Chambers AND PARTNERS

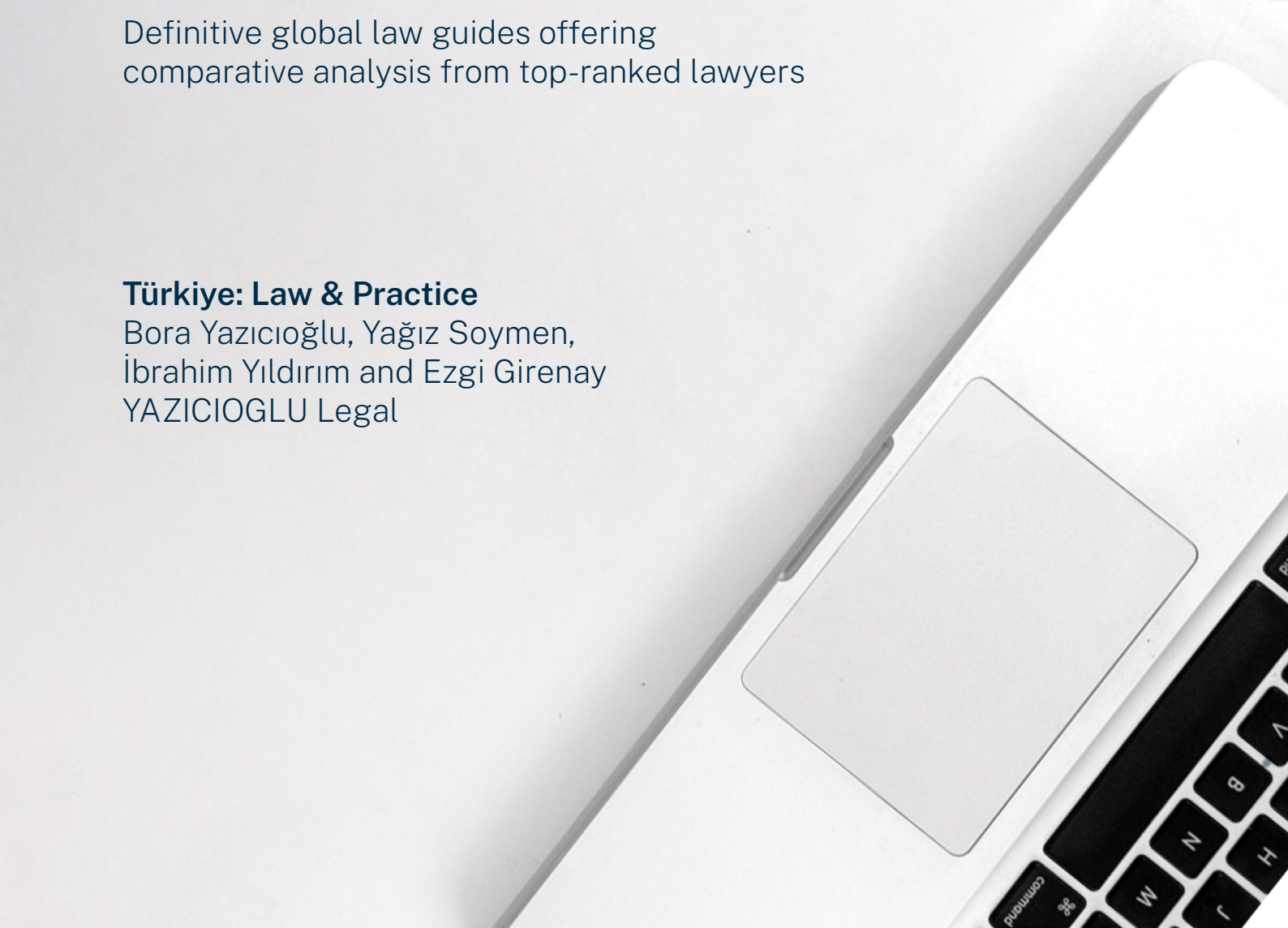
CHAMBERS GLOBAL PRACTICE GUIDES

Data Protection & Privacy 2026

Definitive global law guides offering comparative analysis from top-ranked lawyers

Türkiye: Law & Practice

Bora Yazıcıoğlu, Yağız Soymen, İbrahim Yıldırım and Ezgi Girenay
YAZICIOGLU Legal



TÜRKIYE

Law and Practice

Contributed by:
Bora Yazıcıoğlu, Yağız Soymen, İbrahim Yıldırım and Ezgi Girenay
YAZICIOGLU Legal

Contents

YAZICIOGLU Legal is an Istanbul-based boutique technology law firm. The firm focuses on legal matters related to technology, media & telecommunications and data protection/cybersecurity. It also has solid expertise in cross-border transactions, corporate and commercial matters, intellectual property, regulatory compliance, e-commerce, consumer protection, and dispute resolution. YAZICIOGLU Legal has a dedicated team of 16 lawyers working on data protection and cybersecurity. The majority of the firm's workload involves data protection-related matters. In particular, the firm is known for successfully representing its clients on investigations and data breaches before the Turkish Data Protection Authority. It also provides assistance to several clients, both local and international, including but not limited to Acer, Reddit, and Workday in ensuring compliance with data protection legislation, particularly in cross-border data transfers. The firm is also a Bronze Corporate Member of the International Association of Privacy Professionals (IAPP).

Authors

Bora Yazıcıoğlu is the managing partner at YAZICIOGLU Legal. He has significant experience in advising national and international clients on various aspects of data protection, cybersecurity, and e-commerce law. Bora has represented several major clients on data breaches and investigations before the Turkish Data Protection Authority. He is one of the founding members and the current president of the Data Protection Association of Türkiye. Bora acts as the data controller representative for Zoom, Acer, Cerus, and Ookla in Türkiye.

Yağız Soymen is a senior associate at YAZICIOGLU Legal. He has experience in providing consultancy, audit, and training services regarding compliance processes with data protection regulations. He also works as lead auditor for ISO/IEC 27001 and ISO/IEC 27701. Since 2021, he has been serving as co-director of the Privacy Innovation Lab at Istanbul Bilgi University, where he contributes to training and research activities in the field of data privacy.

İbrahim Yıldırım is a mid-level associate at Yazıcıoğlu Legal. He focuses mainly on various fields of law, including personal data protection, AI, IT law, e-commerce law, contract law, international arbitration, and labour law.

Ezgi Girenay is a legal trainee at YAZICIOGLU Legal. She is working in the fields of data protection, cybersecurity, and e-commerce law.

YAZICIOGLU Legal

NidaKule – Göztepe
Merdivenköy Mahallesi Bora Sokak
No: 1 Kat: 7 34732
Kadıköy / Istanbul
Türkiye

Tel: +90 216 468 88 50
Fax: +90 216 468 88 01
Email: info@yazicioglulegal.com
Web: www.yazicioglulegal.com

1. Legal and Regulatory Framework

1.1 Overview of Data and Privacy-Related Laws

The Right to Protection of Personal Data

The right to protection of personal data is regulated under the Constitution of the Republic of Türkiye (the "Constitution") as an individual right.

According to Article 20 (3) of the Constitution, the right to protection of personal data includes the right to:

- be informed about the processing of personal data;
- have access to personal data;
- rectification or deletion of personal data; and
- be informed about whether personal data is used in accordance with the appropriate purposes.

According to the same Article, personal data may be processed if the processing is allowed by the law, or if the data subject gives explicit consent. The Article finally states that the procedures and principles of processing personal data must be regulated by law.

The Turkish Data Protection Law

Pursuant to the Constitution, the Turkish Data Protection Law (DP Law) was enacted, which is the first general law that regulates the rules for processing personal data in Türkiye. It entered into force on 7 April 2016.

Although it came into force only one month before the European Union General Data Protection Regulation (GDPR), the DP Law was drafted considering only EU Directive 95/46/EC. Currently, efforts are underway to align the DP Law with the GDPR. As part of these efforts, the Law on Amendments to the Criminal Procedure Law and Certain Laws, which also includes amendments to the DP Law (DP Law Amendments) was published on 12 March 2024.

Upon the entry into force of the DP Law Amendments on 1 June 2024, these efforts were followed by the publication of the By-law on the Procedures and Principles Regarding the Transfer of Personal Data Abroad (By-law on Data Transfers Abroad) and the Guidelines on the Transfer of Personal Data Abroad (Guidelines on Transfers Abroad), refer to the European Data Protection Board's (EDPB) guidelines in interpreting the new cross-border transfer rules.

The DP Law does not expressly regulate its territorial scope. Nevertheless, the Turkish Data Protection Authority (DPA) has consistently taken the position that the DP Law may apply to data controllers established outside Türkiye where certain criteria are met. Although these criteria are not explicitly set out in the legislation, they can be inferred from the DPA's decisions. In certain decisions, the DPA adopts an effects-based approach, pursuant to which the DP Law is applicable where processing activities are carried out or produce effects in Türkiye. In other instances, the DPA has also applied a targeting-based approach, where the DP Law applies when individuals in Türkiye are targeted through the provision of services or profiling activities.

The DP Law establishes a framework by outlining the general obligations and principles for data processing activities. Its implementation is further supported by secondary legislation, resolutions and guidelines issued by the DPA, including:

- the By-law on the Deletion, Destruction, or Anonymisation of Personal Data (By-law on the Disposal of Personal Data);
- the By-law on the Registry of Controllers;
- the By-law on Data Transfers Abroad;
- the Communique on Principles and Procedures to Be Followed in Fulfilment of the Obligation to Inform (Communique on Obligation to Inform); and
- the Communique on Principles and Procedures for the Request to Controllers.

Turkish Cybersecurity Law

The Turkish Cybersecurity Law (Cybersecurity Law) entered into force on 19 March 2025. Cybersecurity Law introduces a comprehensive legal framework governing cybersecurity in Türkiye and aims to establish a centralised regulatory structure in a field that was regulated through dispersed legal instruments and sector-specific rules.

Before the Cybersecurity Law, cybersecurity obligations were addressed through various instruments which primarily applied to public institutions and criti-

cal infrastructure operators. In addition, the DP Law imposed obligations regarding the security of personal data, and certain sector-specific regulations also contained cybersecurity provisions. However, these rules did not establish a comprehensive cybersecurity regime. The Cybersecurity Law therefore functions as an overarching framework, and secondary legislation is expected to regulate its implementation further.

The Cybersecurity Law broadly applies to public institutions, private entities, real persons, and other organisations operating in cyberspace. It grants the Cybersecurity Presidency extensive supervisory powers and imposes several obligations on organisations, including co-operation with audits, implementation of cybersecurity measures, and notification of cybersecurity incidents, with administrative fines and criminal sanctions introduced for non-compliance.

Turkish Criminal Law

Certain actions that violate the protection of personal data are defined as crimes in the Turkish Criminal Law ("TCrC"). The TCrC also outlines criminal sanctions for these violations:

- unlawful recording of personal data is subject to imprisonment of one to three years;
- unlawful transfer, publication, or acquisition of personal data is subject to imprisonment of two to four years – if these are realised by exploiting the advantages of a profession or art, such actions are subject to imprisonment of three to six years; and
- failure to destroy personal data after the retention period set forth in the law has passed is subject to imprisonment of two years.

The investigation may commence without requiring a complaint. There is no established jurisprudence on how criminal sanctions will be harmonised with the DP Law.

Turkish Civil Law and the Turkish Code of Obligations

Personal data is considered a part of personality under Turkish law; as such, it is also protected under the protection of personality rights in the Turkish Civil Law (TCiC). Therefore, an individual whose right to the protection of personal data is violated may file a lawsuit before civil courts.

General provisions of the Turkish Code of Obligation (TCO) may also apply in cases of breach of an obligation, particularly when it comes to liability for damages and compensation for harm caused by violating contractual or non-contractual obligations.

Per the TCiC and the TCO, data subjects can not only seek compensation but also ask courts to:

- prevent a threatened infringement;
- cease an existing infringement; and/or
- make a declaration that the infringement is unlawful.

Other

There are also sector-specific regulations governing the processing of personal data in areas such as telecommunications, banking, electronic payment, health, and education.

It is important to consider these legislations, as the DP Law specifies that provisions in other laws regarding the deletion, destruction, or anonymisation, or transfer of personal data, are reserved.

1.2 Rights and Obligations

General Principles and Data Subject Rights

Personal data processing is governed by the principles of lawfulness, fairness, accuracy, and being up to date. Processing must be for specific, explicit, and legitimate purposes, remaining relevant, limited, and proportionate to the intended use. Under the DP Law, data subjects have the right to learn whether their personal data is processed, obtain information about any such processing, its purposes, and the third parties to whom the data is transferred, to request the rectification or deletion of their personal data and the notification of such actions to third parties, to object to decisions based solely on automated processing, and to claim compensation for damages arising from unlawful processing.

Obligations established by the DP Law are imposed on controllers, who determine the purpose and means of processing personal data. Key obligations include;

- Registration to the Registry of Controllers (VERBIS): Controllers meeting specific criteria must register with the VERBIS. Those obliged controllers must also maintain a data processing inventory and implement a Personal Data Retention and Destruction Policy. Additionally, they must designate a "contact person" responsible for submitting information to VERBIS and facilitating communication with the DPA.
- Privacy Notices: Controllers must provide data subjects with clear notices detailing the processing activity.
- Technical and Administrative Measures: Controllers must implement appropriate organisational and technical safeguards to prevent unauthorised access and unlawful processing.
- Request Management: Controllers must respond to data subject requests within 30 days.
- Breach Notification: Any personal data breach must be notified to the DPA without any delay and within 72 hours of becoming aware of the breach, where possible. Affected individuals must also be informed promptly.
- Processor Oversight: Controllers are jointly responsible for ensuring that processors implement the necessary technical and administrative measures while processing data on their behalf.

1.3 Special Categories of Personal Data

Special categories of personal data are defined in DP Law as follows: data relating to race, ethnic origin, political opinion, philosophical belief, religion, religious sect or other belief, appearance, membership of associations, foundations or trade unions, data concerning health, sexual life, criminal convictions and security measures, and biometric and genetic data.

The processing of special categories of personal data is governed by Article 6 of the DP Law and secondary regulations issued by the DPA.

The processing conditions specified in Article 6 of DP Law are as follows:

- explicit consent;
- being explicitly prescribed by law;
- being mandatory to protect the life or physical integrity of a person who is physically unable to give consent;
- being made public by the data subject;
- being mandatory for the establishment, exercise, or protection of a right;
- being mandatory for the fulfilment of legal obligations in the fields of employment, occupational health and safety, social security, or social assistance;
- being mandatory for activities carried out by foundations, associations, or other non-profit organisations for their members, provided the data is not disclosed to third parties; and
- being mandatory for medical diagnosis, treatment, care services, or the planning and management of health services and financing.

Controllers must also comply with the DPA's decision, setting out specific technical and administrative measures for the processing of special categories of personal data.

DP Law does not foresee a specific regime for the processing of minors' personal data; however, the DPA occasionally publishes guidelines and materials aimed at raising awareness.

1.4 Processing of Personal Data for Research and Development Purposes

Unlike the GDPR, the DP Law does not provide a specific legal basis for processing and/or anonymising health data for scientific purposes. Under the DP Law, (i) the processing of personal data for purposes such as research, planning, and statistics through anonymisation, and (ii) the processing of personal data for scientific purposes, provided that it does not violate national defence, national security, public security, public order, economic security, the right to privacy, or personality rights, and does not constitute a criminal offence, are completely exempt from the application of the DP Law. Moreover, according to the By-law on Personal Health Data, health data may be used for scientific purposes when the exemptions in the DP Law are triggered.

However, since (i) the DP Law does not define scientific research, and (ii) the DPA has not adopted a clear

stance on the application of this exemption to health data processing for scientific purposes, relying on this exemption may not be possible, especially considering the commercial nature of such activities, which creates legal uncertainty.

In terms of the open health data space, the By-law on Personal Health Data stipulates that the data contained in systems used by organisations affiliated with the Ministry of Health, with a consideration on regulations related to data privacy and security, shall be made accessible to everyone through a dedicated website with the aim to ensure transparency and accountability in the healthcare system, guide policies and strategies for healthcare service delivery, support scientific research in the health sector, and facilitate the development of health-related products and services.

Lastly, according to the By-law on the Protection and Processing of Data Within the Social Security Institution (SSI), data obtained by the SSI may be anonymised and transferred upon the Institution's approval, for purposes such as the development of health and social security policies, the protection of public health, the preparation of statistics, and scientific or academic research.

1.5 Processing of Personal Data in the Context of Artificial Intelligence

Türkiye does not currently have an AI law but is focused on regulating AI in the future, setting goals for a comprehensive legal framework and AI governance in line with international trends, including the EU's AI Act, as outlined in its strategy documents. In addition, the DP Law does not establish a specific regime for processing activities carried out through AI systems.

However, the DPA has issued specific guidance titled "the Guideline on Generative Artificial Intelligence and Personal Data Protection (AI Guideline)". The AI Guideline provides clarifications on how to ensure compliance with the DP Law in processes involving generative AI. The AI Guideline provides recommendations aimed at facilitating transparency in the development, deployment, and use of generative AI, and it recommends a human oversight mechanism, but it does not establish a risk-based regime. Consequently, the AI Guideline serves as a resource for those developing, deploying, and using generative AI. However, a few statements in the AI Guideline appear to have potential to give rise to uncertainty in practice.

The DPA has also published a guidance titled "Use of Generative AI Tools in Workplaces", which highlights key risks related to the use of third-party generative AI tools, such as data protection, information security, trade secrets, and inaccurate outputs, and provides governance recommendations for companies, without introducing specific legal obligations.

Lastly, in March 2026, the DPA accomplished a guideline in AI governance by issuing its Guideline on Agentic Artificial Intelligence "Agentic AI Guideline", indicating DPA's growing emphasis on setting clarity for autonomous systems. The Board's dedication to providing more clarity through technical definitions and classifications, such as the distinction between integrated Agentic AI systems and task-specific AI Agents, is demonstrated in the Agentic AI Guideline. The Agentic AI Guideline is firmly based on the Law's core data protection principles, even if it provides a more detailed examination of these technologies through sectoral examples in healthcare and finance. The DPA gives organisations a road map for navigating data controller responsibilities in the era of digital agents by reiterating that even the most autonomous systems must adhere to fundamental obligations, such as transparency, purpose limitation, and human oversight, rather than departing from accepted norms.

1.6 Data Breach Requirement

There is no explicit definition of "data breach" under the DP Law. However, the obligation to notify the DPA arises "in the event that personal data is obtained by others through unlawful means", pursuant to the DP Law. Considering this explicit provision, it can be interpreted that data breach notification under the DP Law is limited solely to the breach of the data's confidentiality; therefore, it could be argued that, unlike the GDPR, the loss of data integrity or availability is not regulated as a breach that triggers a notification obligation within the framework of the DP Law.

Despite this, it is observed that in the DPA's Breach Notification Form, "data integrity" and "data access/

availability" elements are also evaluated under the heading of Breach Impact, indicating that the DPA interprets this concept broadly.

Controllers are required to notify the DPA without delay and no later than 72 hours after becoming aware of the breach. Additionally, controllers must inform affected data subjects as soon as possible, with the necessary details regarding the breach and the potential risks to their personal data. The DP Law does not establish risk thresholds for assessing the requirement to notify the breach to the DPA and the data subjects, meaning that every breach must be reported, regardless of its perceived risk level.

In terms of supervision, written audits are typically preferred by the DPA over on-site inspections, although the DPA is entitled to conduct the latter. After reporting the breach to the DPA, controllers should keep an internal breach log and be prepared for any ex officio inquiries. Immediate internal documentation, prompt official notifications, and the compilation of technical evidence for written regulatory inquiries are important action items.

Additionally, the Cybersecurity Law obliges those who provide services, collect data, process data, or conduct similar activities using information systems to notify the Cybersecurity Presidency, without delay, of any vulnerabilities or cyber incidents they detect in the field in which they provide services. Therefore, when controllers suffer a personal data breach, the breach will most likely also be notified to the Cybersecurity Presidency.

1.7 Regulators

The primary supervisory and regulatory authority is the DPA. It is an independent administrative institution.

The DPA regulates data protection activities and safeguards the rights of data subjects. Some of its duties and powers are as follows:

- conducting investigations and taking temporary measures;
- concluding the complaints;
- imposing administrative sanctions;
- issuing adequacy decisions; and
- approving transfer mechanisms that require DPA approval.

The Ministry of Trade is authorised to oversee marketing communications (see **4.2 Personalised Advertising and Other Online Marketing Practices**).

Additionally, sector-specific administrative institutions as the Banking Regulation and Supervision Agency, the Capital Markets Board, the Turkish Republic Central Bank, and the Cybersecurity Presidency have the authority to regulate issues within their respective sectors.

1.8 Enforcement Proceedings and Fines

The DPA may initiate investigations upon receiving a complaint from a data subject or ex officio if it becomes aware of the alleged violation.

The Course of an Investigation

The DPA may request information and/or documents from controllers. Controllers are required to provide requested information and/or documents within 15 days, unless they constitute a state secret. The DPA may request additional information and/or documents and conduct an on-site inspection during an investigation.

Administrative Fines

The DP Law outlines five types of violations, each subject to administrative fines that are adjusted annually. As of 2026, they are:

- failure to inform data subjects of processing activities (between TRY85,437 and TRY1,709,200);
- failure to take the necessary technical and organisational measures (interpreted broadly, including unlawful data transfer abroad and breach of fundamental principles) (between TRY256,357 and TRY17,092,242);
- failure to comply with the decisions issued by the DPA (between TRY427,263 and TRY17,092,242);
- failure to comply with the obligation to register with VERBIS and failure to submit information to VERBIS (between TRY341,809 and TRY17,092,242); and

- failure to notify the DPA within five business days following the signature of the standard contracts (SCCs) (between TRY90,308 and TRY1,806,177).

Unlike other failures stipulated in the DP Law where only the controller is responsible, both controllers and processors can be held liable for failure to notify the DPA regarding SCCs.

The DPA must consider the severity of the breach, the fault of the breaching party, and its economic condition.

Administrative Orders

The DPA may also order controllers to bring their processing activities into compliance with the DP Law. When the DPA issues such an order, this decision must be implemented without any delay and, at the latest, within 30 days upon receipt of the notification by the controller.

The DPA is also entitled to cease certain personal data processing activities or transfers abroad if it finds that such processing activities result in damages that are difficult or impossible to compensate for, and if the act is clearly unlawful.

Appeal Mechanisms

Controllers have the right to appeal against the DPA's decisions. They may object to such decisions before the administrative courts within 60 days of receiving the decision.

The decisions of the administrative courts can be appealed to the Regional Administrative Courts, and the decisions of the Regional Administrative Courts can be further appealed to the Council of State, provided that the administrative fine exceeds the applicable thresholds.

However, if the DPA's decision includes only an administrative measure rather than an administrative fine, decisions of both the administrative courts and Regional Administrative Courts can be appealed, regardless of the relevant minimum thresholds.

Civil Orders

A data subject who suffers damage due to the unlawful processing of their personal data under the DP Law has the right to seek compensation by applying to the competent civil court.

Criminal Orders

The TCrC governs criminal liability for data-related offences. Under the TCrC, unlawful recording of personal data is punishable by imprisonment from one to three years. Article 136 stipulates that any individual who unlawfully provides, disseminates, or obtains personal data shall face a prison sentence of two to four years. Article 138 addresses the failure to destroy personal data; if a person responsible for data management fails to delete or anonymise personal data despite the expiry of legally mandated retention periods, they are subject to imprisonment for one to two years.

Enforcement Under the Cybersecurity Law

The Cybersecurity Presidency is still being established and has not yet initiated any enforcement actions. However, according to the Cybersecurity Law, the Cybersecurity Presidency is entitled to conduct on-site inspections, request information and technical materials, and examine systems; in certain cases, searches, copying, and seizure require a judge's decision or, in urgent cases, a prosecutor's written order, subject to prompt judicial approval. Administrative fine decisions may be challenged before the administrative courts. The law does not provide a settlement mechanism.

Sanctions include both administrative fines and criminal penalties. Administrative fines apply, for failing to report vulnerabilities or cyber incidents, failing to meet procurement/certification obligations, and obstructing audits, among others; in some cases, fines for companies may reach up to 5% of annual gross sales. Criminal sanctions include imprisonment and judicial fines for withholding requested information, operating without required approvals, breaching confidentiality, unlawfully disclosing leaked data, spreading false leak claims, carrying out cyber-attacks, or abusing statutory powers. Penalties are generally shaped by the nature of the breach, repetition, any benefit gained, or damage caused, turnover where relevant, and aggra-

vating factors such as commission by public officials, multiple offenders, or organised groups.

1.9 Enforcement Trends

The DPA has focused on specific topics and issued important decisions and announcements regarding its actions.

Loyalty Programmes and In-Store Consent Practices

The DPA emphasises the importance of authentication mechanisms in loyalty programmes, requiring controllers to verify whether the person using the loyalty account during a purchase is the account holder. Additionally, the DPA emphasises that SMS verification codes used during purchases or service processes must not be misleadingly presented as mandatory if they also serve purposes such as obtaining consent for data processing or commercial communications.

Online Protection of Minors

The DPA has initiated an ex officio investigation into several social media platforms to examine how children's personal data are processed and what safeguards are implemented. The investigation aims to assess whether adequate measures are in place to protect children from potential risks in the digital environment, considering the best interests of the child and the need to ensure protection of their personal data when using social media services.

Focus on AI

Although it has not yet resulted in an enforcement action, the DPA has issued several guidelines regarding the use of AI.

2. Privacy Litigation

2.1 Privacy Litigation Overview

Tracking privacy litigation trends in Türkiye is challenging, due to the limited accessibility of case law. Only Constitutional Court decisions are required to be published in the Official Gazette, while decisions from other courts remain largely unpublished. This lack of transparency makes it challenging to predict how data protection laws will be interpreted and applied by the courts, hindering the ability to identify clear trends in privacy litigation at this stage.

In recent years, the court has rendered a limited number of decisions directly concerning personal data, primarily focusing on the exercise of the rights to deletion and rectification, as well as the overall effective protection of data privacy.

A notable decision by the court addressed the protection of personal data within the context of inaccurate judicial records. In this case, the court held that the refusal to delete a citizen's status as a "complainee" from the National Judiciary Network Information System, despite the formal absence of an actual complaint, constituted a violation of the right to request the rectification of personal data. The court further emphasised that the failure of judicial authorities to conduct a substantive review of the rectification request effectively deprived the individual of an effective legal remedy.

Another significant ruling by the Constitutional Court clarified the State's positive obligations regarding the ineffective investigation of unlawful personal data acquisition and use between private individuals. The court ruled that a superior's use of a subordinate's personal records – such as union membership forms and internal petitions – as evidence in a private lawsuit violated the right to data protection. This was confirmed by the fact that the institution holding the data had never transferred it to the judiciary, and therefore the data was obtained without administrative action or explicit consent.

The DP Law refrains from establishing specific provisions for the compensation of damages arising from the unlawful processing of personal data and makes no distinction between material and moral harm. Instead, it stipulates that the right to compensation for those whose personality rights are violated is reserved under general provisions, while the TCiC explicitly allows for both material and moral claims in such instances. To seek damages based on a violation of the DP Law, the absence of legal justification, a breach of the data controller's duty of care, and a clear causal link between the unlawful act and the resulting harm must be established. Regarding compensation

for moral damages, a causal link between the unlawful attack and the moral damage is required.

2.2 Recent Case Law

Due to the lack of transparency (see **2.1 Privacy Litigation Overview**), a concrete determination regarding the existing case law cannot be made. As such, it is not always possible to determine which privacy lawsuits are currently ongoing or to identify landmark cases.

In practice, it is known that legal remedies have been pursued against the decisions and administrative fines imposed by the DPA. However, tracking these cases is not always feasible and, therefore, it would be appropriate to state that no standout cases have been identified.

Both ordinary and extraordinary legal remedies have been pursued against the decisions and administrative fines imposed by the DPA within the framework of the DP Law, as well as under legislation relating to the right to data protection. For instance, ongoing legal proceedings exist relating to the crime of unlawful recording of personal data under the TCrC, as well as civil proceedings under the TCiC concerning the prevention of and/or compensation for unlawful processing of personal data as a violation of personal rights.

An example, recently issued by the Turkish Supreme Court, is a decision addressing moral compensation claims arising from the unauthorised disclosure of banking records and personal data by a financial institution. The court argued that the bank, acting as a "trust institution" and as the data controller, violated the principles of "purpose limitation" and "data minimisation" by submitting extensive account movements that exceeded the specific timeframe requested by the judiciary. It further stated that such an unlawful disclosure constituted a direct violation of the data subject's personality rights and emphasised that the subsequent publication of this data by third parties did not break the causal link between the bank's negligence and the resulting moral damage.

2.3 Collective Redress Mechanisms

There is no concept of collective redress for privacy litigation under the Turkish legal system, nor have there been any developments in this area.

That said, associations and other legal entities may file lawsuits on behalf of their members or the group of people they represent, to protect their interests, address unlawful situations, or prevent future violations. For instance, under the Turkish Consumer Protection Law consumer organisations, relevant public institutions and the Ministry of Trade may take legal action before the consumer courts to prevent or halt unlawful situations affecting consumers, excluding unfair commercial practices and advertisements. However, these provisions do not explicitly address collective actions related to privacy.

3. Requirements for the Protection and Processing of Non-Personal Data

3.1 Objectives and Scope of Data Regulation

Unlike the EU Data Act, there is no specific regulation addressing non-personal data in Türkiye. General rules apply.

As for future endeavours, the 12th Development Plan (2024–2028), states that a national data governance framework will be established and the necessary technical, institutional, and legislative infrastructure will be developed.

Additionally, the Medium-Term Programme (2026–2028), sets the development of a governance framework that safeguards data privacy and security as a goal, and states that the National Data Strategy and Action Plan will be implemented in the third quarter of 2026.

3.2 Interaction of Data Regulation and Data Protection

Since there are no specific standalone data regulations, general rules apply.

3.3 Rights and Obligations Under Applicable Data Regulation

Due to the absence of a standalone regulation specifically addressing the use of non-personal data, general obligations outlined in the DP Law apply in so far as these services involve processing of personal data (see **1.2 Rights and Obligations**).

3.4 Regulators and Enforcement

As Türkiye currently lacks comprehensive data regulations beyond those pertaining to personal data protection, there is no specific regulatory body solely tasked with enforcement in this area. However, when relevant actors process personal data, the DPA will be responsible for overseeing the process. That being said, sector-specific regulations may grant authority to certain regulatory bodies over specific data-related matters.

4. Sectoral Topics

4.1 Use of Cookies

Under Turkish law, there is no legislation explicitly governing the use of cookies, except for the Electronic Communications Law (ECL), which applies only to electronic communications service providers. The ECL permits cookies for communication or if users are informed and give explicit consent.

The DPA considers data collected through cookies as personal data, thus subject to the DP Law. The DPA issued the Guidelines on Cookie Applications (Cookie Guidelines) providing best-practice recommendations for data controllers, including cookie banners, consent management platforms, and a sample cookie policy.

Cookie Guidelines is limited to the use of cookies and does not cover other tracking technologies such as Software Development Kits (SDKs) and device identifiers. However, as the DPA has not issued specific guidance on the latter and given their similar processing nature, the Cookie Guidelines may also serve as an important reference in terms of the DPA's approach to tracking technologies other than cookies.

The Cookie Guidelines also refer to the ECL and provide two criteria for processing activities where controllers rely on legitimate interest. Controllers are advised to perform a balancing test, weighing the individual's rights and freedoms against the controller's legitimate interests, taking into account whether:

- cookies are essential for communication via electronic communication networks; or
- cookies are strictly necessary for information society services explicitly requested by the user.

Moreover, the Cookie Guidelines include several recommendations for situations where controllers obtain data subjects' explicit consent for the use of cookies, for which an opt-in mechanism is required. For instance, using consent management platforms allowing data subjects to manage their preferences is cited as a good practice. However, since frequent requests may cause "consent fatigue", consent reminders are advised to align with the cookie's lifespan.

Furthermore, consent obtained through cookie walls – where access to a website is conditioned on accepting cookies – is generally considered invalid if it prevents users from making a genuine choice. However, a cookie wall may be deemed acceptable on a case-by-case basis, provided that fair alternatives are offered to the user for accessing the service without compromising their free will.

In cases where the use of cookies involves transferring data abroad, controllers should also consider the requirements outlined in the DP Law (see **5.1 Restrictions on International Data Transfers**).

Special Considerations for Analytics Cookies

The Cookie Guidelines classify cookies by duration, purpose and party. While these categories largely mirror EU practice, there is a key difference for analytics cookies; explicit consent may not be required for first-party analytics cookies, provided that:

- their use is limited to measuring site or application's target audience;
- personal data collected through cookies – which are not strictly required for the purpose of processing – is anonymised;
- the personal data collected through cookies is only used for anonymous statistics;

- the duration of cookies is reasonable, and personal data collected is not transmitted to third parties.

In this scenario, personal data collected through cookies should not be used to track users across multiple sites or devices.

Non-essential cookies are subject to strict opt-in requirements. Organisations must seek explicit consent before using cookies and SDKs for advertising, marketing, or performance-tracking purposes. In contrast, necessary cookies follow an opt-out paradigm, which means they can be used without agreement as long as clear information is provided and an opt-out option is accessible for the users.

4.2 Personalised Advertising and Other Online Marketing Practices

Online Marketing

Online marketing is mainly governed by the Law on Regulation of Electronic Commerce, the By-law on Commercial Communication and Commercial Electronic Messages (together "E-Commerce Legislation"), and the DP Law.

According to the E-Commerce Legislation, prior approval from recipients must be obtained before making calls or sending SMS or emails for marketing purposes (marketing communications). This approval is a specific authorisation for sending marketing communications and is distinct from the explicit consent required under the DP Law for processing personal data for marketing purposes. Although the Ministry of Commerce, which oversees compliance with the E-Commerce Legislation, does not consider push notifications as marketing communications, the DPA requires data subjects' explicit consent to send push notifications. The Ministry of Trade has decided that enabling push notifications on a phone does not by itself constitute consent for marketing messages and that users must be given the option to receive only informational notifications.

The E-Commerce Legislation provides an exemption for marketing communications sent to tradespeople or craftspeople in the business-to-business (B2B) context, where their approval is not required, but they must be given the option to opt out.

Marketing communications must include the sender's precise identification information, as well as an option to opt out.

All senders of marketing communications are required to register with the Message Management System (MMS) and upload information regarding the approvals and withdrawals for this purpose. MMS is an online platform where recipients can manage their approvals for receiving marketing communications and opt out if desired. Any approval or withdrawal received by the sender must be uploaded to the MMS within three business days of receipt.

Personalised Advertising

Turkish law does not have specific provisions for behavioural and targeted advertising. Therefore, these activities are subject to general provisions of the DP Law. In line with the DPA's general approach to this matter, in principle, prior explicit consent from data subjects is required for behavioural or targeted advertising.

That being said, as far as it is known, the DPA has ruled in an unpublished decision that, in specific cases, controllers may rely on legitimate interest for behavioural or targeted advertising. However, as the details of this decision have not been published, the DPA's rationale behind this decision remains unclear.

Unlike the Digital Services Act, Turkish law does not include specific restrictions on the profiling of minors for online advertising. Nevertheless, as mentioned in **1.9 Enforcement Trends**, the online protection of minors is a trending topic for the DPA, and additional obligations in this area may be expected in the future.

4.3 Employment Privacy Law

Employment privacy is not governed by a specific, standalone regulation in Turkish law. However, some provisions related to employment privacy are included in diverse laws, such as:

- the TCO provides that an employer may use an employee's personal data only to the extent necessary for the employee's employability or the performance of the employment contract;

- Turkish Labour Law obliges employers to handle information obtained about their employees under the rules of good faith and law and prohibit disclosing any information that the employee has a justified interest in keeping confidential;
- Occupational Health and Safety Law mandates that health data must be kept confidential to protect the private life and reputation of the employee.

Essentially, the general principles of the DP Law apply in the workplace and controllers must comply with its obligations. However, due to the unique relationship between employers and employees, controllers face certain challenges in practice.

Monitoring Workplace Communications

In some of its decisions, the DPA addressed the monitoring of employee communications in the workplace. Accordingly, an employer is entitled to monitor work computers, work mobile phones, and other electronic devices provided to employees, provided that the following conditions are met:

- informing employees in advance;
- pursuing a legitimate purpose; and
- observing the principle of proportionality.

These principles also apply to the implementation of cybersecurity tools.

The Constitutional Court addressed this issue in several decisions. In one case, an employer examined an employee's corporate email and used the correspondence to terminate the employment contract. The court highlighted that the contract specified the corporate email was for work purposes and could be monitored without prior notice. It emphasised that using the emails for legal purposes in a judicial process was reasonable and proportionate. In another case, holiday pictures and emails sent from the corporate email were used as evidence in the judgment.

Essentially, the Constitutional Court appears to consider the following criteria for employers when monitoring employees' communication tools:

- the terms governing the use of work equipment;
- employee awareness of these terms;
- the proportionality of the interference with employees' rights; and
- whether contract termination is reasonable in light of the employee's actions.

Obtaining Explicit Consent

Employees' explicit consent may not always be considered valid, as employees may not have complete freedom in their relationship with their employer due to the imbalance of power between the parties. Therefore, controllers should carefully assess whether the requirements for explicit consent are met, particularly for processing activities within an employment relationship.

This does not mean that explicit consent obtained from employees will always be deemed invalid. In a decision involving a controller based abroad that obtained employees' personal data through its liaison office, the DPA clarified that employees' explicit consent for the transfer of personal data abroad may be considered valid, as the employee understands that their data will ultimately be processed by the controller abroad.

Processing Special Categories of Personal Data

Before the DP Law Amendments, the legal bases for processing special categories of personal data were limited, creating challenges for controllers, particularly employers processing health data in an employment context. Especially, the introduction of a legal basis allowing the processing of employees' health data where "for the fulfilment of legal obligations in the fields of employment" has significantly facilitated the lawful processing of such data by controllers.

Background Checks

Records related to criminal convictions are considered special categories of personal data under the DP Law. Thus, processing criminal convictions for background checks is considered the processing of special categories of personal data. There is debate over whether employers can process this information based on explicit consent or if it can be processed under the legal basis of "necessity for fulfilling legal obligations in employment". The DPA's Guidelines on the Processing of Special Categories of Personal Data states that decisions such as criminal convictions, imprisonment,

conditional release, judicial fines, or revocation of a driver's licence are considered processing of special categories of personal data. Therefore, some interpretations in the sector suggest that processing criminal record documents showing a clear background (ie, no convictions) does not count as processing special categories of personal data.

Processing for Job Applications

The DP Law does not provide a specific regime regarding the processing of job applications, and general provisions apply. In this regard, personal data related to a job application can be processed without explicit consent based on the legal basis of "processing is necessary for establishment or performance of the contract". However, the data must be stored only for the purpose of which it was processed. Data of the candidate who is not selected should be deleted after reasonable period.

4.4 Data Protection in M&A

As the DP Law does not explicitly regulate M&A transactions, such processes are governed by the general principles of the DP Law. Key requirements can be categorised as follows:

Due Diligence Phase

- Legal Basis: Controllers must ensure they rely on the appropriate legal bases outlined in the DP Law when transferring personal data.
- Data Minimisation: Sellers must redact or anonymise personal data whenever possible. Data-sharing should be strictly limited to what is necessary for the transaction's valuation and legal assessment.
- Data Rooms: Access must be restricted on a "need-to-know" basis. Data rooms should use pseudonymisation, redaction, or anonymisation where feasible.
- Data Protection Compliance Audit: A holistic audit must be conducted to evaluate the target company's compliance with data protection laws.

Notification

- Data Subjects: Data subjects must be informed about the data processing and transfer activities. In cases where the transfer relies on explicit consent, the data controller must ensure that explicit consent should be obtained.
- VERBIS: The DPA must be informed by any changes of the controller's representative or contact information.
- Data Transfers Abroad: If the buyer is a foreign entity and the data is being transferred to servers outside of Türkiye, the parties must comply with the DP Law, which may require SCCs which are subject to notification to the DPA.

Post-Closing Phase

- Data Migration and Security: During the technical migration of databases, the buyer must implement robust technical and organisational measures, including encryption and access logs, to safeguard data confidentiality and integrity.

5. International Considerations

5.1 Restrictions on International Data Transfers

With the DP Law Amendments, the previous system has been significantly amended. Current provisions of the DP Law foresee a gradual and alternative regime for international transfers, comprising three levels based on;

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

While the DP Law does not include a definition of "data transfer abroad", the By-law on Data Transfers Abroad fills this gap by defining it as "the transmission of personal data by a data controller or data processor within the scope of the DP Law to a data controller or data processor abroad or making it accessible by any other means".

With its Guidelines on Transfers Abroad, the DPA further clarified that direct collection of personal data does not constitute data transfer under the new regime, in contrast to its previous position.

Adequacy Decisions

Adequacy decisions provide a valid legal basis for transferring data abroad. The DPA has the authority to issue adequacy decisions not only for countries but also for international organisations and specific sectors within third countries (a "Whitelist").

Adequacy decisions must be reviewed by the DPA at least once every four years. If the DPA determines that adequate protection is no longer ensured, these decisions may be amended, suspended, or revoked with prospective effect following the review, or in any other cases it deems necessary.

Since the DPA has not yet established a Whitelist, alternative mechanisms for transferring data abroad must be considered in practice.

Appropriate Safeguards

In the absence of an adequacy decision, data transfers abroad can still occur through the implementation of appropriate safeguards. However, these safeguards can only be utilised if the conditions for processing personal data are met, and if it is feasible for data subjects to exercise their rights and access effective legal remedies in the third country where the data will be transferred.

There are four methods to deploy appropriate safeguards:

- an agreement between "public institutions and organisations or international organisations abroad" and "public institutions and organisations or public professional organisations in Türkiye", subject to the DPA's approval;
- binding corporate rules (BCR), subject to the DPA's approval;
- a written undertaking containing provisions that will provide adequate protection, subject to the DPA's approval; and
- SCCs announced by the DPA, with a requirement for notification to the DPA within five business days from the execution date. The By-law on Data Transfers Abroad states that notifications of SCCs can be made physically, via registered electronic mail, or through other methods determined by the DPA. In this context, the DPA introduced an online "SCC Notification Module" in 2024.

Due to the challenges in obtaining approval from the DPA, SCCs have been the most viable option in market practice.

The DPA published SCCs modules that cover data transfers from (i) controller to controller, (ii) controller to processor, (iii) processor to processor, and (iv) processor to controller.

While the English-language versions are also available on the DPA's website, the By-law on Data Transfers Abroad clearly emphasises that if SCCs are executed in a foreign language, the Turkish version will prevail. This is further confirmed in the Guidelines on Transfers Abroad, stating that double-column SCCs will be considered valid by the DPA, provided that the Turkish version is properly executed.

The SCCs published by the DPA must be executed without any modification, except where explicitly allowed within the relevant sections of the SCCs. While various practices emerged due to uncertainties arising from the lack of guidance, the Guidelines on Transfers Abroad provided clarifications on how to complete each section of the annexes to be filled out by the parties. For instance, while many practitioners only included the categories of personal data transferred, the guidelines clarified that both the categories and the specific data transferred should be stated.

The notifications should include:

- the final version of the SCCs, with relevant sections filled out and signed by authorised individuals of the parties;
- documents proving authority of those signing the SCCs;
- notarised translations of foreign-language documents.

The Guidelines on Transfers Abroad also confirmed that official documents from foreign authorities can be included in the notification, with authentication of signatures, titles, or seals required. This verification is usually done by consular or diplomatic officials. How-

ever, under the Convention Abolishing the Requirement of Legalisation for Foreign Official Documents, documents from signatory countries are exempt from this process, and an apostille is sufficient.

Occasional Transfers

If data transfers abroad cannot occur with an adequacy decision, and if one of the appropriate safeguards cannot be ensured, the data transfer abroad is possible if the transfer is occasional and one of the legal bases laid down for occasional transfer is met.

The By-law on Data Transfers Abroad defines occasional transfers as "transfers that are not regular, occur only once or a few times, are not continuous, and are not in the ordinary course of business". Examples, largely based on EDPB guidelines, are provided in the Guidelines on Transfers Abroad.

When relying on explicit consent for an occasional transfer, the data subject must be informed of the specific risks, including that the destination country may not provide adequate protection or implement sufficient security measures. This may involve the absence of a supervisory authority or guarantees for data processing principles and individual rights.

Onward Transfers

It should be noted that the requirements regarding personal data transfer abroad also extend to onward transfers conducted by either controllers or processors.

Other Regulations

The DP Law states that provisions on data transfers abroad in other laws are reserved. The Guidelines for Good Practices on Personal Data Protection in the Banking Sector emphasise that specific provisions outlined in the Banking Law should be considered when transferring information that constitutes client secrets abroad. Likewise, the By-law on Measures for Preventing Money Laundering and Financing of Terrorism provides details on the required information that must be included in an international e-transfer, adding further compliance obligations for financial institutions.

Sectoral regulations imposing specific restrictions regarding data transfers abroad should also be considered.

5.2 Government Notifications and Approvals

As detailed under **5.1 Restrictions on International Data Transfers**, data transfers abroad can occur through the implementation of appropriate safeguards and, except for SCCs, these safeguards require the DPA's prior approval.

Furthermore, without prejudice to the provisions of international agreements, in cases where the interest of Türkiye or the data subject will be seriously harmed, personal data may only be transferred abroad with the permission of the DPA. The DPA must obtain the opinions of relevant public institutions and organisations before it grants its permission.

Sector-specific regulations may also require further notifications or approvals. For instance, under the Regulation on Geographic Data Permissions, transferring geographic data is subject to the authorisation from the Ministry of Environment, Urbanisation, and Climate Change.

In the health sector, the transfer of personal health data is subject to the evaluation of the Ministry of Health under the By-law on Personal Health Data. Similarly, in the civil aviation sector, airline operators or institutions may share passenger information with third countries upon request under the Turkish Civil Aviation Law, provided that they obtain approval from the Ministry of Interior.

5.3 Data Localisation Requirements

While there is no standalone legislation governing data localisation, certain sector-specific regulations do apply. Key sectors include:

Banking and Finance Entities

The following entities must keep their primary and secondary information systems in Türkiye:

- banks;
- payment institutions and electronic money institutions;
- insurance and private pension companies;

• capital markets institutions; and
• financial leasing, factoring, and finance companies.

Electronic Communications Providers

In principle, electronic communications providers cannot transfer traffic and location data abroad, for national security reasons. In certain cases, such data may be transferred abroad by obtaining the explicit consent of data subjects.

Specific requirements for obtaining consent from users are further regulated in secondary legislation. For instance, in cases where traffic and location data will be transferred, users must be informed about the scope of the data to be transferred, the name and address of the recipient party, the purpose and duration of the transfer, and, if the third party is located abroad, the name of the country to which the data will be transferred, at the time of obtaining their consent.

In 2019, the Information and Communication Technology Authority (ICTA) mandated that all infrastructure, systems, and storage units related to eSIM technologies, including eSIM subscription management, must be set up in Türkiye either by operators authorised in Türkiye or by third parties designated by the operators, with the operator bearing full responsibility. Additionally, any data generated through eSIM technologies must be stored in Türkiye.

Social Network Providers (SNPs)

SNPs with daily access exceeding one million must implement the necessary measures to ensure that the data of their Turkish users is retained within Türkiye. The ICTA further emphasised that priority should be given to storing essential user data, along with any other data specified.

Commercial Electronic Message Management System Integrators

The Communique on Commercial Electronic Message Management System Integrators mandates that authorisation from the Ministry of Trade is required to act as an integrator for service providers in registering approvals and rejections of marketing communications in the MMS, or to carry out these transactions through the MMS. The communique stipulates that the information processing system used in integrator services, including software, hardware, and server infrastructure, must be located within a local database.

Critical Infrastructure Service Providers

The Decree on Information and Communication Security Measures issued by the Presidency of Türkiye (Presidency Decree), sets specific measures to mitigate security risks, particularly for critical data that could jeopardise national security or public order if compromised. It provides an obligation to store critical data (eg, population, health, and communication records, genetic and biometric data) securely.

The Presidency Decree applies not only to businesses providing critical infrastructure services (eg, energy, electronic communications, banking, transportation) but also to public institutions and organisations.

It stipulates that data from public institutions must not be stored in cloud services unless hosted in the institutions' own private systems or with local service providers under their control.

5.4 Blocking Statutes

Türkiye does not have specific "blocking" statutes, but there are general statutory provisions to prevent the disclosure of matters relating to national interests.

5.5 Recent Developments

Following the most recent amendments to the DP Law, the DPA has made efforts to clarify the recently amended international personal data transfer regime with the Guidelines on Transfers Abroad and the announcement on the "Key Considerations for Standard Contracts to be Used in the Transfer of Personal Data Abroad".

The DPA has recently made an announcement regarding the use of foreign messaging applications in public institutions. The DPA emphasised that official documents containing confidential or critical data should not be shared through such applications, considering that these applications do not have data centres within the country.

The DPA has also announced that an agreement (not qualifying as an international treaty) between the Min-

istry of the Interior's Directorate General of Migration Management and the United Nations High Commissioner for Refugees, which serves as the basis for the transfer of personal data abroad, was reviewed and authorised.

Furthermore, efforts to align with the GDPR are ongoing. According to the Medium-Term Programme (2026–2028), the alignment of the DP Law with the GDPR and other EU legislation is expected to be completed by the third quarter of 2026. Additionally, the 12th Development Plan (2024–2028) identifies alignment efforts as a key goal for the coming years.

CHAMBERS GLOBAL PRACTICE GUIDES

Chambers Global Practice Guides bring you up-to-date, expert legal commentary on the main practice areas from around the globe. Focusing on the practical legal issues affecting businesses, the guides enable readers to compare legislation and procedure and read trend forecasts from legal experts from across key jurisdictions.

To find out more information about how we select contributors, email Rob.Thomson@chambers.com