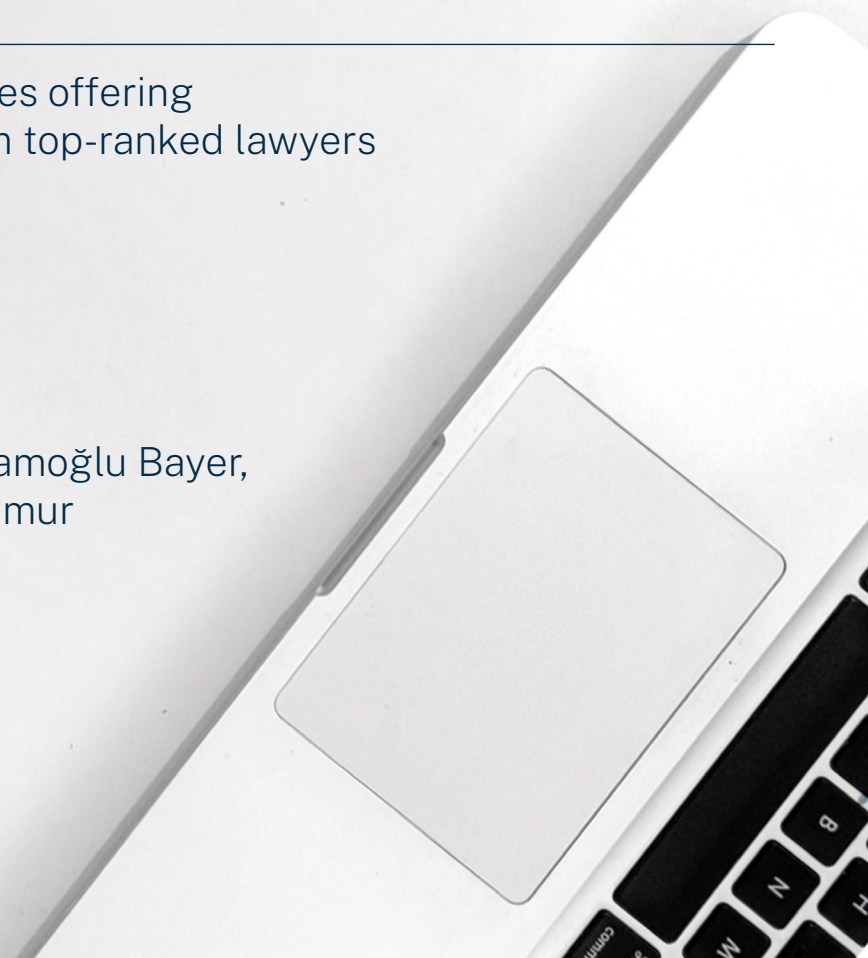
Chambers
AND PARTNERS

CHAMBERS GLOBAL PRACTICE GUIDES

# Data Protection & Privacy 2025

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



**Türkiye: Law & Practice**
Bora Yazıcıoğlu, Kübra İslamoğlu Bayer,
Simge Yüce and Yiğit Aktimur
YAZICIOGLU Legal

# TÜRKIYE


## Law and Practice

**Contributed by:**
Bora Yazıcıoğlu, Kübra İslamoğlu Bayer, Simge Yüce and Yiğit Aktimur
**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 17 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 ranked in several legal directories on TMT and 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 advising national and international clients on several 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.

**Yiğit Aktimur** is an associate at YAZICIOGLU Legal. He focuses on various areas of law, including data protection and e-commerce. Yiğit is a member of the Istanbul Bar Association's Data Protection Commission.

**Kübra İslamoğlu Bayer** is a senior managing associate at YAZICIOGLU Legal. She advises clients on data protection, e-commerce, and cybersecurity laws. Kübra is an active member of the Istanbul Bar Association's IT Law Commission: Artificial Intelligence Study Group and the Data Protection Commission. She gives speeches on data protection on several platforms. She holds a CIPP/E certificate from the International Association of Privacy Professionals.

**Simge Yüce** is a senior associate at YAZICIOGLU Legal. She primarily focuses on data protection and e-commerce laws. Simge is an active member of the Istanbul Bar Association's Data Protection Commission. She holds a CIPP/E certificate from the International Association of Privacy Professionals.

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 has been regulated as an individual right under the Constitution of the Republic of Türkiye (the "Constitution") since its amendment in 2010.

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 only be processed if the law allows it or if the data subject gives explicit consent. The article finally states that the law must regulate the procedures and principles of processing personal data.

### The Turkish Data Protection Law

Pursuant to Article 20(3) of the Constitution, Turkish lawmakers enacted the Turkish Data Protection Law (the "DP Law"), which is the first general law that specifically regulates the procedures and principles 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, including amendments to the DP Law ("DP Law Amendments"), was published in the Official Gazette 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"), which largely refer to the European Data Protection Board's (EDPB) guidelines in interpreting the new cross-border transfer rules.

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 and guidelines issued by the Turkish Data Protection Authority (DPA), with key regulations and guidelines 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");
- the Communique on Principles and Procedures for the Request to Controllers; and
- Guidelines regarding:
  - (a) processing of special categories of personal data;
  - (b) data transfers abroad;
  - (c) application of administrative offences in terms of time;
  - (d) privacy on mobile applications;
  - (e) processing of genetic data;
  - (f) good practices in the banking sector;
  - (g) cookie, practices;
  - (h) right to be forgotten;
  - (i) processing of biometric data;
  - (j) artificial intelligence (AI);
  - (k) preparing an inventory of personal data processing;
  - (l) fulfilment of the obligation to inform;
  - (m) technical and organisational measures;
  - (n) deletion, destruction, or anonymisation of personal data; and
  - (o) the concepts of controller and processor.

In addition, the DPA adopts resolutions, which are published on the DPA's website and/or in the Official Gazette.

### Turkish Criminal Law

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

- 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 to six years.

The investigation may commence without requiring a complaint (ie, ex officio by public prosecutors). However, there is no established jurisprudence for harmonising criminal sanctions with the DP Law.

### Turkish Civil Law & 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 their personal

data is violated may file a lawsuit before civil courts, per the TCiC.

General provisions of the Turkish Code of Obligation (TCO) may also apply in cases of breach of an obligation, particularly regarding 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; and/or
- cease an existing infringement; and/or
- make a declaration that an 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 (**5.3 Data Localisation Requirements**).

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

## 1.2 Regulators

The primary supervisory and regulatory authority in Türkiye is the DPA. It is an independent administrative institution with administrative and financial autonomy.

The DPA is empowered to regulate data protection activities and safeguard data subjects' rights. Some of the primary duties and powers of the DPA are as follows:

- conducting investigations and taking temporary measures, where necessary;
- concluding the complaints of those who claim that their rights concerning personal data protection have been violated;
- maintaining the Registry of Controllers ("VERBIS");
- imposing administrative sanctions provided in the DP Law;
- determining and announcing those countries with adequate levels of protection of personal data for the purpose of international data transfers; and
- approving the written undertaking of controllers in Türkiye, as well as the Binding Corporate Rules (BCR) and the transfers based on the existence of an agreement between public institutions in Türkiye and abroad that does not qualify as an international convention; for the purpose of international data transfers.

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

Apart from the above, sector-specific administrative institutions such as the Banking Regulation and Supervision Agency (BRSA), the Capital Markets Board, the Turkish Republic Central Bank, and the Information and Communication Technologies Authority (ICTA) have the authority to regulate issues regarding the processing of personal data within their respective sectors.

## 1.3 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 during its investigations. Controllers are required to provide requested information and/or documents within 15 days unless they constitute a state secret. The DPA may also 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 2025:

- failure to inform data subjects of processing activities (between TRY68,083 and TRY1,362,021);
- failure to take the necessary technical and organisational measures (interpreted very broadly, including unlawful data transfer abroad and breach of fundamental principles) (between TRY204,285 and TRY13,620,402);
- failure to comply with the decisions issued by the DPA (between TRY340,476 and TRY13,620,402);
- failure to comply with the obligation to register with VERBIS and failure to submit information to VERBIS (between TRY272,380 and TRY13,620,402); and
- failure to notify the DPA within five business days following the signature of the standard contracts (SCCs) (between TRY71,965 and TRY1,439,300).

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

As per the Misdemeanours Law, the DPA must consider the severity of the breach, the fault of the breaching party, and the party's economic condition when determining fines.

### 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 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 DPA's 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.

On the other hand, 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.

## 1.4 Data Protection Fines in Practice

In recent years, the DPA has been reluctant to publish its decisions. Practitioners often learn about these decisions through press coverage

or other practitioners who follow investigation files as complainants or representatives.

To the best of our knowledge, the highest fine issued by the DPA to date is TRY11.5 million, imposed on Instagram in 2024. This fine was due to Instagram's failure to implement adequate technical and administrative measures to ensure data security. Additionally, the platform was penalised for converting private Instagram accounts of child users into business accounts without proper age verification or parental consent.

Another notable fine was imposed in 2023 when WhatsApp and Meta were each fined approximately TRY2.65 million for failing to register with VERBIS and ordered to comply with the registration requirement.

Recently, a significant DPA decision was shared online by its complainant. This decision addressed location-based marketing and the concept of joint controllership – a concept not explicitly outlined in the DP Law. In this case, a mobile operator processed location data to send SMS messages promoting discounts on behalf of a clothing store. Both parties jointly determined the purpose and means of processing, which the DPA interpreted as joint controllership.

The DPA also emphasised obtaining explicit consent, specific to the intended purpose, from data subjects for location-based marketing and subsequent SMS communications. Due to non-compliance, the DPA issued administrative fines of approximately TRY1 million to the clothing store and TRY2 million to the mobile operator.

### 1.5 AI Regulation

Currently, there is no specific legislation dedicated solely to AI. Nevertheless, general provisions from existing laws apply to the use of AI systems.

In particular, the principles outlined in the DP Law apply whenever AI systems involve the processing of personal data. The DPA issued Recommendations on the Protection of Personal Data in the Field of Artificial Intelligence, providing guidance for developers, manufacturers, service providers, and decision-makers. These recommendations address AI-related concerns in the context of personal data processing. The DPA has also published an informational document on chatbots, emphasising transparency principles, potential risks related to the use of AI chatbot applications, and specific measures to be considered when developing such applications.

Additionally, sector-specific regulations may also apply to AI use. For instance, the Regulation on Remote Identification Methods Used by Banks and the Establishment of Contractual Relationships in the Electronic Environment, grants authority to the BRSA to establish principles and procedures for ID verification transactions conducted by customer representatives using AI-based methods. However, the BRSA has not yet issued regulations on this matter.

The Digital Transformation Office, responsible for coordinating the digital transition of public institutions and organisations and matters such as cybersecurity and AI, also closely monitors AI topics. In June 2023, it published a research report on "Chatbot Applications and the ChatGPT Example."

Türkiye is also closely following international legislative trends in AI. The National AI Strategy for 2021–2025 emphasised the importance of global legislative efforts and Türkiye's commit-

ment to the field, though it lacked detailed objectives for legislative modifications. In its updated 2024–2025 Action Plan, the National AI Strategy outlines ambitious goals, including establishing a Central Public Data Centre, creating an International AI Studies Monitoring and Coordination Committee to oversee global AI developments, and drafting regulations for AI governance.

The 12th Development Plan (2024–2028), issued by the Presidency of Strategy and Budget (PSB), identifies the development of an ethical-legal framework for AI as a key objective. Additionally, the Medium-Term Programme (2025–2027), published by the PSB and adopted by Presidential Decree on 5 September 2024, commits to introducing legal reforms to harmonise Türkiye's legislation with the European Union's Artificial Intelligence Act.

The Grand National Assembly of Türkiye established the Parliamentary Research Commission on 5 October 2024 to explore steps to "harness AI's benefits, establish its legal framework, and mitigate associated risks." The president of the commission stated that they aim to complete their report by May 2025.

Last but not least, a Draft Bill on Artificial Intelligence was submitted to the Turkish Grand National Assembly on 25 June 2024. This draft bill aims to ensure the secure, ethical, and fair use of AI technologies. Although its approval is unlikely, it marks a significant milestone as the first legislative initiative in this field.

### 1.6 Interplay Between AI and Data Protection Regulations

Unlike the European Union, Türkiye currently lacks legislation specifically addressing AI that directly impacts data protection.

## 2. Privacy Litigation

### 2.1 General 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 the courts will interpret and apply data protection laws, hindering the ability to identify clear trends in privacy litigation at this stage.

In 2024, the Constitutional Court published only a few decisions directly related to personal data protection. These decisions primarily addressed employment privacy, with a focus on workplace monitoring of employee communications and employees' access rights to their personal data. These decisions can be interpreted as a growing trend in privacy litigation related to workplace privacy (see **4.3. Employment Privacy Law**).

Additionally, the Constitutional Court has also issued decisions indirectly related to the protection of personal data, addressing broader legal principles such as the criteria for imposing administrative fines, with a particular focus on the principle of legal certainty.

In recent years, the "right to be forgotten" has also gained increasing attention in Türkiye despite not being explicitly defined in the DP Law. Prompted by the CJEU's landmark 2014 decision, Turkish courts have gradually recognised this right, with the Turkish Supreme Court first referencing it in 2015. The Constitutional Court has since issued eight published decisions on the matter, finding a rights violation in only one case. Nevertheless, references to the right to be forgotten are rising, and more data

subjects are pursuing legal action based on this claim.

With the DP Law Amendments, the appeal mechanism to the DPA's decisions has been significantly changed, as the former system was heavily criticised by practitioners and legal scholars. This change was also prompted by a decision from the Constitutional Court on 12 October 2023, which raised important questions regarding the adequacy of the appeal body. Under the new framework, appeals against administrative fines imposed by the DPA can now be filed with administrative courts (see **1.3 Enforcement Proceedings and Fines**).

### 2.2 Recent Case Law

Due to the lack of transparency (see **2.1 General 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, specific legal remedies have been pursued against the decisions and administrative fines imposed by the DPA. However, tracking these cases can be challenging, so it is appropriate to conclude that no notable 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 Turkish DP Law, as well as under legislation relating to the right to data protection. For instance, ongoing legal proceedings exist related to the crime of unlawful recording of personal data under the TCC and civil proceedings under the TCiC concerning the prevention of and/or compensation for unlawful processing of personal data as a violation of personal rights. A notable example, albeit not recent, is a decision issued by the Turkish Supreme Court, which addressed moral compensation claims resulting from the unlawful acquisition of personal data. The court argued that the use of the complainant's identification information constituted a violation of their personality rights and further stated that an appropriate moral compensation should have been determined.

### 2.3 Collective Redress Mechanisms

Under the Turkish legal system, there is no concept of collective redress for privacy litigation, and there have been no 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. Data Regulation on IoT Providers, Data Holders and Data Processing Services

### 3.1 Objectives and Scope of Data Regulation

Unlike the European Union's Data Act, no specific regulation addresses IOT services or the rights and obligations of data holders and data processing services in Türkiye. General rules apply.

### 3.2 Interaction of Data Regulation and Data Protection

There are no specific data regulations on IOT providers, data holders, and data processing services; 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 IOT and data processing services, general obligations outlined in the DP Law apply insofar as these services involve the processing of personal data.

Accordingly, the obligations applicable to providers of IOT services and data processing services may vary depending on their role as a controller or processor in data processing. Obligations established by the DP Law are predominantly imposed on controllers, who determine the purpose and means of processing personal data. Key obligations are outlined below.

- Registering with the Registry of Controllers (VERBIS): Controllers who meet specific criteria must register with VERBIS. To register with VERBIS, controllers based outside Türkiye are also required to appoint a representative to act on their behalf before the DPA and data subjects. Additionally, they must designate a "contact person" responsible for submitting information to VERBIS and facilitating communication between the DPA and controllers.
  (a) Controllers required to register with VERBIS must also maintain a data processing inventory and implement a Personal Data Retention and Destruction Policy, as outlined in the By-Law on the Disposal of Personal Data.
- Providing privacy notices: Controllers are obligated to inform data subjects about the processing of their personal data, including any transfers to third parties. The Communique on Obligation to Inform outlines the minimum information to be included in privacy notices. Additionally, based on DPA decisions, privacy notices are expected to clearly specify the types of personal data (and/or categories), the purposes of processing, the legal basis for processing, and the methods used for data collection.
- Implementing technical and administrative measures: Controllers must implement appropriate technical and organisational measures to prevent unlawful processing and unauthorised access, as well as to ensure the protection of personal data.
- Addressing data subject requests: Controllers must promptly address requests from data subjects (and no later than 30 days). If the request is rejected, the response is insufficient, or there is no response within the timeframe, data subjects can file a complaint with the DPA within 30 days of receiving the response or 60 days from the application date.
- Notifying the DPA of data breaches: In the event of a data breach, controllers must notify the DPA immediately and within 72 hours of becoming aware of the breach, where possible. Additionally, controllers must inform affected data subjects as soon as possible, providing them with the necessary details regarding the breach and potential risks to their personal data.

Furthermore, a controller's accountability extends to its processing activities and those of its processors. Per the DP Law, controllers are jointly responsible for ensuring that processors implement the necessary technical and administrative measures while processing data on their behalf. Therefore, in practice, proces-

sors' accountability to the controller should be reinforced through data protection agreements that clearly define the processors' roles, responsibilities, and obligations, with particular emphasis on penalties and indemnity clauses for non-compliance.

### 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 parties – such as IOT service providers, data holders, and data processing service providers – process personal data, the DPA will be responsible for overseeing compliance with the DP Law.

That being said, sector-specific regulations may grant authority to certain regulatory bodies over specific data-related matters.

## 4. Sectoral Issues

### 4.1 Use of Cookies

Under Turkish law, there is no legislation explicitly governing the use of cookies, with the only exception being the Electronic Communications Law (ECL), which includes limited provisions that apply only to electronic communications service providers. According to the ECL, service providers can use cookies only for the purpose of ensuring communication or if subscribers/users are informed about the processing of their data and have provided explicit consent.

To address this gap, in June 2022, the DPA issued its Guidelines on Cookie, Applications ("Cookie, Guidelines"), which includes recommendations on cookie, practices for all controllers. Annexes of the guidelines include a compliance checklist with examples of best practices, such as banner usage and cookie, preference management platforms, as well as a sample cookie, policy.

#### Privacy Notices for Cookies

Controllers must meet the requirements for privacy notices when fulfilling the obligation to inform data subjects about cookies. Therefore, privacy notices regarding cookies should, at least, include the following, per the Communique on Obligation to Inform:

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

Moreover, the Cookie, Guidelines recommend that cookie, privacy notices include information on the name, purpose, duration of the cookies, and whether the cookie, is first-party or third-party.

The Cookie, Guidelines also emphasise that when third-party cookies are used, both the website owner and the third party are responsible for ensuring that users are informed about the cookies and obtaining their consent if required.

#### Legal Bases for Processing

When processing personal data, controllers must satisfy one of the following legal bases as provided by Article 5 of the DP Law:

- explicit consent of the data subject is obtained;

- it is expressly provided for by law;
- it is necessary for the protection of the life or physical integrity of the person (or of any other person who is unable to explain their consent due to physical disability or whose consent is not deemed legally valid);
- processing of personal data of the parties to a contract is necessary, provided that it is directly related to the establishment or performance of the contract;
- it is necessary for compliance with a legal obligation to which the controller is subject;
- personal data has been made public by the data subject themselves;
- data processing is necessary for the establishment, exercise, or protection of any right; and/or
- processing of data is necessary for the legitimate interests pursued by the controller, provided that this processing shall not violate the fundamental rights and freedoms of the data subject.

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.

The Cookie, Guidelines also provide examples of the legal bases controllers may rely on for different types of cookies.

If the use of cookies involves the processing of special categories of personal data, the legal bases provided in Article 6 of the DP Law must be considered (see **4.3. Employment Privacy Law**).

Moreover, the Cookie, Guidelines include several recommendations for cases where controllers obtain data subjects' explicit consent for using cookies. For instance, using consent management platforms that allow data subjects to manage their preferences is cited as a good practice. On the other hand, 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 users must consent to access a website – is considered invalid, as consent must be freely given.

In cases where cookies involve 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 also categorise cookies based on the criteria outlined below.

- Duration – session cookies and persistent cookies.
- Purpose – essential cookies, functional cookies, performance/analytics cookies, and advertising/marketing cookies.
- Parties – first-party cookies (placed by the visited domain) and third-party cookies (placed by external domains).

While these categorisations align with EU practices, there is a key distinction regarding performance/analytics cookies. Unlike the EU, explicit

consent may not be required for first-party analytics cookies if:

- their use is limited to measuring the 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; and
- personal data collected through cookies is not used to track users across multiple sites or devices.

## 4.2 Personalised Advertising and Other Online Marketing Practices

### Online Marketing

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

According to the E-Commerce Legislation, prior approval must be obtained from recipients before making calls or sending SMS or emails for marketing purposes (marketing communication). 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.

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

Marketing communication must include the sender's certain 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 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, to the best of our knowledge, 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.

## 4.3 Employment Privacy Law

Employment privacy is not governed by a specific, standalone regulation in Turkish law. How-

ever, some provisions related to employment privacy are included in diverse laws, such as:

- 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 in accordance with the rules of good faith and law and prohibits disclosing any information that the employee has a justified interest in keeping confidential; and
- Occupational Health and Safety Law mandates that health data must be kept confidential to protect the employee's private life and reputation.

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 specifically 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 (eg, through a privacy notice);
- pursuing a legitimate purpose (eg, a compliance investigation based on a reasonable doubt); and
- observing the principle of proportionality (eg, emails or files should not be opened or reviewed if they are clearly personal).

These principles also apply to the implementation of cybersecurity tools and insider threat detection and prevention programs.

The Constitutional Court also addresses this issue in several decisions. For instance, it examined a case where an employer reviewed an employee's corporate email and used the correspondence to terminate the employment contract. The court noted that the employee's contract specified that the corporate email was for work purposes only and could be monitored by the employer without prior notice. It emphasised that the use of the employee's emails for legal purposes in a judicial process was within reasonable limits and in line with the principle of proportionality. In another decision, the applicant's holiday pictures and emails sent from their corporate accounts were considered 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

As a general principle, controllers should rely on either the legal bases provided by the DP Law or the data subject's explicit consent when processing personal data.

However, 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 power imbalance between the parties, nor the ability to withdraw consent without facing negative consequences. Therefore, controllers should carefully assess whether the requirements for explicit consent are met, particularly for processing activities within an employment relationship.

That said, 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, legal bases for processing special categories of personal data were limited, which posed challenges for controllers, particularly employers processing health data in an employment context. However, with the DP Law Amendments, controllers now have more options and may rely on the following legal bases:

- explicit consent;
- being necessary for the protection of public health, preventive medicine, medical diagnosis, treatment and care services, and the planning, management, and financing of health services by persons under the obligation of secrecy or by authorised institutions and organisations;
- being necessary for the protection of life or physical integrity of a person who cannot express themselves due to an actual impossibility or whose consent is not deemed legally valid or of any other person;
- personal data made public by the data subject themselves, provided that it aligns with their intention to make it public;
- being necessary for the establishment, exercise, or defence of a right;
- being necessary for the fulfilment of legal obligations in the fields of employment, occupational health and safety, social security, social services, and social assistance; or
- being limited to current or former members and affiliates of foundations, associations, or other non-profit organisations or entities established for political, philosophical, religious, or trade union purposes or to persons who are in regular contact with such organisations and entities; provided that it:
  - (a) complies with the legislation applicable to these organisations and entities and aligns with their purposes,
  - (b) remains confined to their fields of activity, and
  - (c) is not disclosed to third parties.

The DP Law Amendments explicitly introduced the employment relationship as a legal basis for processing special categories of data. While this new framework is expected to ease practical challenges, it may not be an ultimate solution, as controllers may rely on this legal basis in very limited cases.

Recently, in February 2025, the DPA published the Guidelines on the Processing of Special Categories of Personal Data, emphasising how these legal bases will be interpreted by the DPA. The guidelines also outline the scope and definitions of special categories of personal data, provide practical real-life examples for applying legal bases to process such data, and specify

the measures data controllers must take to comply with the new DP Law regime.

### 4.4 Transfer of Personal Data in Asset Deals

The DP Law does not contain specific provisions regarding the transfer of personal data in asset deals. As a result, the general principles of the DP Law apply.

#### Legal Bases for Processing

Controllers must ensure they rely on the appropriate legal bases outlined in the DP Law when transferring personal data in asset deals (see **4.1. Use of Cookies** and **4.3. Employment Privacy Law**). If the transfer involves transferring personal data abroad, controllers must also comply with the specific requirements set for international data transfers (see **5.1 Restrictions on International Data Transfers**).

#### Obligation to Inform

In practice, a key challenge is the obligation to inform data subjects. While some controllers include a general statement in their privacy notices about potential data transfers in asset deals, the DPA's general stance is that privacy notices should not include vague references to possible transfers. Instead, if the details of the transfer (eg, what personal data will be transferred, the purposes of the transfer, and the recipients) are already known, data subjects should be informed at the time of data collection.

Unlike the GDPR, the DP Law does not provide an exemption from the obligation to inform in cases where personal data is not directly collected from data subjects. Therefore, in such cases, data subjects should be informed at the latest when their data is transferred.

## 5. International Considerations

### 5.1 Restrictions on International Data Transfers

With the DP Law Amendments, the previous system has been significantly amended. Accordingly, 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, in contrast to its previous position, direct collection of personal data does not constitute data transfer under the new regime.

#### 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 (referred to as the "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 fol-

lowing the review or, in any other cases, it deems necessary. However, since the DPA has not yet established a Whitelist, alternative mechanisms for transferring data abroad must be considered.

### 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 (excluding international treaties) 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;
- 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 date of execution.

As of the time this note is written, only ten controllers have obtained approval for written undertakings, and no BCR has been approved. Therefore, due to the challenges in obtaining approval from the DPA, SCCs have been the most viable option in market practice since their recognition.

The DPA published four versions of SCCs that cover data transfers from:

- controller to controller;
- controller to processor;
- processor to processor; and
- 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. Furthermore, in an announcement on 5 February 2025, the DPA highlighted that both the data exporter's and the data importer's signatures must be present in the column containing the Turkish text.

The SCCs published by the DPA must be executed without any modification, except where explicitly allowed within the relevant sections of the SCCs (eg, details of the transfer, technical and administrative measures, etc). While various practices emerged due to uncertainties arising from the lack of guidance, the Guidelines on Transfers Abroad clarified 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.

While SCCs are not subject to the DPA's approval, there is still an obligation to notify the DPA about the execution of SCCs within five business days from the date of execution. The By-Law on Data Transfers Abroad states that notifications of SCCs can be made physically, via registered electronic mail (KEP), or through other methods determined by the DPA. In this context, on 17

October 2024, the DPA introduced an online "SCCs Notification Module", now available for notifications.

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 the 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 the required authentication of signatures, titles, or seals. Consular or diplomatic officials usually do this verification. However, 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 following criteria is met:

- the data subject has explicitly consented to the transfer after having been informed of the possible risks of such transfer;
- the transfer is necessary for the performance of a contract between the data subject and controller or the implementation of pre-contractual measures taken at the data subject's request;
- the transfer is necessary for the conclusion or performance of a contract concluded between the controller and another natural or legal person in the interest of the data subject;
- the transfer is necessary for an overriding public interest;
- the transfer is necessary for the establishment, exercise, or defence of a right;
- the transfer is necessary for the protection of the life or physical integrity of a person who is unable to give consent due to actual impossibility or whose consent is not legally valid; and
- the transfer is made from a register open to the public or to persons with a legitimate interest, provided that the conditions required to access the registry in the relevant legislation are met and the person with legitimate interest requests it.

The By-Law on Data Transfers Abroad defines occasional transfers as "*transfers that are not regular, occurring only once or a few times, are not continuous and are not in the ordinary course of business.*" The Guidelines on Transfers Abroad also interpret occasional transfers very narrowly, stating that these transfers should occur under unforeseen conditions and provide examples of occasional transfers, largely based on EDPB guidelines.

When relying on explicit consent for an occasional transfer, the data subject must be informed of the specific risks, including the fact 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 are reserved in other laws. For example, 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 details the required information that must be included in an international e-transfer, adding further compliance obligations for financial institutions.

Furthermore, sectoral regulations imposing specific restrictions regarding data transfers abroad should also be considered (see **5.3 Data Localisation Requirements**).

## 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. Except SCCs, these safeguards require the DPA's prior approval.

Furthermore, without prejudice to the provisions of international agreements, in cases where Türkiye's or the data subject's interests will be seriously harmed, personal data may only be transferred abroad upon the DPA's permission. 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 authorisation from the Ministry of Environment, Urbanisation, and Climate Change.

In the health sector, the transfer of personal health data is subject to the Ministry of Health's evaluation in accordance with 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 no standalone legislation governing data localisation exists, certain sector-specific regulations do apply. Key sectors are as follows.

### 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 (excluding services like email, teleconference, or videoconference);
- 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. However, in certain cases, such data may be transferred abroad by obtaining the explicit consent of data subjects.

Moreover, 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 a 2019 decision, 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. ICTA further emphasised that priority should be given to storing essential user data and any other data specified by ICTA within Türkiye.

### Commercial Electronic Message Management System Integrators

Recently, on 18 September 2024, the Communique on Commercial Electronic Message Management System Integrators was published in the Official Gazette. It 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 further stipulates that the information processing system used in integrator services, including software, hardware, and server infrastructure, must be located within a database inside Türkiye.

### Critical Infrastructure Service Providers

The Decree on Information and Communication Security Measures issued by the Presidency of Türkiye (the "Presidency Decree") sets specific measures to mitigate security risks, particularly for critical data that could jeopardise national security or public order if compromised. It mandates that critical infrastructure (eg, energy, electronic communications, banking, transportation) service providers ensure their primary and back-up data systems remain within Türkiye.

The Presidency Decree applies not only to businesses providing critical infrastructure services but also to public institutions and organisations, which must ensure the storage of critical data (eg, population, health and communication records, and genetic and biometric data) within Türkiye.

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

## 5.4 Blocking Statutes

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

## 5.5 Recent Developments

Introduced in March 2024 through DP Law Amendments and came into effect on 1 June 2024, the new regime governing data transfers

abroad is relatively recent and, as such, has presented a variety of practical challenges.

While the By-Law on Data Transfers Abroad has clarified some aspects of the new regime, practitioners eagerly waited for guidance from the DPA, as many points of uncertainty remained. On 2 January 2024, the DPA published its Guidelines on Transfers Abroad, which aimed to offer more clarity on the provisions governing international data transfers. These guidelines addressed certain issues that had sparked differing views among practitioners, particularly regarding the requirements for completing the SCCs process.

Despite the DPA's efforts to clarify some aspects, several issues remain unresolved, and the DPA has indicated that the Guidelines on Transfers Abroad will be reviewed and updated based on practical experience gained through the implementation of the DP Law.

On the other hand, efforts to align with the GDPR are ongoing. According to the Medium-Term Programme (2025–2027), the alignment of the DP Law with the GDPR and other EU legislation is expected to be completed by the final quarter of 2025. The 12th Development Plan (2024–2028) also identifies alignment efforts as a key goal for the coming years.

In practice, the new regime has introduced some challenges but has generally been well-received by practitioners. A key reason for this is that, under the previous legal framework, obtaining approval from the DPA for data transfers was a lengthy and complex process. As a result, controllers had practically no option but to rely on data subjects' explicit consent for data transfers abroad, leading to practical difficulties.

The Guidelines on Transfers Abroad further confirmed the challenges of obtaining DPA approval. They revealed that three applications for BCR had been submitted to the DPA but were rejected due to procedural and substantive deficiencies. Furthermore, only ten requests for written undertakings have been approved by the DPA.

Consequently, while SCCs should be notified to the DPA, they have become a more viable approach for many businesses as they do not require prior approval from the DPA. On the other hand, since SCCs cannot be executed on a multiparty basis, some practitioners have argued that executing individual SCCs with each party is impractical, especially for businesses working with multiple service providers or partners across borders.

However, these arguments have diminished as several service providers have taken the initiative to prepare and implement SCCs for their clients. Yet, in sectors dominated by a few major players, controllers often find themselves in a "take it or leave it" situation, with limited room for negotiation. This imbalance in bargaining power further exacerbates the challenges faced by smaller companies.

## 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