

PANORAMIC

DATA PROTECTION & PRIVACY

Türkiye

LEXOLOGY

Data Protection & Privacy

Contributing Editors

Aaron P Simpson and Lisa J Sotto

Hunton Andrews Kurth LLP

Generated on: September 15, 2026

The information contained in this report is indicative only. Law Business Research is not responsible for any actions (or lack thereof) taken as a result of relying on or in any way using information contained in this report and in no event shall be liable for any damages resulting from reliance on or use of this information. Copyright 2006 - 2026 Law Business Research

Contents

Data Protection & Privacy

LAW AND THE REGULATORY AUTHORITY

- Legislative framework
- Data protection authority
- Cooperation with other data protection authorities
- Breaches of data protection law
- Judicial review of data protection authority orders

SCOPE

- Covered uses of PI
- Exempt sectors and institutions
- Interception of communications and surveillance laws
- Other laws
- PI formats
- Extraterritoriality

LEGITIMATE PROCESSING OF PI

- Legitimate processing – grounds
- Legitimate processing – types of PI

DATA HANDLING RESPONSIBILITIES OF OWNERS OF PI

- Transparency
- Exemptions from transparency obligations
- Data accuracy
- Data minimisation and purpose limitation
- Data retention

SECURITY

- Security obligations
- Notification of data breach

INTERNAL CONTROLS

- Accountability
- Data protection officer
- Record-keeping
- Risk assessment
- Design of PI processing systems

REGISTRATION AND NOTIFICATION

- Registration

Other transparency duties

SHARING AND CROSS-BORDER TRANSFERS OF PI

Sharing of PI with processors and service providers

Restrictions on third-party disclosure

Cross-border transfer

Further transfer

Localisation

RIGHTS OF INDIVIDUALS

Access

Other rights

Compensation

Enforcement

EXEMPTIONS, DEROGATIONS AND RESTRICTIONS

Further exemptions and restrictions

SPECIFIC DATA PROCESSING

Cookies and similar technology

Electronic communications marketing

Targeted advertising

Children's data

Age verification

Sensitive personal information

Profiling

Automated decision-making

Cloud services

UPDATE AND TRENDS

Key trends and future developments

Contributors

Türkiye

YAZICIOGLU Legal

YAZICIOGLU
LEGAL

Bora Yazicioglu

bora@yazicioglullegal.com

Nafiye Yucedag

nafiye@yazicioglullegal.com

Devrim Ece Eksioglu

ece@yazicioglullegal.com

Cagatay Efe Tatar

cagatay@yazicioglullegal.com

Serife Amine Mumin

serife@yazicioglullegal.com

LAW AND THE REGULATORY AUTHORITY

Legislative framework

Summarise the legislative framework for the protection of personal information (PI). Does your jurisdiction have a dedicated data protection law? Is the data protection law in your jurisdiction based on any international instruments or laws of other jurisdictions on privacy or data protection?

The protection of personal information (PI) is governed by multiple laws in Türkiye. The right to the protection of PI was explicitly recognised as a fundamental individual right through a 2010 amendment to the Constitution of the Republic of Türkiye.

The first comprehensive legislation in this area is the Personal Data Protection Law No. 6698 (DP Law) which came into force in 2016. The DP Law sets out the main principles and rules for processing PI and its implementation is further supported by secondary regulations and guidelines issued by the Turkish Data Protection Authority (DPA). While the DP Law was initially modelled on the EU Directive 95/46/EC, ongoing efforts aim to bring it in line with the standards set by the EU General Data Protection Regulation (GDPR).

In addition, certain violations of PI protection are classified as criminal offences under the Turkish Criminal Code (TCrC). PI is also considered part of personality rights under Turkish law and is thus protected under the Turkish Civil Code (TCiC).

Lastly, the Cybersecurity Law, which entered into force on 19 March 2025, establishes a comprehensive cybersecurity framework in Türkiye and introduces a centralised structure previously governed by dispersed and sector-specific rules. It also relates to the protection of PI through cybersecurity obligations and incident reporting, with sanctions for non-compliance.

Sector-specific regulations also govern the processing of PI in fields such as telecommunications, banking, electronic payments, health and education.

Law stated - 11 June 2026

Data protection authority

Which authority is responsible for overseeing the data protection law?
What is the extent of its investigative powers?

The primary supervisory and regulatory authority in Türkiye is the DPA. It is authorised to initiate investigations either upon receiving a complaint from a data subject or *ex officio* if it becomes aware of the alleged violation.

The DPA may request information or documents from controllers – who must respond within 15 days unless the information constitutes a state secret – during its investigations and may also require additional documents or conduct on-site audits.

Law stated - 11 June 2026

Cooperation with other data protection authorities

Are there legal obligations on the data protection authority to cooperate with other data protection authorities, or is there a mechanism to resolve different approaches?

Although no specific mechanism exists, the DPA may monitor international developments and cooperate with international organisations.

Law stated - 11 June 2026

Breaches of data protection law

Can breaches of data protection law lead to administrative sanctions or orders, or criminal penalties? How would such breaches be handled?

If the DPA finds a violation of the DP Law, whether following a data subject complaint, or *ex officio* it may impose administrative fines ranging from 85,437 to 17,092,242 Turkish lira – adjusted annually – based on the type of the violation.

The DPA may also order controllers to bring processing activities in compliance with the DP Law, with such instructions to be fulfilled without delay and no later than 30 days from the notification. It is entitled to suspend PI processing or transfers abroad if it finds that such activities may result in damages which are difficult or impossible to remedy and are clearly unlawful.

In addition, criminal penalties are prescribed under the TCrC for unlawful recording of PI, unlawful transfer, publication, or acquisition of PI, and failure to destroy PI after the retention period set forth in the law has passed. Such criminal investigations may be initiated *ex officio* by public prosecutors without requiring a complaint, though how these sanctions align with the DP Law remains unclear in practice.

Law stated - 11 June 2026

Judicial review of data protection authority orders

Can PI owners appeal to the courts against orders of the data protection authority?

Controllers may challenge DPA decisions before the administrative court within 60 days of notification. If the fine exceeds a certain threshold, further appeals may be made to the Regional Administrative Court and, under certain conditions, to the Council of State. If the decision only involves an administrative measure, both appeal avenues remain available regardless of the fine amount.

Law stated - 11 June 2026

SCOPE

Covered uses of PI

Is all processing or use of PI covered? Is a distinction made between those who control or own PI and those who provide PI processing services to owners? Do owners', controllers' and processors' duties differ?

The Personal Data Protection Law No. 6698 (DP Law) covers all processing of PI, regardless of the context or purpose. However, it distinguishes between controllers and processors when determining applicable obligations.

Controllers bear primary responsibility for ensuring compliance with the DP Law while processors are mainly required to follow controllers' instructions, implement appropriate security measures, and assist controllers in fulfilling their legal obligations. Thus, although both controllers and processors have duties under the DP Law, controllers hold a broader scope of responsibility.

Law stated - 11 June 2026

Exempt sectors and institutions

Does the data protection law cover all sectors and types of organisation, or are some sectors or institutions outside its scope?

The DP Law applies broadly to all sectors and types of organisations. However, there are limited exemptions under the DP Law, which include processing;

- by natural persons for purely personal or household activities, provided that PI is not disclosed to third parties and security obligations are met;
- of anonymised data for official statistics;
- of PI for artistic, historical, literary, or scientific purposes, or within the framework of freedom of expression, provided it does not violate national defence, national security, public security, public order, economic security, privacy rights, or personal rights, and does not constitute a crime;
- for preventive, protective, and intelligence activities by public institutions authorised by law to maintain national defence, national security, public security, public order, or economic security; and
- of PI by judicial or execution authorities for investigation, prosecution, or judicial proceedings.

The DP Law also outlines certain cases exempt from some of its obligations.

Law stated - 11 June 2026

Interception of communications and surveillance laws

Does the data protection law cover interception of communications, electronic marketing or monitoring and surveillance of individuals?

The DP Law applies if PI processing is involved. Accordingly, such activities must comply with the general principles and legal bases set out under the DP Law, including requirements on transparency, proportionality, and data minimisation.

In this context, the DPA has taken the view that the use of biometric systems such as facial recognition may constitute a disproportionate interference where less intrusive methods are available to achieve that aim, and that while the use of security cameras may be permissible, their scope and placement must be carefully determined so as not to infringe individuals' reasonable expectation of privacy.

Law stated - 11 June 2026

Other laws

Are there any further laws or regulations that provide specific data protection rules for related areas?

Several laws and regulations in Türkiye provide specific PI protection rules in related areas.

Voice calls and text messages are protected under the constitutional rights to privacy and freedom of communication. TCrC includes specific offences safeguarding communication secrecy and private life. Only under very limited circumstances, and by a judge's or public prosecutor's decision in the cases of peril in delay, is intervention in private communication permitted.

Electronic marketing is primarily regulated by the Law on Regulation of Electronic Commerce and the By-Law on Commercial Communication and Commercial Electronic Messages (together E-Commerce Legislation), which requires prior consent for commercial electronic messages (CEM) to protect individuals from unsolicited contact.

Various sector-specific laws regulate monitoring practices, particularly in employment contexts. For example, the Turkish Labour Law imposes limits on employer monitoring to safeguard employees' privacy rights. In addition, the Regulation on Processing of Personal Health Data sets out specific rules governing the processing, access, and security of personal health data.

Law stated - 11 June 2026

PI formats

What categories and types of PI are covered by the law?

The DP Law defines any information relating to an identified or identifiable natural person as PI.

Certain types of PI are classified as special categories due to their sensitive nature and receive enhanced protection. Special categories of PI are specified as an exhaustive list that includes race, ethnic origin, political opinions, philosophical beliefs, religion, religious sect or other beliefs, appearance and dress, membership in associations, foundations, or trade unions, health sexual life, criminal convictions, security measures, as well as biometric and genetic PI.

Extraterritoriality

Is the reach of the law limited to PI owners and processors physically established or operating in your jurisdiction, or does the law have extraterritorial effect?

While the DP Law is silent on territorial scope, as a general rule regarding the territoriality principle, it applies to controllers and processors established in Türkiye.

However, in its Guidelines on the Transfer of Personal Data Abroad (Guidelines on Transfers Abroad), the DPA emphasises that the enforcement of territorial scope is linked to the general principles of Misdemeanour Law and the rules set forth in the TCrC. This implies that if the behaviour or its effects occur in Türkiye, the DP Law will be applicable.

That said, due to the cross-border nature of PI processing, the DPA considers strict territorial application insufficient to effectively protect individuals' rights and applies the 'effect principle', extending the scope of the DP Law to situations where PI processing affects individuals in Türkiye, regardless of whether the processing takes place in Türkiye.

Law stated - 11 June 2026

LEGITIMATE PROCESSING OF PI**Legitimate processing – grounds**

Does the law require that the processing of PI be legitimised on specific grounds, for example to meet the owner's legal obligations or if the individual has provided consent?

Personal information (PI) may be processed under article 5 of the Personal Data Protection Law No. 6698 (DP Law) where one of the following legal bases exists; the data subject's explicit consent, the necessity for the performance or conclusion of a contract, compliance with a legal obligation, the protection of vital interests, the data being made public by the data subject, or the existence of a legitimate interest, provided that it does not harm the fundamental rights and freedoms of the data subject.

The Data Protection Authority (DPA) considers that reliance on explicit consent as a legal ground is unfair where another valid legal ground for processing is available.

Law stated - 11 June 2026

Legitimate processing – types of PI

Does the law impose more stringent rules for processing specific categories and types of PI?

The DP Law establishes more stringent legal bases for processing special categories of PI as outlined in article 6.

Additionally, specific technical and administrative measures are required by the DPA to ensure adequate protection. These requirements were highlighted in a 2018 DPA decision and further elaborated through DPA guidelines, including those on biometric and genetic data.

Recently, in February 2025, the DPA published the Guideline on the Processing of Special Categories of Data (Special Categories Data Guideline), which primarily emphasises the scope of special categories of PI, provides interpretative guidance on the applicable legal bases, and outlines compliance requirements with the DP Law, including those introduced by the 2024 amendments to the DP Law.

Law stated - 11 June 2026

DATA HANDLING RESPONSIBILITIES OF OWNERS OF PI

Transparency

Does the law require owners of PI to provide information to individuals about how they process PI? What must the notice contain and when must it be provided?

Controllers are required to inform data subjects of the processing of their personal information (PI).

Privacy notices must, at least, include the following, per the Communiqué on Principles and Procedures to Be followed in Fulfilment of the Obligation to Inform;

- identity of the controller and its representative (if any);
- purposes for which PI will be processed;
- persons to whom PI will be transferred and the purpose of such transfer;
- method and legal basis for collecting PI; and
- data subjects' rights

According to the Communiqué, data subjects shall be informed by controllers, or a party authorised by them, at the time PI is obtained. Where PI is not collected directly from the data subject, the obligation to inform must be fulfilled:

- within a reasonable period after obtaining PI;
- at the first instance of communication if PI is used to contact the data subject; or
- at the time of the first transfer of PI at the latest, if PI is to be transferred.

The Data Protection Authority (DPA) is particularly strict regarding explicit consent. In fact, in its resolution dated 18 February 2026 on the requirement for separate preparation of consent and information notices, the DPA held that, due to the distinct legal nature of the obligation to inform and explicit consent, these texts must be prepared separately.

Law stated - 11 June 2026

Exemptions from transparency obligations

When is notice not required?

Subject to compliance with the purpose and fundamental principles of the Personal Data Protection Law No. 6698 (DP Law), and the requirement of proportionality, notification to the data subject is not required in the following 'exceptional cases';

- when necessary for a criminal investigation or the prevention of crime;
- when PI is made public by the data subject;
- when necessary for the execution of supervisory or regulatory duties and for disciplinary investigation or prosecution by authorised public institutions and organisations and professional organisations with public institution status, based on the authority granted by law; and
- when necessary to protect the state's economic and financial interests in budget, tax, or financial matters.

Law stated - 11 June 2026

Data accuracy

Does the law impose standards in relation to the quality, currency and accuracy of PI?

PI must be processed lawfully and fairly and kept accurate and up to date when necessary.

Law stated - 11 June 2026

Data minimisation and purpose limitation

Does the law restrict the types or volume of PI that may be collected?

Collected PI must be relevant, limited, and proportionate to the intended purpose. PI must be collected for specific, explicit, and legitimate purposes and must not be processed in a manner incompatible with those.

Law stated - 11 June 2026

Data retention

Does the law restrict the amount of PI that may be held or the length of time for which PI may be held?

The DP Law does not set specific limits on the amount or duration of PI retention. However, it requires that PI be relevant, limited, and proportionate to the processing purpose and retained only for the period required by the relevant legislation or necessary to fulfil that purpose.

Law stated - 11 June 2026

SECURITY

Security obligations

What security obligations are imposed on PI owners and service providers that process PI on their behalf?

Controllers are required to implement necessary measures to prevent unlawful processing of personal information (PI) and unauthorised access, and to maintain their safekeeping, thereby ensuring data security. They must also conduct necessary audits within their organisation to ensure compliance. A controller's accountability also extends to processing activities conducted by its processors, as controllers hold joint responsibility for ensuring that processors implement appropriate measures when processing PI on their behalf.

While the Personal Data Protection Law No. 6698 (DP Law) does not mandate a specific set of measures, the Data Protection Authority (DPA) emphasises key safeguards in its Personal Data Security Guideline (PI Security Guideline), which is further supplemented by the Special Categories Data Guideline for the processing of special categories of PI and relevant DPA decisions.

Law stated - 11 June 2026

Notification of data breach

Does the law include (general or sector-specific) obligations to notify the supervisory authority or individuals of data breaches? If breach notification is not required by law, is it recommended by the supervisory authority?

Unlike the General Data Protection Regulation (GDPR), the DP Law requires controllers to notify the DPA of all data breaches, regardless of whether the breach poses a risk to the rights and freedoms of natural persons. Notification must be made to the DPA within 72 hours of the controller becoming aware of the incident. Additionally, affected data subjects must be informed without undue delay. The DPA may, if necessary, also publish the data breach on its website for a period limited to 60 days, or through other appropriate means.

The Cybersecurity Law also requires those who provide services, collect data, process data, or conduct similar activities using information systems to promptly notify the Cybersecurity Presidency of any vulnerabilities or cyber incidents. Therefore, when controllers experience a personal data breach, it will likely also be notified to the Cybersecurity Presidency.

Law stated - 11 June 2026

INTERNAL CONTROLS

Accountability

Are owners or processors of PI required to implement internal controls to ensure that they are responsible and accountable for the PI that they collect and use, and to demonstrate compliance with the law?

All controllers must be able to demonstrate their compliance with the Personal Data Protection Law No. 6698 (DP Law) in the event of an investigation or an information request by the Data Protection Authority (DPA).

The DP Law mandates all controllers to conduct internal audits to ensure compliance. Additionally, in accordance with the DPA decisions, controllers are expected to maintain procedures for responding to data breaches and adopt a policy for processing special categories of PI.

Controllers meeting certain criteria must register online with the publicly accessible Data Controllers' Registry (VERBIS), ensuring transparency by documenting their processing activities. VERBIS-registered controllers must also maintain a personal information (PI) inventory and implement a retention and destruction policy.

While controllers bear primary responsibility for compliance, the duty to comply also extends to their processors. To this end, the DPA's PI Security Guideline recommends that controllers execute written data processing agreements with processors and periodically audit them, including on-site inspections where appropriate.

Law stated - 11 June 2026

Data protection officer

Is the appointment of a data protection officer mandatory? What are the data protection officer's legal responsibilities? Are there any criteria that a person must satisfy to act as a data protection officer?

There is no requirement to appoint a data protection officer.

Law stated - 11 June 2026

Record-keeping

Are owners or processors of PI required to maintain any internal records relating to the PI they hold?

Controllers required to register with VERBIS must also maintain a PI Inventory detailing their processing activities in line with the By-Law on Data Controllers' Registry.

Law stated - 11 June 2026

Risk assessment

Are owners or processors of PI required to carry out a risk assessment in relation to certain uses of PI?

Data protection risk assessments are not specifically regulated but may be considered a measure that controllers should implement as per the DPA's guidelines. For example, the Generative AI Guideline states that, although not mandated under DP Law, it would be beneficial to carry out a data protection impact assessment in relation to processing

activities involving generative AI systems and models that may produce significant consequences for individuals' lives, particularly when balancing interests in cases of legitimate interest-based processing.

Law stated - 11 June 2026

Design of PI processing systems

Are there any obligations in relation to how PI processing systems must be designed?

Unlike the GDPR, the DP Law does not include the concepts of 'privacy by design' or 'privacy by default'. However, per the DPA's decisions and guidelines, controllers are required to apply such concepts to comply with the DP Law, particularly with the general principles and PI-processing conditions it sets forth.

Law stated - 11 June 2026

REGISTRATION AND NOTIFICATION

Registration

Are PI owners or processors of PI required to register with the supervisory authority? Are there any exemptions? What are the formalities for registration and penalties for failure to do so?

Controllers in Türkiye – subject to certain criteria – are required to register with VERBIS. For foreign controllers, however, it remains unclear whether the registration requirement applies to all of them or only to those that engage in personal information (PI) processing activities in Türkiye directly or through their branches. Given this uncertainty, it may be prudent for all foreign data controllers to register with VERBIS until the issue is further clarified. Processors, on the other hand, are not subject to this obligation.

The Data Protection Authority (DPA) may grant exemptions and has done so for specific professions and sectors. Controllers in Türkiye are exempt if they:

- have fewer than 50 employees and an annual financial balance sheet total below 100 million Turkish lira, provided their core activity does not involve processing special categories of PI; or
- have fewer than 10 employees and an annual balance sheet below 10 million Turkish lira, whose main activity consists of processing special of PI (categories as of 2026). Exemptions also apply in 'exceptional cases'.

As of 2026, non-compliance with VERBIS obligations may result in administrative fines ranging from 341,809 to 17,092,242 Turkish lira, subject to annual adjustment.

Law stated - 11 June 2026

Other transparency duties

| Are there any other public transparency duties?

There are no additional obligations beyond those outlined above. However, the DPA also publishes data breach notifications and summaries of certain decisions on its website to enhance transparency.

Law stated - 11 June 2026

SHARING AND CROSS-BORDER TRANSFERS OF PI

| **Sharing of PI with processors and service providers**

How does the law regulate the sharing of PI with entities that provide outsourced processing services?

There are no specific rules for outsourced processing services; the sharing of personal information (PI) with such entities is subject to the general provisions under article 8 of the Personal Data Protection Law No. 6698 (DP Law). However, specific provisions under other laws are reserved.

Law stated - 11 June 2026

| **Restrictions on third-party disclosure**

Are there any specific restrictions on the sharing of PI with recipients that are not processors or service providers?

There are no specific restrictions based on the recipient's status. Instead, the DP Law distinguishes between domestic and international data transfers. Accordingly, general provisions apply to all recipients.

Law stated - 11 June 2026

| **Cross-border transfer**

Is the transfer of PI outside the jurisdiction restricted?

The DP Law provides for a gradual regime for cross-border transfers, comprising three levels:

- adequacy decisions;
- appropriate safeguards; and
- occasional causes.

The Data Protection Authority (DPA) is authorised to issue adequacy decisions for countries, specific sectors and international organisations. However, no adequacy decisions have been issued to date.

In the absence of such a decision, PI transfers may still proceed if appropriate safeguards are implemented and data subjects are able to exercise their rights and access effective legal remedies in the recipient country. Appropriate safeguards include the following:

- agreements between foreign and Turkish public institutions or international organisations;
- binding corporate rules;
- standard contracts; and
- written undertakings.

If no adequacy decision exists and appropriate safeguards cannot be ensured, PI transfers may still occur if they are occasional and one of the conditions set out in the DP Law is met. Furthermore, in contrast to the GDPR, the DP Law requires that standard contracts be notified to the DPA within five business days following their execution. In addition, standard contracts must also be executed with wet signatures.

Law stated - 11 June 2026

Further transfer

If transfers outside the jurisdiction are subject to restriction or authorisation, do these apply equally to transfers to service providers and onwards transfers?

Since the DP Law does not distinguish between service providers and other recipients, general PI transfer rules apply. It also explicitly states that international transfer requirements extend to onward transfers by both controllers and processors.

Law stated - 11 June 2026

Localisation

Does the law require PI or a copy of PI to be retained in your jurisdiction, notwithstanding that it is transferred or accessed from outside the jurisdiction?

While the DP Law does not mandate PI retention within Türkiye, sector-specific rules impose local data storage obligations as follows:

- Banking and finance entities such as banks, insurers, capital markets institutions and leasing or factoring companies must keep their primary and secondary IT systems within Türkiye.
- Electronic communications providers are, in principle, prohibited from transferring traffic and location data abroad unless they obtain explicit consent from users in certain cases.
- eSIM-technologies-related infrastructure, systems, and storage units, as well as data generated through eSIM technologies, must be stored in Türkiye.
- Ministry of Trade authorisation is required for Message Management System integrators and all systems (software, hardware, servers) used by integrators must be hosted within Türkiye.
-

Critical infrastructure service providers must retain their primary and backup data systems within Türkiye.

- Public institutions and organisations are required to store critical data within Türkiye. Additionally, they must not store data in cloud services unless it is hosted on their own infrastructure or by local service providers under their control.

Furthermore, social network providers with daily access exceeding one million are required to take necessary measures to store Turkish user PI within Türkiye.

Law stated - 11 June 2026

RIGHTS OF INDIVIDUALS

Access

Do individuals have the right to access their personal information held by PI owners? Describe how this right can be exercised as well as any limitations to this right.

Individuals have the right to

- learn whether their personal information (PI) is being processed;
- request information about PI processing;
- learn the purposes of processing and whether their PI is being used for those purposes; and
- know the third parties to whom their PI is transferred, which falls within the scope of the right of access.

To exercise their rights, data subjects may submit their requests in writing or via other methods designated by the Data Protection Authority (DPA) in accordance with the Communiqué on the Principles and Procedures for Requests to Data Controllers. The Communiqué requires that requests include at a minimum:

- name and surname (and signature if submitted in writing);
- Turkish ID number for citizens, or nationality and passport or ID number for foreigners;
- residential or workplace address for notifications;
- if available, email address, telephone and fax number; and
- the subject of the request.

The Personal Data Protection Law No. 6698 (DP Law) also provides that data subject rights, including the right of access, do not apply in “exceptional cases”.

Law stated - 11 June 2026

Other rights

Do individuals have other substantive rights?

In addition to the above-mentioned rights, data subjects have the right to request the following;

- rectification of incomplete or inaccurate PI;
- erasure or destruction of PI;
- that rectification, erasure or destruction of their PI be notified to third parties to whom their PI has been transferred;
- object if an analysis carried out through solely automated systems results in a decision that adversely affects them; and
- to claim compensation for damage arising from unlawful processing.

Law stated - 11 June 2026

Compensation

Are individuals entitled to monetary damages or compensation if they are affected by breaches of the law? Is actual damage required or is injury to feelings sufficient?

Individuals whose personal rights have been violated are entitled to seek compensation under the general provisions of Turkish law.

Specifically, the TCiC provisions protecting personality rights and the liability principles under the Turkish Code of Obligations apply in such cases. Unlawful processing of PI may constitute a violation of an individual's personality rights, entitling them to claim both material and non-material damages.

If a data subject suffers material damage as a result of the unlawful processing of their personal data, they may claim compensation for that damage.

Where the breach results also in emotional distress, reputational harm, or a violation of dignity, individuals may still be entitled to compensation for the non-material damage suffered. This principle is further supported by decisions from the Turkish Supreme Court, which have recognised moral compensation claims arising from unlawful acquisition or processing of PI. For example, in a recent decision of the Turkish Supreme Court, the Court held that a bank, as a data controller, breached the principles of purpose limitation and data minimisation by disclosing excessive account movements that exceeded the specific timeframe requested by the Court and found that this unlawful disclosure violated the data subject's rights, ultimately awarding the compensation of immaterial damages.

Law stated - 11 June 2026

Enforcement

Are these rights exercisable through the judicial system or enforced by the supervisory authority or both?

Data subjects may submit requests to controllers to exercise their rights. Controllers are required to respond to such requests promptly and no later than 30 days. If the request

is rejected, the response is insufficient, or no response is provided within this period, data subjects may file a complaint with the DPA within 30 days of receiving the response or within 60 days from the date of their original request.

However, although the DPA may investigate complaints and impose administrative sanctions, including fines, on data controllers, it has no authority to award compensation. Individuals seeking compensation for violations of their personal rights must pursue their claims through the general courts. In addition, data subjects whose personality rights have been violated may also bring actions before the courts for the prevention, determination and cessation of unlawful conduct.

Law stated - 11 June 2026

EXEMPTIONS, DEROGATIONS AND RESTRICTIONS

Further exemptions and restrictions

Does the law include any derogations, exclusions or limitations other than those already described?

In addition to the exemptions outlined above, the Personal Data Protection Law No. 6698 (DP Law) preserves the application of specific provisions set out in other laws. In particular, while articles 8 and 9 of the DP Law regulate the transfer of personal data domestically and internationally, they are subject to any exceptions provided under other laws.

Also, the erasure, destruction and anonymisation of personal information may also be subject to exceptions set out in other laws.

Law stated - 11 June 2026

SPECIFIC DATA PROCESSING

Cookies and similar technology

Are there any rules on the use of 'cookies' or equivalent technology?

Under Turkish law, no specific legislation governs cookies, except for limited provisions in the Electronic Communications Law (ECL), which apply to electronic communications service providers. The ECL allows the use of cookies either for communication purposes or where users are informed and have given explicit consent.

When controllers process PI via cookies or similar technologies, the Personal Data Protection Law No. 6698 (DP Law) applies. To enhance clarity, the Data Protection Authority (DPA) issued its Guidelines on Cookie Applications in 2022, providing recommendations for the use of cookies and later updated these guidelines in July 2025.

The guidelines primarily outline that controllers must fulfil privacy notice requirements when informing data subjects about cookies and rely on the legal bases under the DP Law. It also recommends including information on the cookies' name, purpose, duration, and whether it is first-party or third-party in the privacy notices and provides a compliance checklist with best practice examples, such as banner usage, cookie preference management, and a sample cookie policy.

Law stated - 11 June 2026

Electronic communications marketing

Are there any rules on marketing by email, fax, telephone or other electronic channels?

In Türkiye, online marketing is regulated mainly by the E-Commerce Legislation and the DP Law.

The E-Commerce Legislation requires marketers to obtain prior approval from recipients before making marketing calls or sending commercial electronic messages (CEMs). This approval is a specific authorisation and is separate from the explicit consent required under the DP Law for processing PI for marketing. Also, in a resolution, DPA underlines that explicit consent for the CEMs should not be presented as a condition for the provision of goods or services; accordingly consent should be obtained after the transaction or it should be clearly stated that giving consent is optional and preferences can be changed at any time..

The E-Commerce Legislation exempts CEMs sent to tradespeople or artisans in a business-to-business context from the approval requirement, though recipients must be given the option to opt out. CEMs must include specific sender identification details and provide an option to opt out. All senders are required to register with the Message Management system (MMS) and upload records of approvals and withdrawals. Any approval or withdrawal received must be uploaded to the MMS within three business days.

Although the Ministry of Commerce, which oversees compliance with the E-Commerce Legislation, does not classify push notifications as CEMs, the DPA requires explicit consent from data subjects before sending push notifications.

In an announcement, the DPA also emphasised that data subjects must be provided with the ability to customise the types of push notifications they wish to receive, such as distinguishing between informational and marketing notifications, through in-app settings or the device's operating system settings.

Law stated - 11 June 2026

Targeted advertising

Are there any rules on targeted online advertising?

Turkish law does not contain specific rules for targeted online advertising; general provisions of the DP Law apply and, in principle, prior explicit consent from data subjects is typically required for targeted advertising.

Law stated - 11 June 2026

Children's data

Are there any specific rules relating to the use of children's PI?

The use of children's PI remains a priority for relevant institutions and regulatory authorities, including the DPA.

In this respect, the DPA has issued certain decisions providing guidance on how children's PI should be approached.

The DPA has also recently announced that it has initiated an *ex officio* investigation into several social media platforms to examine how children's PI are processed and what safeguards are implemented.

Alongside these, the law titled 'Law Amending the Social Services Law and Certain Other Laws', recently adopted by the Turkish Grand National Assembly (GNAT) and expected to enter into force by the end of 2026, introduces stricter obligations for the protection of children in the digital environment. These include a prohibition on providing services to children under the age of 15 and requirements to implement age verification and tailored content moderation measures for users aged 15 and above.

Law stated - 11 June 2026

Age verification

Are there any specific rules relating to the use of PI for age verification purposes online?

'Law Amending the Social Services Law and Certain Other Laws', recently adopted by the Grand National Assembly of Turkey (GNAT), introduces a ban on access to social media platforms for children under the age of 15 and imposes an obligation on social network providers to implement all necessary technical and administrative measures, including age verification mechanisms, to enforce this restriction.

While the law does not explicitly regulate which types of PI may be used or how such data may be processed for age verification purposes, it provides that the relevant principles governing the implementation of the relevant provision will be determined by the Information and Communication Technologies Authority (ICTA), indicating that more detailed rules may be introduced by the ICTA in the future.

Law stated - 11 June 2026

Sensitive personal information

Are there any rules on the processing of 'sensitive' categories of personal information?

Processing special categories of PI is prohibited under the DP Law except for the legal bases set out in article 6 of the DP Law. Although explicit consent is one legal basis, controllers should not rely on it if other bases apply.

The DPA's Special Categories Data Guideline explains how these legal bases are interpreted by providing practical examples and outlines the scope and definitions of special categories of PI, as well as outlining the additional measures that controllers processing such data

must implement. The DPA has also issued specific guidelines on certain special categories, including biometric and genetic data.

Law stated - 11 June 2026

Profiling

Are there any rules regarding the use of PI for individual profiling?

Turkish law does not contain specific provisions on profiling, general provisions of the DP Law apply. In line with the DPA's approach, explicit consent from data subjects is typically required for profiling.

Law stated - 11 June 2026

Automated decision-making

Does the law restrict the use of PI in automated decision making that affects individuals without human intervention?

No, it is not specifically restricted. However, data subjects have the right to object if an analysis carried out through solely automated systems results in a decision that adversely affects them.

In addition, in its Generative AI Guideline, the DPA has emphasised the importance of ensuring that, where generative AI systems are used in decision-making processes, the right to object serves not only to challenge the reasoning behind decisions, but also to ensure that such processes remain transparent, accountable, and open to human intervention where necessary.

Law stated - 11 June 2026

Cloud services

Are there any rules or regulator guidance on the use of cloud computing services?

Türkiye lacks a dedicated legal framework specifically regulating cloud computing; instead, a fragmented set of general and sector-specific rules applies. Since cloud computing often involves the processing of PI, the legal framework for the protection of PI generally applies to cloud computing services.

Certain laws, particularly in sectors such as banking, payment services, and electronic money institutions, include confidentiality obligations that may restrict transfers to cloud environments or between cloud systems, allowing disclosure only to authorised entities. In addition, sector-specific regulations also set requirements for cloud users and providers, including strict data localisation rules.

From a PI protection standpoint, general technical and administrative requirements apply to cloud services, with the DPA prescribing specific safeguards.

UPDATE AND TRENDS

Key trends and future developments

Are there any emerging trends or hot topics in data protection in your jurisdiction, and are there any proposed changes to the current legislation?

Following the new cross-border transfer regime introduced through amendments which was introduced in 2024 to the Personal Data Protection Law No. 6698 applies. To enhance clarity, the Turkish Data Protection Authority (DPA) has taken steps to clarify the recently amended international data transfer regime through the Guidelines on Transfers Abroad and its announcement on key considerations for standard contracts.

While these amendments have aligned the Turkish data protection framework more closely with the General Data Protection Regulation (GDPR), the '2026 Presidential Annual Programme' indicates that full harmonisation with the GDPR is planned to be completed by the third quarter of 2026.

Moreover, with the growing integration of AI, notable developments have emerged in Türkiye's data protection law regarding AI-related PI processing. In this context, the DPA issued the Generative AI Guideline, as well as documents on the 'Use of Generative AI Tools in the Workplace' and 'Agentic AI'. Particularly, Generative AI Guideline addresses the scope of information to be provided to data subjects in AI-based processing activities and sets out recommended technical and organisational measures to mitigate AI-specific risks.

Law stated - 11 June 2026