

CHAMBERS GLOBAL PRACTICE GUIDES

Data Protection & Privacy 2024

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

Türkiye: Law & Practice

Bora Yazıcıoğlu, Kübra İslamoğlu Bayer,
Simge Yüce and İdil Kula
YAZICIOGLU Legal



TÜRKIYE

Law and Practice

Contributed by:

Bora Yazicioğlu, Kübra İslamoğlu Bayer, Simge Yüce and İdil Kula
YAZICIOĞLU Legal



Contents

1. Basic National Regime p.5

- 1.1 Laws p.5
- 1.2 Regulators p.6
- 1.3 Administration and Enforcement Process p.7
- 1.4 Multilateral and Subnational Issues p.8
- 1.5 Major NGOs and Self-Regulatory Organisations p.8
- 1.6 System Characteristics p.9
- 1.7 Key Developments p.9
- 1.8 Significant Pending Changes, Hot Topics and Issues p.9

2. Fundamental Laws p.12

- 2.1 Omnibus Laws and General Requirements p.12
- 2.2 Sectoral and Special Issues p.15
- 2.3 Online Marketing p.20
- 2.4 Workplace Privacy p.20
- 2.5 Enforcement and Litigation p.21

3. Law Enforcement and National Security Access and Surveillance p.23

- 3.1 Laws and Standards for Access to Data for Serious Crimes p.23
- 3.2 Laws and Standards for Access to Data for National Security Purposes p.23
- 3.3 Invoking Foreign Government Obligations p.23
- 3.4 Key Privacy Issues, Conflicts and Public Debates p.24

4. International Considerations p.24

- 4.1 Restrictions on International Data Issues p.24
- 4.2 Mechanisms or Derogations That Apply to International Data Transfers p.24
- 4.3 Government Notifications and Approvals p.25
- 4.4 Data Localisation Requirements p.25
- 4.5 Sharing Technical Details p.25
- 4.6 Limitations and Considerations p.26
- 4.7 "Blocking" Statutes p.26

5. Emerging Digital and Technology Issues p.26

- 5.1 Addressing Current Issues in Law p.26
- 5.2 "Digital Governance" or Fair Data Practice Review Boards p.26
- 5.3 Significant Privacy and Data Protection Regulatory Enforcement or Litigation p.26
- 5.4 Due Diligence p.26
- 5.5 Public Disclosure p.26
- 5.6 Digital Technology Regulation/Convergence of Privacy, Competition and Consumer Protection Laws (Including AI) p.27
- 5.7 Other Significant Issues p.27

YAZICIOĞLU 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. Yazıcıoğlu Legal has a dedicated team of 13 lawyers working on data pro-

tection 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. 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 in Yazıcıoğlu Legal. He has significant experience in 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 and Acer in Türkiye.



Kübra İslamoğlu Bayer is a senior managing associate in Yazıcıoğlu Legal. She advises clients on data protection, e-commerce and cybersecurity laws. She is an active member of the Istanbul Bar Association's IT Law Commission: Artificial Intelligence Study Group, and the Data Protection Commission. Furthermore, Kübra is the founder and general co-ordinator of the KOIOS Data Protection Law Study Group and manages a website dedicated to data protection law.



Simge Yüce is a mid-level associate in Yazıcıoğlu Legal. She mainly focuses on data protection and e-commerce laws. Simge is a member of the Istanbul Bar Association's Data Protection Commission and the KOIOS Data Protection Law Study Group.



İdil Kula is a legal intern in Yazıcıoğlu Legal. She focuses on various areas of law including data protection and e-commerce.

YAZICIOGLU Legal

NidaKule – Goztepe
Merdivenköy Mahallesi Bora
Sokak No:1
Kat:7 34732 Kadıköy / İstanbul
Türkiye

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



1. Basic National Regime

1.1 Laws

The right to protection of personal data is regulated under the Constitution of the Turkish Republic (the “Constitution”) as an individual right, 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 be processed only if the processing is allowed by the law, or if the data subject gives their explicit consent. The article finally states that the procedures and principles of processing personal data must be regulated by the law.

The Turkish Data Protection Law

Pursuant to Article 20(3) of the Constitution, Turkish lawmakers enacted the Turkish Data Protection Law No 6698 (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 by considering only EU Directive 95/46/EC. Currently, efforts are underway to align DP Law with the GDPR. As part of these efforts, the Law on Amendments to the Criminal Procedure Law and Certain Laws (which includes also DP Law Amendments) was published in the official gazette on 12 March 2024 (see **1.8 Significant Pending Changes, Hot Topics and Issues**).

Important secondary regulations issued by the Personal Data Protection Authority (DPA) include:

- the By-Law on the Deletion, Destruction or Anonymisation of Personal Data;
- the By-Law on the Registry of Controllers;

- the Communiqué on Principles and Procedures to Be Followed in Fulfilment of the Obligation to Inform;
- the Communiqué on Principles and Procedures for the Request to Controllers;
- processing of genetic data;
- good practices on personal data protection in the banking sector;
- cookie practices;
- processing of biometric data;
- artificial intelligence (AI);
- preparing an inventory of personal data processing;
- fulfilment of the obligation to inform;
- technical and organisational measures;
- deletion, destruction or anonymisation of personal data; and
- the concepts of controller and processor.

In addition, the Personal Data Protection Board (DPB) adopts resolutions, which are published on the DPA's website and/or in the Official Gazette.

Turkish Criminal Law

Certain actions, which violate protection of personal data, are defined as crimes in the Turkish Criminal Code (TCrC) (see **2.5 Enforcement and Litigation**).

Turkish Civil Law

Personal data is considered a part of personality under Turkish law; hence it is also protected under the protection of personality rights in the Turkish Civil Code (TCiC).

Other

There is also some sector-specific legislation on the processing of personal data in certain sectors, such as the telecommunications, banking, electronic payment, health and education sectors.

Currently, there is no specific legislation dedicated solely to AI. However, an exception exists in Additional Article 1 of the Regulation on Remote Identification Methods Used by Banks and the Establishment of Contractual Relationships in the Electronic Environment. This provision grants authority to the Banking Regulation and Supervision Agency (BRSA) to establish principles and procedures for ID verification transactions conducted by customer representatives using AI-based methods. The BRSA has not yet regulated this issue.

Moreover, the DPA released Recommendations on the Protection of Personal Data in the Field of Artificial Intelligence (the "Recommendations on AI"), highlighting concerns associated with the utilisation of AI in processing personal data.

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 to safeguard the rights of data subjects.

The decision-making body of the DPA is the DPB. Some of the main duties and powers of the DPB are as follows:

- conducting investigations following complaints of data subjects or ex officio if it becomes aware of the alleged violation, 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 the 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 and the relevant foreign country that undertakes to provide adequate protection, when adequate protection is not provided, for the purpose of international data transfers.

The Ministry of Trade is authorised to oversee marketing communication.

Apart from the above, sector-specific administrative institutions such as the BRSA, the Capital Markets Board, the Turkish Republic Central Bank and the Information and Communication Technologies Authority (ICTA) have authority to regulate issues regarding AI and the processing of personal data within their respective sectors. However, there is no specific authority solely dedicated to regulating AI matters in Türkiye.

1.3 Administration and Enforcement Process

The DPB may initiate investigations either 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 DPB may request information and/or documents from controllers during its investigations. Controllers must provide this information and/or documents within 15 days, unless they constitute a state secret. The DPB may request further information and/or documents, and on-site inspection during an investigation.

Administrative Fines

If the DPB identifies a violation of the DP Law, it can impose administrative fines, which may vary between TRY47,303 and TRY9,463,213 depending on the type of violation.

As per the Misdemeanours Law No 5326, when determining fines, the DPB must consider the severity of the breach, the fault of the breaching party and its economic condition.

Administrative Orders

The DPB may also order the controller to bring processing activities in compliance with the DP Law.

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 which are difficult or impossible to compensate for, and the act would be clearly unlawful.

When the DPB issues an order to a controller to bring its processing activities into compliance with the DP Law, this decision must be implemented without any delay and, at the latest, within 30 days upon receipt of the notification by the controller.

Appealing a Sanction

Controllers have the right to appeal against the DPB's decisions.

If the DPB's decision includes only an administrative fine, the controller may object to this decision before the Magistrates' Court within 15 days from receipt of the decision. The decisions of the Magistrates' Court can be appealed to another Magistrates' Court in the same district.

Where the DPB's decision includes an administrative order bundled with or without an administrative fine, the controller can object to the decision before the administrative courts, whose decisions can be appealed to the Council of State.

However, the DP Law Amendments foresees that the DPB's decisions with administrative fines will be appealed before administrative courts rather than Magistrates' Court as of 1 June 2024 (see **1.8 Significant Pending Changes, Hot Topics and Issues**).

1.4 Multilateral and Subnational Issues

Türkiye does not belong to any multinational system such as the European Union (EU) or the European Economic Area. However, the European system has a highly noticeable effect on DP Law practice.

Türkiye was one of the first countries to become a member of the Council of Europe and signed Convention No 108 in 1981, ratifying it in 2016, shortly before the adoption of the DP Law. However, Türkiye has not yet signed the Modernised Convention (also known as Convention 108+).

As a candidate member state of the EU, Türkiye aims to align its national legislation with the EU acquis. As outlined in the Medium-Term Programme adopted by the Presidential Decree on 6 September 2023 (the "Medium-Term Programme"), the alignment process of the DP Law with EU legislation (particularly with the GDPR) is expected to conclude in the final quarter of 2024 (see **1.8 Significant Pending Changes, Hot Topics and Issues**).

The National Artificial Intelligence Strategy for 2021–2025 introduced by the Turkish government in August 2021 (the "National AI Strategy")

underscores Türkiye's dedication to keeping pace with global advancements in AI, promoting partnerships, actively participating in international research endeavours, and strengthening connections between the domestic AI community and stakeholders worldwide.

Furthermore, as a member state of the Council of Europe, Türkiye initially held membership in the Ad hoc Committee on Artificial Intelligence (CAHAI) between May 2019 and December 2021, and joined the Committee on Artificial Intelligence in February 2022 following the dissolution of CAHAI. Türkiye joined the Global Partnership on Artificial Intelligence, as of 22 November 2022. Additionally, as a member, Türkiye adheres to the studies and recommendations made by the OECD.

1.5 Major NGOs and Self-Regulatory Organisations

Certain industry-specific organisations and chambers of commerce/industry have created working groups to assist their members in complying with the DP Law and in working on AI-related matters.

Among these working groups, the Data Protection Association founded in 2018 plays an active role in addressing practical challenges arising from the implementation of the DP Law, and organises numerous meetings where scholars and practitioners convene to and discuss pertinent topics in the field.

Additionally, established as an independent association in February 2021, the Artificial Intelligence Policy Association stands out as the first non-governmental organisation dedicated to AI in Türkiye, with the aim of raising awareness about AI.

1.6 System Characteristics

Türkiye follows the EU omnibus model. The DP Law draws a framework for the DPA and controllers by providing a general perspective of the obligations and principles that must be sought for data-processing activities. The DPA steers data-processing practice by regulating secondary legislation and publishing guidelines and/or the DPB's resolutions.

The DPA aims to take a proportionate approach to enforcement, prioritising cases with a significant risk of harm to individuals. The amounts of the administrative fines set forth in the DP Law are considerably lower than those set forth in the GDPR. However, the DPA's tendency for enforcement is relatively higher, in particular on data breaches, when compared to its European counterparts.

1.7 Key Developments

Key developments in Türkiye in the past 12 months are as follows:

- the adoption of the DP Law Amendments (see **1.8 Significant Pending Changes, Hot Topics and Issues**);
- the DPB's decisions approving the undertakings of two more entities for data transfers abroad;
- publication of the Guidelines on the Protection of Personal Data in Election Activities;
- publication of the Guidelines on the Processing of Republic of Türkiye Identity Numbers;
- publication of the Guidelines on Recommendations for Protecting Privacy in Mobile Applications;
- publication of the Guidelines on Issues to be Considered in the Processing of Genetic Data (the "Genetic Data Guidelines").

- announcement on obtaining explicit consent from customers in physical stores via SMS verification codes (see **2.3 Online Marketing**).

1.8 Significant Pending Changes, Hot Topics and Issues

Amendments to the DP Law

The 12th Development Plan (2024–2028), issued on 31 October 2023 by the Presidency of the Republic of Türkiye, envisages the alignment of the DP Law with the GDPR (along with other EU legislation) as one of the major goals for upcoming years.

As per the Medium-Term Programme, the alignment of the DP Law is expected to be completed by the final quarter of 2024.

The DP Law Amendments regarding some most problematic articles were recently published in the official gazette as of 12 March 2024.

DP Law Amendments enter into force on 1 June 2024, and foresee a specific transition period for personal data transfers abroad, based on the explicit consent of data subjects, until 1 September 2024.

The DP Law Amendments have brought significant changes regarding the processing of special categories of personal data, transfer of personal data abroad, and procedures for appealing against DPB decisions.

However, in addition to these amendments, there is also an expectation for broader amendments regarding the DP Law.

Legal grounds for processing special categories of personal data

The DP Law Amendments have introduced five alternative legal bases for processing special

categories of personal data, in addition to existing three legal bases (see **2.2 Sectoral and Special Issues**) applicable to all special categories of personal data as follows:

- 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; and
- for current or former members and affiliates, or individuals who are in regular contact with the foundation, association, and other non-profit organisations or formations established for political, philosophical, religious, or trade union purposes, provided that it is in accordance with the legislation and purposes they are subject to, limited to their field of activity, and not disclosed to third parties.

The previous differentiation among special categories of personal data will no longer apply, and all conditions stipulated in the article will uniformly apply to all special categories of personal data.

Transfer of personal data abroad

The DP Law Amendments foresees a gradual and alternative regime for international transfers of personal data, comprising three levels of transfers based on:

- adequacy decisions,

- appropriate safeguards,
- occasional causes.

In the current DP Law, transfer of personal data abroad is allowed if the data subject's explicit consent is obtained. However, with DP Law Amendments, explicit consent will only be permissible if the data transfer abroad is occasional. Explicit consent obtained for the transfers of personal data abroad will be considered compliant with DP Law until 1 September 2024. After this date, circumstances allowing data transfers abroad based on explicit consent will be restricted.

Parallel to the current DP Law, adequacy decisions remain a valid legal basis for transferring data abroad. The amendments grant the DPB the ability to issue adequacy decisions not only for countries but also for international organisations and specific sectors within third countries. Given that the DPB has yet to establish a Whitelist, it is expected that these amendments will not affect current practices.

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 primarily four established 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 DPB's approval;

- Binding Corporate Rules (BCR), subject to the DPB's approval;
- Standard Contractual Clauses (SCCs) announced by the DPB, with a requirement for notification to the DPB within five 5 business days from the date of the signature of the SCCs; and
- a written undertaking containing provisions that will provide adequate protection, subject to the DPB's approval.

If occasional data transfers abroad occur without an adequacy decision, and if one of the appropriate safeguards cannot be ensured, the data transfer abroad is possible under the condition that the transfer is not repetitive 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 transfers;
- 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 data subject's request;
- the transfer is necessary for the conclusion or performance of a contract concluded between controller and another natural or legal person in the interest of 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 the person who is unable to give themselves consent due to actual impossibility or whose consent is not legally valid; and
- the transfer is made from a register that is 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.

It is crucial to underline that the regulations specified in the DP Law Amendments regarding the personal data transfer abroad and to international organisations also extend to onward transfers conducted by either controllers or processors.

Procedures For appealing against DBP decisions

In the current version of the DP Law, controllers have the right to object to the decision of the DPB before administrative courts only if such decision involves an administrative order. If not, appeals must be made to the Magistrates' Court (see **1.3 Administration and Enforcement Process**).

With the introduction of the DP Law Amendments, administrative courts will be the sole appellate courts.

AI

Published in September 2021, the Recommendations on the Protection of Personal Data in AI (Recommendations on AI) stands as the sole guideline issued by the DPA pertaining to the use of AI in data-processing activities.

The National AI Strategy emphasises international legislative studies' significance and Türkiye's commitment to this field but lacks clarity on its legislative modification objectives.

Developing an ethical-legal framework to address the evolving requirements in AI is outlined as a key goal in the 12th Development Plan.

Geographic Data Rules

Depending on the scope of their activity, natural persons and legal entities engaged in processing geodata were required to seek permits and licences from the Ministry of Environment, Urbanisation and Climate Change (the “Ministry of Environment”). The Ministry of Environment was responsible for regulating the principles and procedures for obtaining such permits.

The Constitutional Court nullified the provisions granting the Ministry of Environment authority to define the scope, duration, procedures, principles and content of permits. The basis for nullification was the lack of adequate specification of the Ministry’s powers in the legislation.

Genetic Data

The Genetic Data Guideline published by the DPA in October 2023 refers to the GDPR for defining genetic data, and outlines conditions for processing data and limitations on its transfer abroad. Controllers must offer detailed privacy notices, separate from general ones, covering processing casueses and risks of cross-border transfers. The guideline stresses the importance of explicit consent and warn against making genetic data processing a prerequisite for services.

2. Fundamental Laws

2.1 Omnibus Laws and General Requirements

Territorial Applicability

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

However, based on the DPB’s decisions, it seems it is of the view that when the relevant data-processing activities are realised in Türkiye or related to data subjects located in Türkiye, the DP Law shall be applicable. In an unpublished decision, the DBP emphasised that the territorial scope provisions of the TCrC should serve as the basis for applying administrative fines defined under the DP Law. This implies that if the behaviour or the result occurs in Türkiye, the DP Law shall be applicable.

Obligation to Register With VERBIS (Controllers’ Registry)

Controllers who meet certain criteria set out by the DP Law are obliged to register with VERBIS. Such controllers are those:

- established in Türkiye and who have equal to or more than 50 employees, or whose total annual financial balance sheet is equal to or more than TRY100 million;
- established in Türkiye and who have less than 50 employees and an annual financial balance of less than TRY100 million, but whose main activity is processing special categories of personal data; and
- established outside Türkiye.

To register with VERBIS, controllers based outside Türkiye are required to appoint a representative to represent controllers before the DPA and data subjects. The representative may be either a Turkish citizen or a legal person in Türkiye.

Those obliged to register with VERBIS should also appoint a “contact person”, who may only be a natural person in Türkiye and is mainly responsible for submitting certain information to VERBIS and facilitating the communication between the DPA and controllers.

Data Protection Principles

The general principles for all data-processing activities are as follows:

- lawfulness and fairness;
- being accurate and kept up to date where necessary;
- being processed for specified, explicit and legitimate purposes (purpose limitation);
- being relevant, limited and proportionate to the purposes for which it is processed (data minimisation); and
- being stored for the period laid down by relevant legislation or the period required for the purpose for which the personal data is processed (storage limitation).

Lawful Basis for Processing of Personal Data

To ensure that the data processing is lawful, controllers must satisfy one of the following legal bases (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 life or physical integrity of the person themselves, 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

- 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.

Lawful Basis for Processing of Special Categories of Personal Data

See 2.2 Sectoral and Special Issues.

Privacy Impact Analyses

Data protection impact assessments are not specifically regulated in the DP Law, but may be considered a technical and organisational measure that controllers should take as per the DPA's guidelines.

Application of the “Privacy by Design” or “Privacy by Default” Concepts

The DP Law does not include the concepts of “privacy by design” or “privacy by default”. However, as per the DPB's decisions, controllers are required to apply the “privacy by design” and/or “privacy by default” concepts to comply with the DP Law, particularly with the general principles and data-processing conditions it sets forth.

Internal or External Privacy Policies

Controllers must provide privacy notices to data subjects. Such privacy notice must at least include:

- the identity of the controller and its representative (if any);
- the purpose(s) of the processing of personal data;
- to whom and for which purposes the processed personal data may be transferred;
- the method and legal basis of the collection of personal data; and
- the rights of data subjects.

Moreover, the DPA expects personal data (and/or categories of personal data), purposes, legal basis and collection methods to be matched in privacy notices.

Controllers who are obliged to register with VERBIS are also obliged to:

- maintain a data-processing inventory; and
- adopt a Personal Data Retention and Destruction Policy, as detailed under the By-Law on the Deletion, Destruction or Anonymisation of Personal Data.

Further, as per the DPB's decisions, controllers are also required to maintain:

- procedures on responding to data breaches; and
- a specific privacy policy for the processing of special categories of data.

Except for the above, controllers are not directly obliged to adopt internal or external privacy policies. However, the DPB considers having internal and external privacy policies on data protection and cybersecurity as one of the organisational measures that controllers should take. Thus, it is recommended to adopt internal and external privacy policies.

Anonymisation, De-identification and Pseudonymisation

The DP Law obliges controllers to erase, destroy or anonymise personal data, ex officio or upon the request of the data subject(s), if the purposes for the processing no longer exist.

The DP Law and the By-Law on the Deletion, Destruction or Anonymisation of Personal Data define the concept of anonymisation as a technique that is used to ensure that personal data

cannot be associated with an identified or identifiable natural person under any circumstances, even if it is matched with other data.

A reference to de-identification is made in the By-Law on Processing of Personal Health Data (the "By-Law on Health Data") issued by the Ministry of Health. The By-Law on Health Data mandates health data controllers to implement partial de-identification measures, such as masking medical details, to safeguard data subjects' identities in printed materials and to prevent unauthorised access.

Similarly, the Regulation on the Sharing of Confidential Information issued by the BRSA refers to the concepts of anonymisation, aggregation, and de-identification as a security measure to be applied within the scope of the data processing if intended purposes can still be achieved following their application, particularly during the sharing of secrets.

Pseudonymisation is not specifically referred to in any legislation, but the DPA considers pseudonymised data as personal data, and regards pseudonymisation as one of the technical and organisational measures that controllers must take.

Injury or Harm

There is no requirement under the DP Law for any "harm" or "injury" to be proved for non-compliance with the DP Law, from an administrative law or criminal law perspective.

However, for a data subject to seek compensation from a controller (or processor) due to its non-compliance with the DP Law, such data subject must prove that they have been harmed or injured (see 2.5 Enforcement and Litigation).

Data Breach Notification Process

Unlike under the GDPR, pursuant to the DP Law, controllers are obliged to notify the DPB of all data breaches, regardless of whether there is a risk to the rights and freedoms of natural persons.

The notification must be made to the DPA within 72 hours of the controller becoming aware of the incident, and to the data subjects who are affected by the breach within the shortest time possible.

Rules on Profiling, Microtargeting, Automated Decision-Making, Online Monitoring or Tracking, Big Data Analysis, AI and Algorithms

According to the DP Law, the “data subject has the right to object to the occurrence of a result against themselves by analysing the data processed solely through automated systems”. This right may be at stake in cases of big data analytics, automated decision-making, profiling or microtargeting, AI (including machine-learning) and autonomous decision-making (including autonomous vehicles). However, the application sphere of this provision has not yet been clarified by the DPB.

Apart from the above provision, there are no specific regulations concerning profiling, automated decision-making, online monitoring or tracking, big data analysis, AI or algorithms. Therefore, the general rules apply.

Data Protection Officers (DPOs)

Unlike under the GDPR, there is no requirement to appoint a DPO for any controller, in the public or private sectors. Neither the representative nor the contact person may be considered to have the same role as the DPO in the GDPR.

The DPA published the Communiqué on Principles and Procedures of the Mechanism About Personnel Certification on 6 December 2021. Even though the concept of a DPO defined in this Communiqué seems similar to the concept of the GDPR's DPO, the DPA announced that the DPO in the Communiqué has a different role.

The Union of Turkish Bar Associations requested the annulment of the Communiqué from the court on the grounds that, according to the Attorneys Act, only lawyers can advise on Turkish law. The approach of the court remains to be seen.

2.2 Sectoral and Special Issues Special Categories of Personal Data

According to the DP Law, special categories of personal data are as follows:

- racial or ethnic origin;
- political opinions;
- philosophical, religious, sect or other beliefs;
- clothing and attire;
- association, foundation or trade union membership;
- health and sexual life;
- criminal convictions and security measures on individuals; and
- biometric and genetic data.

Special categories of personal data may be processed if the data subject's explicit consent is obtained.

Except for data on health and sexual life, special categories of personal data may only be processed without the data subject's explicit consent in the cases provided by law.

Data on health and sexual life may be processed by the persons subject to a confidentiality obligation (eg, doctors) or competent public insti-

tutions and organisations (eg, hospitals) for the following purposes:

- protection of public health;
- operation of preventative medicine;
- medical diagnosis;
- treatment and care services;
- planning and management of health services; and
- financing of healthcare services.

For the amendments on special categories of personal data see **1.8 Significant Pending Changes, Hot Topics and Issues**.

In 2018, the DPB issued a resolution requiring controllers to implement additional technical and organisational measures to ensure adequate protection when processing special categories of data are processed, such as adopting a separate processing policy and implementing two-factor authentication for remote data access.

In 2021, the DPB published a guideline on biometric data. The guideline provides a definition of biometric data, and mentions general principles as well as technical and organisational measures in addition to those mentioned above.

In 2023, the DPA published the Genetic Data Guideline (see **1.8 Significant Pending Changes, Hot Topics and Issues**). The guideline refers to additional technical and organisational measures to be taken when processing genetic data.

Problems With Processing Health Data

The above-mentioned limited legal basis for the processing of health data challenges controllers, particularly in an employment context.

In certain situations, such as absence due to sickness, occupational sickness or workplace

accidents, employers need to process the health data of employees in the course of the employment relationship. In fact, the Occupational Health and Safety Law No 6331 (OHCL) requires employees to do so. However, due to limitations on the legal basis for processing health data as per the DP Law, employers can process health data:

- via an occupational doctor, which is not always a viable option in practice; or
- by obtaining explicit consent from their employees.

However, obtaining employees' explicit consent creates a significant problem considering explicit consent must be freely given and can be withdrawn anytime.

The amendments incorporate specific legal provisions regarding the fulfilment of legal obligations in areas such as employment, occupational health and safety, social security, social services, and social assistance, thereby addressing this issue (see **1.8 Significant Pending Changes, Hot Topics and Issues**).

Employment Data

There is no detailed legislation in Türkiye except for Article 419 of the Turkish Code of Obligations (TCO), Article 75 of the Turkish Labour Law (TLL) and Article 15(5) of the OHCL, which draw the framework for employers when processing their employees' personal data (see **2.4 Workplace Privacy**). Thus, the general rules apply.

Children's Data

Unlike under the GDPR, there is no special provision in the DP Law on the collection or processing of minors' personal data. Only the By-Law on Health Data sets forth the parents' right to access their child's health data.

However, the DPB stated that personal data is strictly considered as an element of personal rights. Thus, a minor who has the power of discernment, as well as the legal representative of the minor, should be able to exercise data protection rights according to the TCiC.

The DPB imposed a fine on TikTok – among others – for failing to take necessary measures to protect children’s data. It particularly, it focused on the protection of data of children under age 13, a criterion not included in the DP Law. Hence, in the authors’ view, the grounds for this decision are debatable.

Additionally, the Guideline on Practices of Cookies (the “Cookie Guideline”) advises tailoring cookie privacy notices for children-targeted websites to their comprehension level, possibly using images. Social network providers (SNPs) must offer segregated services for children as well.

Due to the lack of concrete legislation, and despite the DPB’s above-mentioned decisions and guidelines, the questions as to whether minors may give consent for processing personal data without obtaining their legal representative’s approval – and, if so, which age group is considered to have the power to give consent by themselves – is not crystal clear.

It is important to note that, according to the revised Regulation on Preschool and Primary Education Institutions by the Ministry of National Education on 14 October 2023, written permission both from parents and students supervised by the school counsellor is necessary for publishing images taken during in-school and out-of-school activities.

Confidential Customer Data in the Banking Sector

Except for certain exemptions or as otherwise stipulated by law, personal data specific to banking relationships is also considered as customer secrets under Article 73 of the Banking Law. This information cannot be disclosed or transferred to third parties that are either in Türkiye or abroad, without receiving a request or explicit instruction from the customer to do so, even if the customer’s explicit consent to transfer personal data to a third party is obtained as per the DP Law. This provision is highly criticised in Turkish data protection practice.

Based on its assessment on economic security, the BRSA is authorised to:

- ban disclosing or transferring of any kind of data abroad, including customer secrets or bank secrets, to third parties; and
- order banks to keep the information systems and back-ups that are used in carrying out their activities in Türkiye (obligation of data localisation).

In addition, the Guideline on Good Practices for Personal Data Protection in the Banking Sector, published by the DPA in July 2022, refers to technical and organisational measures to be taken for transfer of customer secrets.

Insurance Data

The By-Law on the Collection, Storage and Sharing of Insurance Data defines insurance data as “all data related with insurance contracts, insurer and insurance companies’ parties of an insurance contract, insureds, beneficiaries and other third parties who directly or indirectly benefit from an insurance contract, and that consists of a basis for risk assessment”. It sets forth the

principles for processing and sharing insurance data.

Internet, Streaming and Video Issues

The Law on Regulation of Publications on the Internet and Combating Crimes Committed by Means of Such Publication No 5651 (the “Internet Law”) sets forth obligations for hosting/platform providers, content providers and access providers, such as obligations relating to the removal of unlawful content (see **1.8 Significant Pending Changes, Hot Topics and Issues**, and under **Social Media** below).

However, the Constitutional Court has nullified certain provisions of the Internet Law, effective from 10 October 2024. If there is no legislative change by this date, natural persons and legal entities claiming that their personality rights were violated by online content will not be able to request its removal from hosting providers or apply to the Magistrates’ Court for the removal of and/or blocking of access to such content. Furthermore, decisions regarding the removal of and/or blocking of access to content related to the listed crimes specified under the law will be restricted, limited only to access-blocking measures and with administrative fines applicable solely to access providers.

Voice Telephony, Text Messaging and Content of Electronic Communications

Personal data processed in the telecommunications sector is subject to the By-Law on Processing of Personal Data and Protection of Confidentiality in the Electronic Communications Sector, in line with the DP Law. However, this By-Law includes more specific provisions on traffic and location data.

Voice communications and text messages are protected under the fundamental right to pri-

vacy (Article 20) and freedom of communication (Article 22) of the Constitution. Certain types of crimes are defined in the TCrC to protect communication secrecy and private life. Only under specific and very limited circumstances, and by a judge’s or public prosecutor’s decision in the cases of peril in delay, is it permitted to intervene in private communication (see **3.1 Laws and Standards for Access to Data for Serious Crimes**).

Cookies and Other Similar Technologies

Electronic Communications Law No 5809 includes a provision on cookies. However, such provision is only applicable to electronic communications service providers.

There is no specific provision on cookies under the DP Law, the DPA published a Cookie Guideline in June 2022.

Social Media

According to the Press Law and Further Laws (the “Disinformation Law”) amendments, SNPs must set up a complaint mechanism in co-operation with the ICTA for removal of hashtags and featured content. Failure to remove illegal content within four hours of notification could result in liability for SNPs.

SNPs with daily access exceeding one million must report hashtags, algorithms for featured or reduced content, advertisements, and transparency policies to the ICTA, along with measures taken to enable users to update their preferences regarding suggested content and options provided to users for limiting the use of personal data. Applicants can request content removal for personality rights violations, with these SNPs being required to respond within 48 hours.

The Disinformation Law also places other obligations on SNPs, such as data retention (see **4.4 Data Localisation Requirements**).

The nullification of certain provisions of the Internet Law by the Constitutional Court may affect certain obligations imposed on SNPs under the Disinformation Law. Consequently, unless there is a legislative amendment, these obligations may cease to be valid as of 10 October 2024 (see under **Internet, Streaming and Video Issues** above).

There is no specific regulation regarding browsing data, viewing data, beacons, tracking technology, behavioural or targeted advertising, search engines, large online platforms and intermediary liability for user-generated content. Thus, the general provisions of the DP Law apply to processing activities that deal with such data or technologies. Nonetheless, the Draft Guideline on Loyalty Programmes places significant importance on establishing certain principles for processing of data via location-tracking technologies.

Addressing Hate, Discrimination and Deepfake

According to the Constitution and TCRC, everyone – regardless of their language, race, nationality, skin colour, gender, political opinion, philosophical belief, religion or sect, etc – is equal before the law.

The TCRC criminalises and penalises with imprisonment certain acts which aim to incite hate and/or discrimination between persons based on language, race, nationality, skin colour, gender, disability, political opinion, philosophical belief, religion or sect, etc.

While there is no specific regulation on deepfakes, its use in criminal activities may lead to punishment. The input data for deepfakes, such as voice or images, falls under personality rights and personal data regulations, with general provisions applying in such cases.

In its Deepfake Memorandum released in January 2024, the DPA also outlined that the use of deepfake technology could lead to criminal charges.

Data Subject's Rights

Data subjects' rights are as follows:

- learning whether their personal data is processed or not;
- requesting information as to whether their personal data has been processed or not;
- learning the purpose(s) of the processing of their personal data and whether such personal data is used in compliance with the purpose or not;
- finding out the third parties to whom their personal data is transferred, in-country or abroad;
- requesting rectification of any incomplete or inaccurate data;
- requesting erasure or destruction of their personal data under the conditions referred to in Article 7 of the DP Law;
- requesting information about third parties to whom their personal data has been transferred;
- objecting to the occurrence of a result against themselves by analysing the data processed solely through automated systems; and
- claiming compensation for the damage arising from the unlawful processing of their personal data.

Unlike under the GDPR, a data portability right is not set forth in the DP Law.

Automated Decision-Making

There is no specific regulation in the DP Law regarding profiling and automated decision-making – apart from the provision that regulates a data subject’s right to “object to the occurrence of a result against themselves by analysing the data processed solely through automated systems” – nor has there been any public DBP decision on the subject.

Right to Be Forgotten

Currently, no specific legislation in Türkiye regulates the “right to be forgotten”. However, it is accepted by Constitutional Court and Court of Cassation decisions that data subjects have the right to be forgotten. Also, the DPA published an opinion on the right to be forgotten and made a resolution that outlined the criteria on exercising this right.

2.3 Online Marketing

Online marketing is governed by the Law on Regulation of Electronic Commerce No 6563 (the “E-Commerce Law”) and the By-Law on Commercial Communication and Commercial Electronic Messages (the “By-Law on Commercial Communication”), as well as by the DP Law.

According to the E-Commerce Law and the By-Law on Commercial Communication, the recipient’s prior approval must be obtained to make calls or send SMS or emails for marketing purposes (marketing communication). The DPB also seeks data subjects’ explicit consent for controllers to send push messages.

However, it is permissible to make a marketing communication without prior consent in the

business-to-business (B2B) model, unless the receiver opts out.

The contents of a marketing communication must include certain identification information of the sender, as well as an option to opt out.

The Message Management System (MMS) is an online platform where receivers can manage their approvals for receiving marketing communications and withdrawals therefrom (ie, opt-outs). All senders of marketing communications must register with the MMS and upload the information regarding the approvals/withdrawals for this purpose. Any approval or withdrawal received by the sender must be uploaded to the MMS within three business days upon their receipt.

The DPA has recently published a public announcement on obtaining explicit consent for electronic commercial messages during in-store shopping via SMS verification codes, which only permits the sending of such SMS after the completion of the shopping process.

There are no specific provisions for behavioural and targeted advertising under Turkish law. Therefore, the relevant processing activities are subject to general provisions of the DP Law. In this regard, based on the DPB’s approach to this matter, it may be argued that prior explicit consent of the data subjects must be obtained in order to carry out behavioural or targeted advertising.

2.4 Workplace Privacy

Privacy in the workplace is not specifically regulated in Turkish law, but can be considered within the scope of the DP Law.

There are also provisions regarding this matter in various laws, for example:

- pursuant to Article 419 of the TCO, an employer can use the personal data of their employee only to the extent that it is necessary for the employee's employability or for the performance of the employment contract;
- pursuant to Article 75 of the TLL, an employer is obliged to use the information obtained about their employee in accordance with the rules of good faith and law, and to not disclose any information that the employee has a justified interest in keeping confidential; and
- pursuant to Article 15(5) of the OHCL, health data must be kept confidential in order to protect the private life and reputation of the employee who has undergone a medical examination.

Monitoring Workplace Communications

According to the decisions of the Constitutional Court and DPB, an employer is entitled to monitor the work computers, work mobile phones and other electronic devices which it provides to its employees, provided that it fulfils the following conditions:

- providing information to employees in advance (eg, by way a privacy notice addressed to the employees);
- pursuing a legitimate purpose (eg, a compliance investigation based on a reasonable doubt); and
- observing the principle of proportionality (eg, if it is clear from the subject of the email/file that it is a personal email/file, it should not be opened and reviewed).

These principles shall also be applied to the implementation of cybersecurity tools, insider threat detection and prevention programmes.

Processing Special Categories of Personal Data

As a general principle for processing special categories of employees' personal data, the explicit consent of employees must be obtained unless a justifying ground is provided by laws (see **2.2 Sectoral and Special Issues**).

The DP Law amendments explicitly foresee employment relationship as a legal ground for processing special categories of data which can be viewed as a positive step addressing a contemporary need in the employment sphere (see **1.8 Significant Pending Changes, Hot Topics and Issues**).

2.5 Enforcement and Litigation Regulators

Under the DP Law, the DPB has extensive enforcement powers, as described in **1.3 Administration and Enforcement Process**. The DPB arguably has a higher tendency for imposing administrative fines compared to its EU counterparts, especially for data breaches.

So far, the DPB has investigated and fined several national and international companies, including Marriot International Inc, Facebook, Amazon Türkiye, WhatsApp and TikTok.

The DP Law outlines four types of violations with administrative fine amounts for these violations subject to annual adjustment each year. At time of writing in 2024:

- failure to inform data subjects of processing activities may be subject to an administrative fine of TRY47,303 to TRY946,308;
- failure to take the necessary technical and organisational measures (interpreted very broadly and including unlawful data transfer abroad, breach of fundamental principles)

may be subject to an administrative fine of TRY141,934 to TRY9,463,213;

- failure to comply with the decisions issued by the DPB may be subject to an administrative fine of TRY236,557 to TRY9,463,213; and
- failure to comply with the obligation to register with VERBIS and failure to submit information to VERBIS may be subject to an administrative fine of TRY189,245 to TRY9,463,213.

The DP Law Amendments introduced a new administrative fine. Failure to notify the DPB within five business days following the signature of the SCCs by either controller or processor result in an administrative fine ranging from TRY50,000 to TRY1,000,000 (see **1.8 Significant Pending Changes, Hot Topics and Issues**). Unlike other failures stipulated in the DP Law where only controller is responsible, for this failure both controller and processor will be liable.

The highest fine issued by the DPB to date is TRY2.65 million, separately imposed on WhatsApp and Meta.

The DPB is also entitled to decide to cease certain data-processing activities or personal data transfers (see **1.3 Administration and Enforcement Process**). The DPB is known to sporadically exercise its enforcement authority.

Criminal Sanctions

There are also criminal sanctions regulated under the TCRC, 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 the need for any complaint – ie, ex officio by public prosecutors. However, there is no established jurisprudence on how criminal sanctions will be harmonised with the DP Law.

Private Litigation

The right to seek compensation is clearly stated as one of the data subject's rights under the DP Law.

Moreover, as per the TCiC and the TOC, data subjects can seek compensation and ask courts to:

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

A controller is jointly liable for the lack of technical and organisational measures which must be taken by the processor, from a civil law perspective.

There is no concept of class action under the Turkish legal system.

3. Law Enforcement and National Security Access and Surveillance

3.1 Laws and Standards for Access to Data for Serious Crimes

The following activities are among those excluded from DP Law coverage:

- processing of personal data by judicial authorities or execution authorities regarding the investigation, prosecution, judicial or execution proceedings; and
- processing of personal data by public institutions and organisations duly authorised and assigned by law regarding maintaining national defence, national security, public security, public order or economic security within the scope of preventative, protective and intelligence activities.

The Turkish Law of Criminal Procedure is the primary source with respect to law enforcement's access to data for the investigation of serious crimes.

Other relevant laws are as follows:

- the Law on Police Duty and Authority;
- the Law on Gendarmerie Organisation Duty and Authority;
- the Law on Governmental Intelligence Services and National Intelligence Agency; and
- the Internet Law.

Law enforcement authorities may request information on personal data when investigating criminal offences.

However, in certain situations, an independent judicial decision is necessary for public prosecutors and law enforcement officers to interfere with IT systems or intercept communications.

In the case of peril in delay, the public prosecutor or law enforcement officer may interfere with IT systems or intercept communications by the public prosecutor's order, which must be approved by a court afterwards.

3.2 Laws and Standards for Access to Data for National Security Purposes

Similar rules to those discussed in **3.1 Laws and Standards for Access to Data for Serious Crimes** apply in the national security realm. In these cases, the authorities can demand information if it is necessary for the prevention of imminent threats.

The National Intelligence Agency is authorised to request any information within its powers and duties, including any personal data. Those who fulfil these requests cannot be held legally or criminally liable.

Although there have been no practical implications at the time of writing, Türkiye is also a signatory state to the OECD's Declaration on Government Access to Personal Data Held by Private Sector Entities dated 14 December 2022.

3.3 Invoking Foreign Government Obligations

The provisions of the DP Law do not provide a clear legitimate basis for invoking a foreign government's request for collecting or transferring data. However, since the fulfilment of a foreign government's request may lead to data transfer abroad, the rules on data transfer abroad set forth in the DP Law must be complied with (see **4.2 Mechanisms or Derogations That Apply to International Data Transfers**).

Furthermore, Türkiye is a signatory to many bilateral or multilateral agreements which aim to promote co-operation between states, especial-

ly on issues related to judicial co-operation and extradition requests. Personal data-processing activities that arise from these obligations are not exempted from the scope of the DP Law, and public institutions are also obliged to comply with the DP Law (see **2.1 Omnibus Laws and General Requirements, 2.2 Sectoral and Special Issues and 4.2 Mechanisms or Derogations That Apply to International Data Transfers**).

Türkiye does not participate in a Cloud Act agreement with the USA.

3.4 Key Privacy Issues, Conflicts and Public Debates

A key privacy issue is inadequate and uncertain regulations about governmental access to data. Although the DP Law is applicable to data processing activities of governmental bodies, the broad exceptions outlined within it are criticised. As this causes the application of the DP Law within governmental bodies to be interpreted as extenuated, which does not facilitate accurate implementation.

Compared to the GDPR, many issues are completely left out of the scope of the DP Law. This is criticised in Turkish data protection practice.

4. International Considerations

4.1 Restrictions on International Data Issues

International transfer of personal data is subject to the DP Law (see **4.2 Mechanisms or Derogations That Apply to International Data Transfers**).

The DP Law states that provisions on data transfer abroad in other laws are reserved. On the other hand, sector-specific regulations may

impose further restrictions regarding data transfer abroad (see **4.4 Data Localisation Requirements**).

Based on its decisions, the DPB also seems to consider direct collection of personal data by controllers located abroad as data transfer abroad, which is, in the authors' view, a debatable approach.

4.2 Mechanisms or Derogations That Apply to International Data Transfers

According to the DP Law, the transfer of personal data abroad is permissible if the data subject's explicit consent is obtained for such transfer.

If the exporter relies on any legal basis other than explicit consent, the following applies.

- The foreign country to which the personal data will be transferred must have an adequate level of protection for personal data. Such countries will be determined and announced by the DPB (ie, the "Whitelist").
- If there is not an adequate level of protection, an exporter controller in Türkiye and data importer abroad must execute a written undertaking to commit to providing an adequate level of protection, similar to Standard Contractual Clauses in GDPR practice (ie, undertaking). Then, such undertaking must be submitted to the DPB, for the approval of the relevant data transfer.
- If the data transfer abroad is only within multinational group companies, a data exporter located in Türkiye may obtain approval from the DPB for binding corporate rules (BCR).

As a Whitelist has not yet been announced by the DPB, only consent, undertakings and BCR remain for controllers to transfer data abroad. However, in several decisions the DPB states

that “the provision of a service cannot be made conditional upon consent”. This principle is based on the argument that if the provision of a service is made conditional upon obtaining consent for data processing (including transfer), such consent is deemed to be not freely given, and hence may be considered as invalid.

Although obtaining valid explicit consent has its own challenges, obtaining regulatory approval from the DPB is just as challenging. Only seven controllers have managed to obtain regulatory approval by executing an undertaking since the enactment of the DP Law.

The set of rules governing international data transfers has been revised with the DP Law Amendments. These amendments will come into effect on 1 June 2024. However, controllers have the option to rely on explicit consent for the transfer of personal data abroad until 1 September 2024 (see **1.8 Significant Pending Changes, Hot Topics and Issues**).

4.3 Government Notifications and Approvals

As mentioned in **4.2 Mechanisms or Derogations That Apply to International Data Transfers**, undertakings and BCRs require the DPB’s approval.

Moreover, as per Article 9(5) of the DP Law, without prejudice to the provisions of international agreements, in cases where the interest of Türkiye or the data subject shall be seriously harmed, personal data may only be transferred abroad upon permission of the DPB. The DPB must obtain the opinions of relevant public institutions and organisations before it grants its permission.

It should be noted that sector-specific regulations may seek further notifications or approvals regarding data transfer abroad (see **2.2 Sectoral and Special Issues**).

4.4 Data Localisation Requirements

Even though there is no data localisation requirement in the DP Law, there are certain sector-specific regulations in Türkiye.

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 (except for services such as email, teleconference or videoconference);
- certain public companies, as well as certain capital markets institutions; and
- financial lease, factoring and finance companies.

Electronic Communications Providers

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

Social Network Providers (SNPs)

SNPs whose daily access is more than one million must take necessary measures to retain data of their Turkish users in Türkiye.

4.5 Sharing Technical Details

Public or private institutions that will use coded/encrypted electronic communication within their electronic communications services must apply

to the ICTA and obtain permission in order to be authorised in accordance with the ICTA's regulations. A copy of the code/encryption must be provided to the ICTA with this application.

4.6 Limitations and Considerations

There are no specific limitations or considerations that apply to an organisation for collecting or transferring data in connection with foreign government data requests and foreign litigation proceedings.

See 3.3 **Invoking Foreign Government Obligations** and 4.2 **Mechanisms or Derogations That Apply to International Data Transfers**.

4.7 “Blocking” Statutes

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

5. Emerging Digital and Technology Issues

5.1 Addressing Current Issues in Law

The DPA issued its Recommendations on AI in September 2021. It is noteworthy that the Recommendations on AI do not provide a detailed view on AI technologies, even though they succeed in covering certain fundamental topics.

Biometric data has been a point of further discussion in the field of data protection, and the processing of biometric data has been assessed extensively in both DPA-issued documents and DPB decisions (see 2.4 **Workplace Privacy** for the use of biometric data in an employment context).

5.2 “Digital Governance” or Fair Data Practice Review Boards

Establishing protocols for digital governance and fair data practice review boards or committees to address the risks of emerging or disruptive digital technologies is not a mandatory and/or common practice in Türkiye.

5.3 Significant Privacy and Data Protection Regulatory Enforcement or Litigation

In a landmark decision dated 15 December 2023, the Constitutional Court examined a Magistrates' Court's assessment of a DPB decision and asserted that the DPB decisions weren't adequately reviewed by the Magistrates' Court's as the appellate authority.

5.4 Due Diligence

Conducting due diligence over a target entity is considered to be on the legal basis of “legitimate interest”.

When requesting and sharing personal data during a due diligence process, “proportionality” and “data minimisation” principles must be taken into consideration.

If a due diligence process requires data transfer abroad, the controller must comply with provisions regarding transferring data abroad. It should be noted that using virtual data rooms, whose servers are located abroad, would constitute a data transfer abroad (see 4.2 **Mechanisms or Derogations That Apply to International Data Transfers**).

5.5 Public Disclosure

VERBIS is an online public registry, which shows the personal data processing inventory of controllers who have registered with, and submitted

information to, VERBIS (see **2.1 Omnibus Laws and General Requirements**).

The information, which is submitted to VERBIS and is hence publicly available, is as follows:

- the categories of personal data;
- the data-processing purposes for each data category;
- retention periods of each data category;
- data subjects for each data category;
- data transferees;
- information on data transfer abroad, for each data category; and
- technical and organisational measures.

The relevant capital markets regulations impose an obligation on companies which will make a public offering to state the risks of the business before such public offering. Although there is no specific requirement to state the risks on data protection and cybersecurity, since these may also include risks regarding data protection, such risks should be mentioned during a public offering.

5.6 Digital Technology Regulation/ Convergence of Privacy, Competition and Consumer Protection Laws (Including AI)

In 2022, the E-Commerce Law and its secondary legislation was amended with the aim of maintaining an effective and fair competition environment on e-commerce platforms.

These amendments impose significant obligations on e-marketplaces and e-sellers. Some of these obligations reflect certain principles brought in by the Digital Services Act.

According to these amendments, e-marketplaces shall:

- remove unlawful content submitted by the seller;
- not lower the seller's position in the ranking or recommendation system without any objective criteria set forth in the agreement executed with the seller;
- not use the data obtained from sellers and buyers with a purpose other than providing intermediary services, in particular to compete with sellers; and
- provide technical facilities, free of charge, to the seller for transferring the data they collected through their sales and for accessing the processed metadata.

The amendments have adopted an incremental system based on total transaction number and net transaction volume per year for the obligations, and non-compliance with these obligations is subject to administrative monetary fines. These fines vary between TRY10,000 and TRY40 million, and certain fines are calculated on a percentage basis, varying between 0.0005% and 10% of the net sales amount of the preceding year.

Although not yet ratified, significant amendments are anticipated in the Law on Protection of Competition No 4054 to enhance alignment with the European omnibus model. Most of the amendments introduced by the draft amendment reflect the ex-ante approach of the Digital Markets Act, and include certain definitions introduced thereby.

5.7 Other Significant Issues

There are no other significant issues.

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 Katie.Burrington@chambers.com