pursuant to the Regulation on Deletion of Personal Data, data controllers are required to prepare a personal data processing inventory and a personal data storage and destruction policy (Policy). Data controllers are also required to take measures to safeguard the data that they are processing, identify persons working in personal data storage and destruction processes, categorize personal data, store and destroy these data, and determine periodic destruction processes.

If the prerequisites for processing personal data provided under LPPD are not met, then the personal data must be deleted, destroyed or anonymized by the data controller (of its own accord or upon the application of related person). All actions related to the execution of this process must be recorded and these records shall be kept for at least three years.

In addition, if a data controller ceases to continue to meet the above conditions for processing personal data, then they must carry out a process of periodic destruction. Periodic destruction is the deletion, destruction or anonymization of personal data at recurring intervals specified in the relevant data controller's Policy. This period cannot exceed six months.

TRANSFER

The LPPD distinguishes between the transfer of personal data to third parties in Turkey and the 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 the explicit consent of the data subject. The conditions and exemptions applied to collection and processing of personal data also apply to the transfer of personal data to third parties.

Transfer of personal data to parties in third countries

In addition to the conditions and exemptions applied to the transfer of personal data to third parties, one 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 controllers in Turkey and in the target country shall undertake protection in writing and obtain the Personal Data Protection Board's permission; and
- Data controller shall sign BCRs published by the Personal Data Protection Board and obtain the approval of the Personal Data Protection Board.

The Personal Data Protection Board shall declare the countries having adequate level of protection. So far, the Personal Data Protection Board has not announced any country as adequate. However, the Personal Data Protection Board has announced the minimum clauses to be found in the undertakings of data controllers by setting out examples of undertaking where there is not an adequate level of protection in the country where personal data is transferred

In addition to the above, based on the announcement made by the Scientific Committee working towards amendments of the LPPD, the cross-border transfer rules will be updated and will be more in line with the GDPR. We are expecting the changes to occur within 2024.

SECURITY

In light of the provisions of the LPPD and consistent with the principles of good faith, those entrusted with personal data are expected to ensure protection of such data. Under the LPPD, the data controller is required to ensure that appropriate technical and organizational 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. Additionally, the data controller has to carry out the necessary inspections on its own institution or organization in order to ensure the implementation of the LPPD.

Data controllers and data processors shall not disclose any personal data in contradiction with the provisions of LPPD and shall not use any personal data for any purposes except for the purpose of processing. This obligation continues after leaving their institution.

In addition, the LPPD enables data subjects to apply to data controllers by various means in relation to their rights stated in Article 11. Data controllers have an obligation to take every necessary administrative and technical measure effectively to finalize these applications in accordance with the LPPD and in good faith. The Communiqué on Procedures and Principles for Application to Data Controller dated March 10, 2018, numbered 30356 outlines the procedures of application.

BREACH NOTIFICATION

There is no explicit definition of a data breach under Turkish Law. However, a breach can be defined as illegal acquisition of personal data by others / third parties.

The LPPD does not contain any thresholds for a notifiable breach. Therefore, all breaches (“illegal acquisition of personal data by others / third parties”) are notifiable to the Authority (within 72 hours) and to concerned data subjects (as soon as possible) without any criteria / threshold.

Under the DPL, controllers must notify the data subject and the Data Protection Authority in case of a data breach. The Data Protection Authority reserves the right to inform the public about the breach if it deems necessary.

While there is no specific time frame stipulated in the DPL, with the decision numbered 2019/10, which was published on February 15 2019, the Data Protection Authority stipulated the procedure for breach notifications, which can be found online.

Notification to the Data Protection Authority

Pursuant to Decision 2019/10, data controllers are required to notify the Data Protection Authority within 72 hours of becoming aware of a breach.

In cases where the notification cannot be sent within 72 hours, the causes for the delay must be sent as well.

Further, with the Decision 2019/10, the Data Protection Authority published the *Data Breach Notification Form*, which can be accessed here.

For all data breach notifications sent to the Data Protection Authority, the Data Breach Notification Form must be used. If it is not possible to fill out all of the information in the Data Breach Notification Form, a partially filled form may be sent to the Data Protection Authority. Therefore, gradual breach notification is possible.

The data breach notification sent to the Data Protection Authority can be sent via e-mail by sending the Data Breach Notification Form to ihlalbildirimi@kvkk.gov.tr with the subject “*Kişisel veri ihlali bildirimi*” or via the Data Protection Authority’s module.

Alternatively, the form can be sent by post to the Data Protection Authority’s address.

Notification to Data Subjects

There is no clear time frame stipulated for notification to data subjects. The **DPL** and the Decision 2019/10 require the data subjects to be notified “as soon as possible”. Notifications can be sent to data subjects directly if the data controller has their contact information. If not, any other appropriate way can be used, such as announcing the breach in data controller’s website.

Other requirements

Pursuant to Decision 2019/10, data controllers are required to prepare a “Data Breach Response Plan” which should specify who, within the organization, should be contacted in the event of a data breach. This person will be the primary person responsible for assessing the consequences of such a breach.

Further, there is a requirement to retain the records regarding (i) information on the data security breach, (ii) impacts of the breach, and (iii) measures taken, and to make these available for a possible assessment by the DPA.

ENFORCEMENT

Under the **DPL**, for the year 2023, the Board may apply administrative fines up to TRY 9.463.213 per breach in line with the following limitations. The amount of the administrative fines will be updated for 2024 based on the re-evaluation percentage to be published on the Official Gazette.

- Non-compliance with the information notice requirements: a fine between TRY 47.303 to TRY 946.308 (approx. € 1,480 to 29,624);
- Non-compliance with the data security obligations a fine between TRY 141.934 to TRY 9.463.213 (approx. € 4,443 to € 296,245);
- Non-compliance with Data Protection Authority orders / decisions: a fine between TRY 236.557 to TRY 9.463.213 (approx.€ 7,405 to 296,245); and
- Non-compliance with the Data Controllers’ Registry requirements: a fine between TRY 189.245 to TRY 9.463.213 (approx. € 5,924 to 296,245).

Further, under the Turkish Criminal Code, the following acts are subject to imprisonment:

- Persons who illegally collect personal data may be subject to imprisonment for a term of between one and three years. If the personal data is sensitive personal data, the offender may be subject to imprisonment for a term of between one and a half years to four and a half years.
- Persons who illegally transfer personal data or make personal data available to the public may be subject to imprisonment for a term of between two and four years.
- If any of the above criminal acts are committed by using the advantage or ease of a specific profession, or by a public officer using the authority given to him / her, the sanctions will be increased by 50%.
- Those responsible for the deletion of data following the expiry of the retention period, and who fail to do so, can be subject to imprisonment for a term of between one and two years.

ELECTRONIC MARKETING

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

Pursuant to the Electronic Trade Law, commercial electronic communications (electronic marketing) can only be sent by if prior consent (opt-in) has been obtained from recipients. Such consent may be obtained in writing or through means of electronic communication, although if the consent is taken in physical from, must contain the recipient's signature. Commercial electronic communications can be sent to craftsman and merchants without obtaining prior consent. The commercial electronic communication must comply with the consent obtained from recipients, and must contain the identity of the service provider, contact information (such as email, SMS, telephone number, fax number (depending on the type of commercial electronic communication)), and, if sent on behalf of a third party, information about that third party.

Pursuant to Regulation on Commercial Communication and Commercial Electronic Messages, a registry named Message Management System (“**IYS**”) is established on January 4, 2020. Pursuant to the Regulation, all entities that wish to send commercial electronic messages (SMS, E-mail or calls) must register with IYS.

Commercial electronic messages are defined as “messages sent to electronic communication addresses (including audio calls) of recipients, for the purpose of promoting or advertising a product, service or business, and / or to increase the reputation of such through content including a greeting or a wish”.

The deadline for the service providers with 150.000 or more collected opt-ins to register with the IYS was December 31, 2020. The deadline for the service providers with 149.999 or less collected opt-ins was 31.05.2021.

Failure to register the collected opt-ins to IYS will result in all opt-ins consents to be invalid.

As of registration, opt-in consents can be obtained in writing or in any other electronic medium via IYS. It is required to report opt-in consents (which were not obtained via IYS) to IYS within 3 business days as of obtaining. All opt-in consents which were not reported to IYS will be deemed invalid.

Also, recipients will be able to submit their opt-out requests via IYS. Opt-out requests (which are not received via IYS) must be reported to IYS within three (3) business days. Sending commercial electronic messages must be stopped within three (3) business days as of receiving the opt-out request of the recipient.

Please note that obtaining opt-in consent is not necessary for commercial electronic messages if it is sent to merchants and craftsmen. However, they should also be registered with IYS and, it required to be checked whether they exercise their right to opt-out.

Consumers have the right to refuse a commercial electronic communication, and the service provider is obliged to allow the free transmission of the refusal. Commercial electronic communications to the recipient must cease within three business days of the receipt of refusal. For 2024, non-compliance with opt-in requirements is subject to administrative fines up to TRY 49.943 (approx. € 1,564).

Since electronic marketing activities include more and more use of personal data, the Electronic Trade Law and the LPPD often may be implicated at the same time. The Personal Data Protection Board Decision dated October 16, 2018 numbered 2018/119 states that commercial electronic communications such as advertisement notifications and marketing telephone calls also fall within the scope of the LPPD. However, this decision raised some questions regarding the application and enforcement of the Electronic Trade Law and LPPD at the same time, especially in relation to fines which may be imposed twice both according to the LPPD and the Electronic Trade Law.

ONLINE PRIVACY

There is no legislation in Turkey that specifically regulates privacy in respect of 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. Further, various amendments were made to the Law No. 5651 on July 31, 2020. One of these amendments was adding the term “*social network provider*” and the obligations of the social network providers have been regulated within this scope.

Social network provider is defined as:

> "A natural or legal person who enables users to create, view, or share texts, images, voice, location, or other types of data for the purpose of social interaction."

The amendment requires foreign social network providers (companies that are not established in Turkey) which have daily access of 1.000.000 or more from Turkey to appoint a representative in Turkey. Also, the foreign social network providers must keep Turkish users’ (users from Turkey) personal data in Turkey within the scope of the Internet Law.

Failure to meet these requirements may result in administrative fines, limitation of bandwidth, and restriction of commercial activities (online marketing) of the social network provider. Moreover, with the recent amendments made in the Internet Law, social network providers may face an administrative fine up to 3% of their global turnover in cases of non-compliance.

Under the Regulation on Protection of Personal Data in the Electronic Communications Sector and Preservation of Privacy, an Operator cannot process traffic data for purposes other than those required for the purposes of their service. Traffic data shall be processed in accordance with the provisions of the relevant legislation for the purposes of traffic management, interconnection, billing, corruption detection and similar transactions or settlement of disputes. The processed and stored traffic data belonging to the subscriber / user shall be deleted or made anonymous after the completion of the required activity to process and store these data.

Traffic data may be processed if required for marketing electronic communication services or providing value added electronic communication services, provided that either it is anonymized, or relevant subscribers / users give their consent after being informed of the traffic data to be processed and the processing time.

Location data not qualifying as traffic data may be processed if required to provide value added electronic communication services, on the condition that it is anonymized or the relevant subscribers / users give their consent after being informed of the location data to be processed and of the purpose and duration of the processing.

Administrative fines of up to three percent of the net sales of the Operator in the previous calendar year shall be imposed if it fails to fulfill its obligation to process traffic data and location data.

KEY CONTACTS

Burak Özdağıstanli
Partner
Ozdagistanli Ekici Attorney Partnership
T +90 216 230 07 48
bozdagistanli@iptech-legal.com

Hatice Ekici Tağa
Partner
Ozdagistanli Ekici Attorney Partnership
T +90 216 230 07 48
hekici@iptech-legal.com

DATA PRIVACY TOOL

You may also be interested in our Data Privacy Scorebox to assess your organization's level of data protection maturity.