PANORAMIC

DATA PROTECTION & PRIVACY

Türkiye

LEXOLOGY

Data Protection & Privacy

Contributing Editors

Aaron P Simpson and Lisa J Sotto

Hunton Andrews Kurth LLP

Generated on: August 1, 2025

Contents

Data Protection & Privacy

SHARING AND CROSS-BORDER TRANSFERS OF PI

RIGHTS OF INDIVIDUALS

EXEMPTIONS, DEROGATIONS AND RESTRICTIONS

SPECIFIC DATA PROCESSING

UPDATE AND TRENDS

Contributors

Türkiye

YAZICIOGLU Legal

Simge Yüce	simge@yazicioglulegal.com
Arda Kilci	arda@yazicioglulegal.com
Cemre Yeşinnar	cemre@yazicioglulegal.com
Yiğit Aktimur	yigit@yazicioglulegal.com
Bora Yazıcıoğlu	bora@yazicioglulegal.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 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 procedures 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).

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

Law stated - 20 Mayıs 2025

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 - 20 Mayıs 2025

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 is required to monitor international developments and cooperate with international organisations.

Law stated - 20 Mayıs 2025

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 breach notification, data subject complaint, or ***ex officio***, it may impose administrative fines ranging from 68,083 to 13,620,402 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 - 20 Mayıs 2025

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 - 20 Mayıs 2025

SCOPE

Exempt sectors and institutions

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

The Personal Data Protection Law No. 6698 (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 - 20 Mayıs 2025

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.

Law stated - 20 Mayıs 2025

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. The Turkish Criminal Code (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 require 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.

Law stated - 20 Mayıs 2025

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.

Law stated - 20 Mayıs 2025

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 Data Protection Authority (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 controller or processor is located abroad.

Law stated - 20 Mayıs 2025

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 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 - 20 Mayıs 2025

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?

In principle, PI cannot be processed without the explicit consent of the data subject. However, controllers may process PI without explicit consent if one of the legal bases set forth in article 5 of the Personal Data Protection Law No. 6698 (DP Law) is satisfied.

Law stated - 20 Mayıs 2025

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 Turkish Data Protection Authority (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.

Law stated - 20 Mayıs 2025

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 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.

Law stated - 20 Mayıs 2025

Exemptions from transparency obligations

When is notice not required?

Under the Personal Data Protection Law No. 6698 (DP Law), notice is not required in the following 'exceptional cases':

- when necessary for a criminal investigation or 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 - 20 Mayıs 2025

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 - 20 Mayıs 2025

Data minimisation

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.

Law stated - 20 Mayıs 2025

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 - 20 Mayıs 2025

Purpose limitation

Are there any restrictions on the purposes for which PI can be used by owners? If there are purpose limitations built into the law, how do they apply?

PI must be collected for specific, explicit, and legitimate purposes and must not be processed in a manner incompatible with those purposes.

Law stated - 20 Mayıs 2025

Automated decision-making

Does the law restrict the use of PI for making automated decisions without human intervention that affect individuals, including profiling?

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.

Law stated - 20 Mayıs 2025

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 PI and unauthorised access, thereby ensuring data security. A controller's accountability extends also 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 Turkish 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 - 20 Mayıs 2025

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.

Law stated - 20 Mayıs 2025

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 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 PI inventory and implement a retention and destruction policy.

While controllers bear primary responsibility for compliance, this obligation 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 - 20 Mayıs 2025

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 - 20 Mayıs 2025

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 - 20 Mayıs 2025

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.

Law stated - 20 Mayıs 2025

Design of PI processing systems

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

Unlike the General Data Protection Regulation (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 - 20 Mayıs 2025

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 the Data Controllers' Registry (VERBIS). For foreign controllers, however, it remains unclear whether the registration requirement applies to all of them or only to those that engage in 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. Additionally, controllers in Türkiye with fewer than 50 employees and an annual financial balance sheet total below 100 million Turkish lira (as of 2025) are also exempt, provided their core activity does not involve processing special categories of PI. Exemptions also apply in 'exceptional cases'.

As of 2025, non-compliance with VERBIS obligations may result in administrative fines ranging from 272,380 to 13,620,402 Turkish lira, subject to annual adjustment.

Law stated - 20 Mayıs 2025

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 - 20 Mayıs 2025

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; general provisions apply.

Law stated - 20 Mayıs 2025

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 Personal Data Protection Law No. 6698 (DP Law) distinguishes between domestic and international data transfers. Accordingly, general provisions apply to all recipients.

Law stated - 20 Mayıs 2025

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.

Law stated - 20 Mayıs 2025

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 - 20 Mayıs 2025

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.
- Social network providers with daily access exceeding one million must retain Turkish user PI 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.

Law stated - 20 Mayıs 2025

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 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 Turkish 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 - 20 Mayıs 2025

Other rights

Do individuals have other substantive rights?

In addition to 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 - 20 Mayıs 2025

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 Turkish Civil Code (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.

In principle, it is not strictly necessary to demonstrate actual pecuniary loss to claim compensation. Where the breach results in emotional distress, reputational harm, or a

violation of dignity, individuals may still be entitled to compensation for the non-pecuniary 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.

Law stated - 20 Mayıs 2025

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, with respect to compensation claims, the DPA is not authorised to handle or rule on such matters. Individuals seeking compensation for violations of their personal rights must pursue their claims through the general courts.

Law stated - 20 Mayıs 2025

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 under the Personal Data Protection Law No. 6698 (DP Law) as outlined above, the requirements of other laws concerning the erasure, destruction, anonymisation, and domestic or international transfer of PI are reserved.

Law stated - 20 Mayıs 2025

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, which apply to electronic communications service providers. These provisions allow 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 Turkish Data Protection Authority

(DPA) issued its Guidelines on Cookie Applications, providing recommendations for the use of cookies.

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 - 20 Mayıs 2025

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 separate from the explicit consent required under the DP Law for processing PI for marketing.

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.

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.

Law stated - 20 Mayıs 2025

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. Consistent with the DPA's stance, prior explicit consent from data subjects is typically required for targeted advertising.

Law stated - 20 Mayıs 2025

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 measures controllers must implement for compliance.

Additionally, the DPA has issued separate guidelines on general principles and specific requirements for certain special categories, including biometric and genetic data.

Law stated - 20 Mayıs 2025

Profiling

Are there any rules regarding 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 - 20 Mayıs 2025

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 particular 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. For example, the PI Security Guideline requires encryption during data transfers and secure disposal of encryption keys once services end. While no specific encryption standards are mandated, special categories of PI must be transferred via VPN or secure file transfer protocol per the Special Categories Data Guideline.

The DPA also issues guidance for certain types of special categories of PI. For instance, the Guidelines on Genetic Data advise against storing genetic information in the cloud and, where necessary, recommend enhanced safeguards such as detailed logging, off-cloud backups, and two-factor authentication.

Law stated - 20 Mayıs 2025

UPDATE AND TRENDS

Key developments of the past year

Are there any emerging trends or hot topics in international data protection in your jurisdiction?

The new cross-border transfer regime introduced through amendments to the Personal Data Protection Law No. 6698 (DP Law), effective from 1 June 2024, marks a significant step toward aligning Türkiye's PI transfer rules with the General Data Protection Regulation (GDPR).

Following these amendments, the By-Law on the Procedures and Principles Regarding the Transfer of Personal Data Abroad was published in July 2024 by the Turkish Data Protection Authority (DPA), providing essential clarifications on the new framework. To address remaining uncertainties, the DPA issued the Guidelines on Transfers Abroad in January 2025, offering detailed guidance – especially on standard contracts (SCCs), which had generated varied interpretations among practitioners.

The DPA further clarified its stance with a February 2025 announcement outlining key considerations related to SCCs. Despite these efforts, some challenges persist, prompting the DPA to signal that the guidelines will be updated based on practical experience gained over time.

In practice, SCCs have become a preferred solution, as they remove the need for prior DPA approval, although notification remains mandatory. Critics have highlighted the impracticality of SCCs for multi-party arrangements, since SCCs cannot be executed on a multiparty basis. However, this concern has diminished as service providers increasingly implement SCCs with their clients. Nonetheless, in sectors dominated by a few major players, controllers often face limited negotiation power, having to accept offered terms without alternatives.

Law stated - 20 Mayıs 2025