TerraLex

Turkey

Authors

Contributed by:	Erdem & Erdem Gulnur Cakmak Ergene Sevgi Ünsal Özden
Date posted:	April 21 2026
Last update:	March 11 2026

Legislation and regulations

What national laws regulate the processing of personal data in your jurisdiction?	The processing of personal data is regulated under the Law on the Protection of Personal Data No. 6698 (“LPPD”), which entered into force on April 7, 2016, together with the relevant provisions of the Turkish Constitution and the Turkish Criminal Code No. 5237 (“TCC”). In addition to the LPPD, several secondary regulations have also been enacted to provide further guidance and specificity regarding the implementation of data protection obligations. These include, the Regulation on the Deletion, Destruction or Anonymization of Personal Data; the Regulation on the Data Controllers’ Registry (“VERBIS”); the Regulation on Personal Health Data; the Regulation on the Rules and Procedures for Cross-Border Transfers; the Communiqué on the Principles and Procedures to be Followed in Fulfillment of the Obligation to Inform; the Communiqué on the Principles and Procedures on the Application to the Data Controller; decisions of the Personal Data Protection Board (“Board”); and relevant Guidelines published by the Personal Data Protection Authority (“Authority”). In addition to these main data protection legislations, there are also various sector-specific or general regulations, that while not primarily focused on data protection, include provisions governing the processing of personal data in the context of the regulated activities. These may include, for example, regulations in the fields of banking, electronic communications, labor law etc. Given the breadth of such legislation, it is not possible to exhaustively list all such regulations. It should also be noted that the LPPD was enacted based on the European Union General Data Protection Regulation (“GDPR”)’s predecessor EU Directive 95/46/EC on data protection. Although the LPPD predominantly follows the main concepts and terms in Directive 95/46/EC, there are certain differences. Furthermore, notable amendments were introduced to the provisions regarding processing of sensitive data (Article 6) and cross-border transfer (Article 9) on March 12, 2024, in accordance with the Omnibus Law published in the Official Gazette numbered 32487.
To whom do the laws apply?	The LPPD and its associated secondary legislation apply to all natural and legal persons processing personal data within

	the territory of Türkiye. It governs the processing of personal data carried out wholly or partially by automated means, or by non-automated means provided that the data form part of a data filing system. Although it is not explicitly stated in the LPPD, it is accepted that it has an extraterritorial effect. Data controllers located outside of Türkiye may fall within the scope of the LPPD if they process personal data of individuals located in Türkiye or if their processing activities have an impact in Türkiye.

Scope of protection

What type of data is covered by the law?	The LPPD provides protection for all personal data, which is defined as any information relating to an identified or identifiable natural person. This includes any data that can be used to directly or indirectly identify a person, such as name, surname, identification number, contact information, location data etc. The law also sets out additional protections for "sensitive personal data" (also referred to as "special categories of personal data"), which are considered to be more sensitive in nature and are therefore subject to stricter protection measures. These categories are explicitly defined under the LPPD, and only the data types listed therein may be regarded as sensitive personal data. Within this scope, data concerning an individual's race, ethnic origin, political opinion, philosophical belief, religion, sect or other beliefs, appearance and clothing, membership in associations, foundations or trade unions, health, sexual life, criminal convictions and security measures, as well as biometric and genetic data, are classified as sensitive personal data.
What are the main exemptions (if any)?	Following exemptions are regulated under Article 28 (1) of the LPPD: • Processing of personal data by natural persons solely for personal or household activities, provided that the data is not disclosed to third parties and data security obligations are observed. • Processing of personal data for purposes such as official statistics research, planning, and statistics, after anonymization. • Processing of personal data within the scope of freedom of expression, or for artistic, historical, literary, or scientific purposes, provided that national defense, national security, public security, public order, economic security, privacy, or personal rights are not violated and the processing does not constitute a criminal offence. • Processing of personal data by public institutions and organizations authorized by law, within the scope of preventive, protective, and intelligence activities for purposes of safeguarding national defense, national security, public security, public order, or economic security, • Processing of personal data by judicial authorities or enforcement bodies in relation to investigation, prosecution, trial, or execution proceedings. In addition, Article 28(2) of the LPPD provides for partial exemptions from certain obligations under the LPPD (such as the obligation to inform data subjects, the exercise of specific data subject rights, and the requirement to register with VERBIS). These include cases where: • Processing is necessary for the prevention of a crime or criminal investigation. • Personal data is made public by the data subject. •

	Processing is necessary for supervisory or regulatory duties carried out by authorized public bodies or professional organizations with public institution status. • Processing is required for the protection of the State's economic and financial interest in matters of budget, tax, or financial policy.
What rights do the laws grant to the data owners?	Every data subject whose personal data is processed has the right to apply to the data controller and request information regarding whether their personal data has been processed, and if so, to obtain information relating thereto. The data subject also has the right to inquire about the purpose of processing and whether the data has been used in accordance with that purpose. Furthermore, the data subject may request information about third parties to whom the data has been transferred domestically and abroad; may demand the rectification of personal data if it has been processed incompletely or inaccurately; and may request the erasure or destruction of their personal data. The data subject also has the right to request that such rectification, erasure or destruction be communicated to third parties to whom the data has been disclosed. In cases where decisions are made solely based on automated processing and such decisions produce results detrimental to the data subject; the individual has the right to object. Additionally, if the data subject suffers damages due to unlawful processing of personal data, they are entitled to claim compensation for such damages. Data subjects have also always the right to withdraw their consent for processing.

Processing requirement and main obligations

What are the lawful grounds for processing personal data or sensitive personal data (if different)?	Article 5 of the LPPD regulates the conditions under which personal data may be processed. Accordingly, personal data may be processed: • where it is explicitly prescribed by law. • where it is necessary for the protection of life or to prevent the physical injury of a person, in cases where that person cannot express consent or whose consent is legally invalid due to physical incapacities. • where it is required to process personal data that is related to the parties of the contract, provided that it is directly related to the establishment or performance of a contract. • for the fulfillment of a legal obligation. • where the data has been made manifestly public by the data subject. • where processing is necessary for the establishment, exercise, or protection of a legal right. • where it is necessary for the legitimate interests of the data controller, provided that such processing does not violate the fundamental rights and freedoms of the data subject. Furthermore, it is possible for the data controller to rely on the data subject's explicit consent, if the above-listed legal grounds are not applicable to the specific processing activity. According to Article 6 of the LPPD, sensitive personal data may be processed in the following cases: • where processing is explicitly required by law. • where processing is necessary for the protection of life or to prevent physical injury, in cases where the data subject is unable to give consent or where consent is legally invalid due to physical incapacity.

- where the data subject has made the data public, provided that the processing is in line with the data subject's intention.
- where processing is necessary for the establishment, exercise, or protection of a legal right.
- for the purposes of protecting public health, preventive medicine, medical diagnosis, treatment and care services, or the planning and management of healthcare services and their financing, by persons or authorized institutions and organizations under an obligation of confidentiality.
- where processing is necessary for the fulfillment of legal obligations in the fields of employment, occupational health and safety, social security, social services, and social assistance.
- where processing is carried out by foundations, associations, and other non-profit organizations or entities established for political, philosophical, religious, or trade union purposes, provided that it is in accordance with their applicable legislation and purposes and limited to their fields of activity.

Furthermore, it is possible for the data controller to rely on the data subject's explicit consent, if the above-listed legal grounds are not applicable to the specific processing activity.

What are the main obligations imposed by the law?

The LPPD imposes several core obligations on data controllers and data processors; however, data processors are subject only to limited and specific statutory obligations, namely (i) joint responsibility with the data controller for implementing appropriate technical and administrative measures to ensure data security, (ii) a strict and continuing statutory duty of confidentiality, under which data processors must not disclose personal data to third parties in breach of the LPPD or use such data for purposes other than the purpose of processing, and which continues even after the termination of their duties, and (iii) compliance with the safeguards, and notification requirements applicable to cross-border personal data transfers under Article 9 of the LPPD.

As regards data controllers, one of the fundamental requirements is to ensure that personal data is processed in accordance with the general principles set forth under Article 4 of the LPPD. These include lawfulness and fairness, accuracy and where necessary keeping data up to date, processing for specific, explicit and legitimate purposes, data minimization (i.e., being relevant, limited and proportionate to the purposes), and storage for no longer than necessary.

In addition to the obligation to comply with general principles, key obligations under the LPPD include:

- Informing data subjects about the processing of their personal data.
- Ensuring appropriate technical and organizational measures are taken to safeguard personal data against unlawful processing, unauthorized access, and accidental or unlawful destruction, loss, or alteration.
- Deleting, destroying, or anonymizing personal data when the processing purposes no longer exist.
- Handling and responding to data subject applications regarding their rights under the LPPD within the legal time frame.
- Registering with VERBIS and preparing a data processing inventory, unless exempt.
- Complying with the legal requirements for domestic and cross-border personal data transfers.
- Notifying both the data subject and the Board of any data breaches or unauthorized access to personal data as soon as possible.

	Data controllers must also ensure that data processing is based on at least one of the above listed legal grounds set out in the LPPD.
Do the laws establish a data retention period to be observed?	The LPPD establishes a general framework regarding the retention of personal data. According to the LPPD, personal data may only be retained for as long as it is necessary for the purposes for which it is processed. The duration of storage depends on the specific purpose of the processing, and once that purpose no longer exists, the data controller is under the obligation to delete, destroy, or anonymize the personal data. If another applicable piece of legislation (such as tax, labor, social security or commercial laws) prescribes a specific retention period, such period must be observed. However, the LPPD does not, by itself, stipulate exact retention periods; rather, it requires that personal data be retained only for the duration necessary to fulfill the relevant purpose and mandates its deletion once that purpose ceases to exist.
Must the data processing activities be recorded under the law?	Yes. Under Article 16 of the LPPD, data controllers must register with VERBIS before processing personal data, unless exempted by the Board. Additionally, data controllers that are required to register with VERBIS must prepare and maintain a Personal data processing inventory. The information to be disclosed to the Registry as part of the VERBIS registration is prepared on the basis of this inventory. The Board has issued several exemption decisions for specific categories, including data controllers processing personal data solely through non-automated means; notaries, lawyers, political parties, associations, foundations, trade unions processing within their lawful scope; customs consultants, mediators, certified and sworn-in public accountants and village legal entities. In addition, data controllers are exempt from VERBIS registration where they employ fewer than 50 employees and have an annual balance sheet total below TRY 100 million; however, where the data controller's main activity consists of processing special categories of personal data, the exemption applies only if the data controller employs fewer than 10 employees and has an annual balance sheet total below TRY 10 million. For data controllers that do not keep books on a balance sheet basis and therefore do not have an annual balance sheet total, the applicability of the exemption is assessed solely on the basis of the number of employees. Registration includes basic information about processing activities and must be kept up to date. VERBIS is a public registry maintained by the Presidency of the Authority. Importantly, exemption from registration does not mean exemption from other obligations under the LPPD.

National authority and DPO

Is there a Data Protection National Authority? If so, what is the National Authority main role?	The Authority is the supervisory and the regulatory body established in order to perform the duties stipulated by the LPPD, whereas the Board is the decision-making body of the Authority. The Authority monitors data protection practices, conducts investigations, cooperates with relevant institutions and international organizations and submits annual activity reports. The Board handles complaints, conducts ex officio investigations, sets data security standards, manages VERBIS, issues administrative sanctions, and approves the Authority's strategic and financial plans.
Does the law impose the obligation of designating a data protection officer (DPO)? If so, what is the role of the DPO under the law?	Unlike the GDPR, the LPPD does not impose a mandatory obligation to appoint a DPO. However, under the Regulation on the VERBIS, data controllers must designate a Turkish citizen

	or a legal entity established in Türkiye as a contact person or representative for VERBIS registration. This role is limited to administrative functions, such as receiving notifications from the Authority and/or Board and handling registry procedures and does not carry the independent oversight duties of a GDPR DPO. Responsibility for compliance remains with the data controller itself.

Cross-border transfers

What rules regulate the transfer of data outside your jurisdiction?	Article 9 of the LPPD and Regulation on the Rules and Procedures for Cross-Border Transfers set out specific requirements governing the cross-border transfer of personal data. Pursuant to these regulations, personal data may be transferred to a foreign country provided that one of the legal grounds for processing outlined above is present and that the foreign country, specific sectors within that country, or the international organizations to which the personal data will be transferred ensure an adequate level of data protection, as determined by an adequacy decision issued by the Board. As of the date hereof, the Board has not issued any adequacy decision permitting the cross-border transfer of personal data. In the absence of an adequacy decision, personal data may be transferred abroad by data controllers and data processors, provided that one of the conditions set out in Articles 5 or 6 is met, the data subject has the possibility to exercise their rights and access effective legal remedies in the country of transfer, and one of the appropriate safeguards listed below is ensured by the parties: • The existence of an agreement, other than an international treaty, concluded between public institutions and organizations or international organizations abroad and public institutions and organizations or professional organizations having the status of a public institution in Türkiye, and the transfer being authorized by the Board. • The existence of binding corporate rules, approved by the Board, which contain provisions on the protection of personal data and are binding on the companies within a group of undertakings engaged in joint economic activity. • The existence of a standard contract announced by the Board, containing provisions on matters such as data categories, purposes of the data transfer, recipients and recipient groups, technical and administrative measures to be implemented by the data recipient, and additional safeguards for sensitive personal data (with the execution of such standard contract to be notified to the Authority within five business days). • The existence of a written undertaking containing provisions ensuring an adequate level of protection, and the transfer being authorized by the Board. In the absence of an adequacy decision and where none of the appropriate safeguards set out above can be ensured, data controllers and data processors may transfer personal data abroad only on an occasional basis, provided that one of the following conditions is met: • The data subject has given explicit consent to the transfer, having been informed of the possible risks. • The transfer is necessary for the performance of a contract between the data subject and the data controller, or for the implementation of pre-contractual measures taken at the request of the data subject. • The transfer is necessary for the establishment or performance of a contract, to be concluded between the data

	controller and another natural or legal person, for the benefit of the data subject. • The transfer is necessary for reasons of overriding public interest. • The transfer of personal data is necessary for the establishment, exercise, or protection of legal rights. • The transfer is necessary to protect the life or physical integrity of the data subject or another person, where the data subject is unable to give consent due to physical impossibility or where consent is not legally valid. • The transfer is made from a register that is open to the public or to persons with a legitimate interest, provided that the conditions for access to such register set out in the relevant legislation are met and the transfer is requested by a person having a legitimate interest. It should be noted that any onward transfer of personal data initially transferred abroad must also comply with the LPPD. Moreover, the provisions set out in other laws regarding the transfer of personal data abroad are reserved.
Is it necessary to notify the National Authority prior to the international transfer?	Yes, depending on the legal basis for the transfer, it may be necessary either to notify the Authority or to obtain prior approval from the Board before transferring personal data abroad. Where the transfer is based on standard contracts published by the Board, the parties are required to notify the Authority within five business days of signing the contract. By contrast, agreements with foreign public bodies, international organizations, or domestic professional bodies with public authority status; binding corporate rules; and written commitments providing adequate protection are subject to the Board's prior approval. In addition, without prejudice to the provisions of international agreements, in cases where the interests of Türkiye or the data subject may be seriously harmed, cross-border data transfers may only be carried out with the permission of the Board, following the opinion of the relevant public institution or organization.

Security standards, data breaches, and sanctions

Do the laws impose any information security standards and/or requirements?	(a) General Security Obligations Under the LPPD Article 12 of the LPPD mandates that data controllers and data processors implement all necessary technical and administrative measures to prevent unlawful processing or access to personal data and to ensure its retention securely. These measures must be determined in accordance with the guidelines and regulations published by the Authority. The Personal Data Security Guide, published by the Authority, outlines examples of technical and administrative measures that data controllers and data processors may implement. These measures are not exhaustive and shall be assessed and applied by each data controller in an appropriate and proportionate manner, taking into account its organizational structure, sector, nature and scope of data processing activities, and the risks involved. By way of example, technical measures include implementing cybersecurity precautions, creating authorization processes that allow employees to access only personal data relevant to their duties, and applying data masking techniques. Additionally, data loss prevention software must be used to prevent unauthorized data transfers. As part of the administrative measures, it is necessary to identify existing risks and threats, regularly train employees on data

security, and establish internal company policies regarding the protection of personal data. The amount and retention periods of personal data must be kept to a minimum, and contracts with third-party data processors should include provisions related to data security.

Furthermore, data controllers are obligated to establish an internal personal data breach response procedure or plan, setting out the roles, responsibilities, and steps to be followed in the event of a personal data breach. Such a plan is intended to ensure the timely detection, assessment, containment, and remediation of data breaches, as well as compliance with the notification obligations towards data subjects and the Board under the LPPD.

(b) Deletion, Destruction, and Anonymization of Personal Data

The Regulation on the Deletion, Destruction, or Anonymization of Personal Data sets out the procedures and principles for securely destroying personal data. Accordingly, all data controllers are required to delete, destroy, or anonymize personal data when the purposes of processing cease to exist and to take the necessary technical and administrative measures in this respect.

In addition, data controllers that are required to register with VERBIS must prepare and implement a Personal Data Retention and Destruction Policy, which sets out the applicable retention periods and the methods and timelines for deletion, destruction, or anonymization.

(c) Security Requirements for Sensitive Personal Data

The Guide on the Processing of Sensitive Personal Data establishes the information security standards and requirements for processing such data:

- For the security of sensitive personal data, systematic, clear, manageable, and sustainable policies and procedures must be implemented. Employees involved in data processing should receive regular training, confidentiality agreements should be signed, and access rights must be clearly defined. The access durations of authorized users must be periodically reviewed, and in the event of a job change or termination, their access rights must be immediately revoked.
- Where sensitive personal data is processed, stored, and/or accessed in electronic environments, appropriate technical and organizational measures must be implemented, including the use of cryptographic methods to protect the data, the secure and separate storage of encryption keys, and the logging and secure retention of records relating to all access and processing activities.
- In addition, security updates for the relevant systems should be continuously monitored, regular security and vulnerability tests should be conducted and documented, role-based access controls should be implemented for any software used to access the data, and at least two-factor authentication should be applied where remote access to such data is required.
- Where sensitive personal data is processed, stored, and/or accessed in physical environments, appropriate physical security measures must be implemented, including safeguards against risks such as fire, flooding, electrical failure, and theft, as well as controls to prevent unauthorized physical access to such environments.
- Where sensitive personal data is transferred, appropriate security measures must be implemented depending on the transfer method, including the use of encrypted corporate email or Registered Electronic Mail (KEP) for email transfers, encryption of data stored on portable media with cryptographic keys kept separately, secure transfer mechanisms such as VPN or sFTP for server-to-server transfers, and en-

	hanced confidentiality and protection measures for transfers in paper form to prevent loss, theft, or unauthorized access. (d) Security Requirements under the Cybersecurity Law No. 7545 In addition to the data security obligations under the LPPD, information security requirements may also arise under Cybersecurity Law No. 7545. This Law establishes a general framework for the protection of information systems, critical infrastructure and cyberspace against cyber-attacks and applies broadly to public and private entities operating in or providing services through cyberspace. The Cybersecurity Directorate is empowered to require the implementation of technical and organisational cybersecurity measures, provide cyber incident response support, collect and evaluate log records, and conduct compliance audits. While the Law does not primarily regulate personal data processing, any personal data processed under its scope must comply with core data protection principles and be deleted, destroyed or anonymised once the relevant purpose ceases to exist.
Do the laws establish any kind of mandatory notification duty?	(a) General Security Obligations Under the LPPD Article 12 of the LPPD mandates that data controllers and data processors implement all necessary technical and administrative measures to prevent unlawful processing or access to personal data and to ensure its retention securely. These measures must be determined in accordance with the guidelines and regulations published by the Authority. The Personal Data Security Guide, published by the Authority, outlines examples of technical and administrative measures that data controllers and data processors may implement. These measures are not exhaustive and shall be assessed and applied by each data controller in an appropriate and proportionate manner, taking into account its organizational structure, sector, nature and scope of data processing activities, and the risks involved. By way of example, technical measures include implementing cybersecurity precautions, creating authorization processes that allow employees to access only personal data relevant to their duties, and applying data masking techniques. Additionally, data loss prevention software must be used to prevent unauthorized data transfers. As part of the administrative measures, it is necessary to identify existing risks and threats, regularly train employees on data security, and establish internal company policies regarding the protection of personal data. The amount and retention periods of personal data must be kept to a minimum, and contracts with third-party data processors should include provisions related to data security. Furthermore, data controllers are obligated to establish an internal personal data breach response procedure or plan, setting out the roles, responsibilities, and steps to be followed in the event of a personal data breach. Such a plan is intended to ensure the timely detection, assessment, containment, and remediation of data breaches, as well as compliance with the notification obligations towards data subjects and the Board under the LPPD. (b) Deletion, Destruction, and Anonymization of Personal Data The Regulation on the Deletion, Destruction, or Anonymization of Personal Data sets out the procedures and principles for securely destroying personal data. Accordingly, all data controllers are required to delete, destroy, or anonymize personal data when the purposes of processing cease to exist and to

take the necessary technical and administrative measures in this respect.

In addition, data controllers that are required to register with VERBIS must prepare and implement a Personal Data Retention and Destruction Policy, which sets out the applicable retention periods and the methods and timelines for deletion, destruction, or anonymization.

(c) Security Requirements for Sensitive Personal Data

The Guide on the Processing of Sensitive Personal Data establishes the information security standards and requirements for processing such data:

- For the security of sensitive personal data, systematic, clear, manageable, and sustainable policies and procedures must be implemented. Employees involved in data processing should receive regular training, confidentiality agreements should be signed, and access rights must be clearly defined. The access durations of authorized users must be periodically reviewed, and in the event of a job change or termination, their access rights must be immediately revoked.
- Where sensitive personal data is processed, stored, and/or accessed in electronic environments, appropriate technical and organizational measures must be implemented, including the use of cryptographic methods to protect the data, the secure and separate storage of encryption keys, and the logging and secure retention of records relating to all access and processing activities.
- In addition, security updates for the relevant systems should be continuously monitored, regular security and vulnerability tests should be conducted and documented, role-based access controls should be implemented for any software used to access the data, and at least two-factor authentication should be applied where remote access to such data is required.
- Where sensitive personal data is processed, stored, and/or accessed in physical environments, appropriate physical security measures must be implemented, including safeguards against risks such as fire, flooding, electrical failure, and theft, as well as controls to prevent unauthorized physical access to such environments.
- Where sensitive personal data is transferred, appropriate security measures must be implemented depending on the transfer method, including the use of encrypted corporate email or Registered Electronic Mail (KEP) for email transfers, encryption of data stored on portable media with cryptographic keys kept separately, secure transfer mechanisms such as VPN or sFTP for server-to-server transfers, and enhanced confidentiality and protection measures for transfers in paper form to prevent loss, theft, or unauthorized access.

(d) Security Requirements under the Cybersecurity Law No. 7545

In addition to the data security obligations under the LPPD, information security requirements may also arise under Cybersecurity Law No. 7545. This Law establishes a general framework for the protection of information systems, critical infrastructure and cyberspace against cyber-attacks and applies broadly to public and private entities operating in or providing services through cyberspace.

The Cybersecurity Directorate is empowered to require the implementation of technical and organisational cybersecurity measures, provide cyber incident response support, collect and evaluate log records, and conduct compliance audits. While the Law does not primarily regulate personal data processing, any personal data processed under its scope must comply with core data protection principles and be deleted, destroyed or anonymised once the relevant purpose ceases to exist.

What are the sanctions for noncompliance with data protection laws?	In cases of non-compliance with data protection laws under the LPPD, both criminal and administrative sanctions may be imposed. Administrative fines are imposed on data controllers pursuant to Article 18 of the LPPD and are updated anually. As of 2026, the following administrative fines apply to data controllers: • TRY 85,437 to TRY 1,709,200 for failure to fulfil the obligation to inform data subjects • TRY 256,357 to TRY 17,092,242 for failure to implement the technical and administrative measures required to ensure personal data security • TRY 427,263 to TRY 17,092,242 for failure to comply with the decisions of the Board • TRY 341,809 to TRY 17,092,242 for failure to comply with registration and notification obligations with VERBIS • TRY 90,308 to TRY 1,806,177 for failure to fulfil the personal data breach notification obligation In addition, in the event of a failure to notify the Authority of the execution of standard contracts for cross-border data transfers, administrative fines may also be imposed directly on data processors, in accordance with Article 18(2) of the LPPD. Civil remedies are also available for data subjects whose rights have been infringed, including compensation claims based on general tort principles.

Other comments

Other comments	—