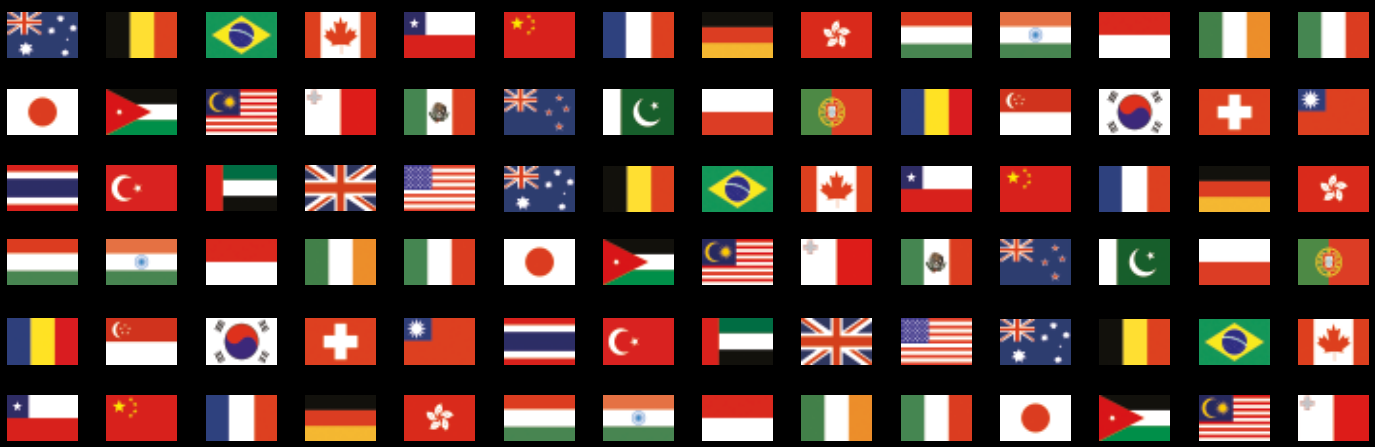
DATA PROTECTION & PRIVACY 2023

Contributing editors
Aaron P Simpson and Lisa J Sotto



LEXOLOGY
Getting the Deal Through

Publisher
Tom Barnes
tom.barnes@lbresearch.com

Subscriptions
Claire Bagnall
claire.bagnall@lbresearch.com

Head of business development
Adam Sargent
adam.sargent@gettingthedealthrough.com

Published by
Law Business Research Ltd
Meridian House, 34-35 Farringdon Street
London, EC4A 4HL, UK

First published 2012
Eleventh edition
ISBN 978-1-83862-997-7

Printed and distributed by
Encompass Print Solutions
Tel: 0844 2480 112

DATA PROTECTION & PRIVACY 2023

Contributing editors
Aaron P Simpson and Lisa J Sotto
Hunton Andrews Kurth LLP

Lexology Getting the Deal Through is delighted to publish the eleventh edition of *Data Protection & Privacy*, which is available in print and online at www.lexology.com/gtdt.

Lexology Getting the Deal Through provides international expert analysis in key areas of law, practice and regulation for corporate counsel, cross-border legal practitioners, and company directors and officers.

Throughout this edition, and following the unique Lexology Getting the Deal Through format, the same key questions are answered by leading practitioners in each of the jurisdictions featured. Our coverage this year includes new chapters on South Korea and United Arab Emirates.

Lexology Getting the Deal Through titles are published annually in print. Please ensure you are referring to the latest edition or to the online version at www.lexology.com/gtdt.

Every effort has been made to cover all matters of concern to readers. However, specific legal advice should always be sought from experienced local advisers.

Lexology Getting the Deal Through gratefully acknowledges the efforts of all the contributors to this volume, who were chosen for their recognised expertise. We also extend special thanks to the contributing editors, Aaron P Simpson and Lisa J Sotto of Hunton Andrews Kurth LLP, for their continued assistance with this volume.

LEXOLOGY
Getting the Deal Through

London
July 2022

Contents

Turkey

Esin Çamlıbel, Beste Yıldızili Ergül, Naz Esen and Canberk Taze

Turunç

LAW AND THE REGULATORY AUTHORITY

Legislative framework

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

The Turkish Constitution has specifically protected PI since 2010.

The protection of PI has also been regulated by specific legislation, namely the Personal Data Protection Law (PDPL), Law No. 6698, which came into force in October 2016. Directive 95/46/EC is the starting point for the PDPL. Even though there are various differences between the PDPL and the EU General Data Protection Regulation (GDPR), the PDPL is generally based on, and follows, the GDPR.

Turkey is a party to the Convention for the Protection of Individuals with regard to Automated Processing of Personal Data of 1981 of the Council of Europe. The Convention was published in the Turkish Official Gazette in March 2016 and became domestic law.

Crimes against data protection and related sanctions are also regulated by the Turkish Criminal Code.

Data protection authority

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

The authority responsible for overseeing the implementation of the PDPL is the Personal Data Protection Authority (the Authority). The Authority is responsible, among other things, for monitoring the latest developments in legislation and practice, making evaluations and recommendations, conducting researches and analyses, and cooperating with public institutions and organisations, international organisations, non-governmental organisations, professional associations and universities.

The Data Protection Board (the Board) is formed within the Authority and has the following duties, among others:

- ensuring that personal data are processed in compliance with the PDPL, and fundamental rights and freedoms;
- promulgating rules and regulations under the PDPL;
- determining administrative sanctions under the PDPL;
- reviewing complaints of PDPL violations;
- taking necessary measures against PDPL violations at its discretion;
- setting a strategic plan for the Authority;
- determining the purpose, targets, service quality standards and performance criteria of the Authority;
- determining additional measures for the processing of sensitive personal data;
- determining specific rules regarding data security, and the duties, powers and responsibilities of data controllers;
- providing comments on legislation and rules drafted by other institutions and organisations that include personal data provisions; and
- approving and publishing periodic reports on the performance, financial situation, annual activities and other matters related to the Authority.

Cooperation with other data protection authorities

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

The Authority is the solely authorised institution under the PDPL. The PDPL tasks the Authority with monitoring and evaluating international developments on personal data issues, and cooperating with international organisations and foreign counterparts.

Despite the limited number of decisions the Board has issued since its formation, the visible trend is that the Board takes decisions of the European Data Protection Board (EDPB) into account when investigating cases. However, there is no mechanism to prevent the Board from taking decisions diverging from those of the EDPB.

Breaches of data protection law

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

Breaches of the PDPL can lead to both administrative fines and criminal penalties. The Board is responsible for ensuring that personal data is processed in compliance with fundamental rights and freedoms, and reviewing complaints of data subjects. The Board can take temporary measures and other adequate measures, such as monetary sanctions, against violations.

In addition, criminal acts such as the unlawful acquisition or registration of personal data, and non-destruction of personal data when required may be subject to criminal penalties under the Turkish Criminal Code.

1.5 Judicial review of data protection authority orders

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

Data subjects can appeal against orders of the Authority to criminal courts of peace within 15 days of the delivery of the decision.

SCOPE

Exempt sectors and institutions

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

The Personal Data Protection Law (PDPL) applies to all natural persons whose personal data is processed. It also applies to all natural and legal persons who process such data using fully or partially automated means, provided that they are part of a data registry system (the 'filing system' under the EU General Data Protection Regulation), through non-automated means. There is no distinction foreseen between private sector institutions and state institutions. As such, the PDPL applies to all types of entities and persons.

However, the PDPL does not apply in the following cases:

- processing by natural persons within the scope of activities relating to either themselves or their family members living in the same household, on the condition that the data is safeguarded and not provided to third parties;
- anonymised processing for statistical, research, planning and similar purposes;
- processing for the purposes of art, history, literature and science, or as part of the exercise of freedom of speech, provided the processing does not prejudice national defence, national security, public order, public safety, economic security, privacy and other personal rights, or constitute a crime;
- processing within the scope of preventive, protective and intelligence activities by state institutions carrying out national defence, national security, public order, public safety or economic security functions; and
- processing by judicial authorities or execution authorities in relation to investigations, prosecutions, court cases, criminal proceedings, and execution and enforcement proceedings.

Interception of communications and surveillance laws

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

No, the PDPL does not directly cover interception of communications, electronic marketing or monitoring and surveillance of the individuals. However, the Data Protection Board (Board) has issued a decision regarding the regulation of contacting individuals via email, SMS or phone calls to make advertisements, where it held that such communications are subject to the same principles under the PDPL as apply to other data processing. Accordingly, these types of communications can be made only based on consent or in reliance on an exemption.

Turkey has specific legislation that covers the interception of communications, electronic marketing, and monitoring and surveillance of individuals. For example, the Law on Electronic Communication regulates all electronic communication methods while the Law on Electronic Trade regulates electronic marketing and trade. The Regulation on Erasure, Destruction and Anonymisation of Personal Data and the Communiqué on Rules and Procedures for the Fulfilment of the Obligation to Inform determine the rules and procedures to be applied to interception of communications, electronic marketing, and monitoring and surveillance of individuals. The Board has also published guidance regarding electronic communications bearing personal information and deemed it necessary for data controllers to take reasonable measures to verify the contact information declared by the relevant data subjects (eg, sending a verification code or link to the person's registered phone number or email address). Per the Board's approach, keeping personal data accurate and up-to-date is both in the interest of the data controller and necessary to protect the fundamental rights and freedoms of the data subject. In addition, channels must be made available at all times for data subjects to update their personal data. The Criminal Code and Criminal Procedural Law regulate the sanctions in case of breach of the applicable legislation.

Other laws

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

There are specific rules that outline data protection rules for various areas. For example, Turkish Labour Law holds that employers are obliged to use the personal data of employees in good faith and accordance with applicable law, and not to disclose any personal data in which an employee has a legitimate interest and has requested to be kept private.

Another example is the Regulation on Processing and Maintaining Privacy of Personal Health Data, regulating the rules and procedures to be used while processing data involving health information.

Turkish Banking Law, the Law on Payment and Security Agreement Systems, Payment Systems and Electronic Currency Organisations and the Law on Bank Cards and Credit Cards regulate the processing and transfer of financial data in Turkey and abroad.

Turkish telecommunications legislation also has provisions regarding data processing and transfers.

PI formats

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

The PDPL does not limit the scope of protection by categories or types. All information relating to an identified or identifiable natural person maintained and stored in any format is covered by the PDPL and secondary legislation promulgated thereunder. However, there are specific provisions in the PDPL that regulate sensitive personal data as 'special categories of personal data'.

Extraterritoriality

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

The PDPL makes no differentiation between data subjects who are nationals or not. The PDPL applies to all natural persons whose personal data are processed.

However, there are specific rules that apply to the transfer of personal data outside of Turkey. As a general rule, personal data cannot be transferred abroad without the explicit consent of the data subject. However, personal data may be transferred abroad without the explicit consent of the data subject provided that one of the conditions specified in the PDPL is met, and that:

- adequate protection is provided in the foreign country where the data are to be transferred (the Board has the authority to determine the countries where an adequate level of protection is deemed to be provided although it has not done so yet); or
- where adequate protection is not provided, the controllers in Turkey and the relevant foreign country guarantee sufficient protection in writing, and the Board authorises such transfer (although data requiring data subject's explicit consent in Turkey will continue to require such consent and will not be automatically covered by the approved undertaking); or
- approved binding corporate rules are followed (although data requiring data subject's explicit consent in Turkey will continue

to require such consent and will not be automatically covered by such rules).

Hence, the applicability of the PDPL is not limited to Turkey.

Covered uses of PI

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

The PDPL covers all processing and use of personal data. Certain distinctions are made among the owners, controllers and processors concerning their duties and liabilities.

LEGITIMATE PROCESSING OF PI

Legitimate processing – grounds

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

As a general rule, personal data cannot be processed without the explicit consent of the data subject. However, if one of the following conditions is met, personal data may be processed without seeking the explicit consent of the data subject:

- the processing is clearly provided for by applicable law;
- the processing is necessary to protect the life or bodily integrity of a person who is unable to give consent due to actual impossibility or whose consent is not legally recognised, or the life or bodily integrity of another person;
- the processing is necessary for the formation or performance of a legal contract to which the data subject is a party;
- the processing is necessary to comply with a legal obligation to which the data controller is subject;
- the data has been made public by the data subject;
- the processing is necessary to establish, use or protect a legal right; and
- the processing is necessary for the purposes of legitimate interests pursued by the controller, provided that the fundamental rights and freedoms of the data subject are not harmed.

Pursuant to the Data Protection Board's (the Board) recent decisions, data processors can request the explicit consent of the data owners only if the above circumstances are not present.

Legitimate processing – types of PI

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

Under the Personal Data Protection Law (PDPL), personal data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, clothing choices and habits, trade union membership, health, sex lives, criminal convictions and security measures, and biometric or genetic information are defined as 'sensitive personal data'. As a general rule, these categories of data cannot be processed without the consent of the data subject, except where permitted or required by applicable law.

Further, personal data relating to health and sex lives may be processed without the explicit consent of the data subject only by persons or authorised public institutions and organisations that have confidentiality obligations, and only to protect public health, the administration of preventive medicine, medical diagnosis, treatment and care services, and the planning, management and financing of healthcare services.

Processing of data must comply with the purposes stated in the data processing notification. If the processor decides to process the data for any reason other than those stated in the data processing notification, a new notification stating the new purpose must be provided to the data subject.

The Board has issued heightened measures for the safekeeping and processing of sensitive personal data. These measures include, among others, training programmes, encryption requirements, two-factor authentication for remote access, and physical security measures, such as access controls.

DATA HANDLING RESPONSIBILITIES OF OWNERS OF PI

Transparency

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

When processing personal data, the controller or the person authorised by the controller is obliged to inform the data subjects. The notification must include:

- the identity of the controller and its representative, if any;
- the purpose of the data processing;
- to whom and for what purposes the processed data may be transferred;
- the method and legal basis for the collection of the personal data; and
- the rights of the data subjects accorded by the Personal Data Protection Law (PDPL).

The notification must be provided at the time of the acquisition of the data and must use easy-to-understand clear and plain language. If the personal data are obtained from a third party (ie, not the data subject), the notification must be made within a reasonable time after the data are obtained, at the time of first contact if obtained for the purpose of communication, and at the time of first transfer if obtained for the purpose of transferring.

Exemptions from transparency obligations

15 When is notice not required?

A notice is not required if:

- processing of the personal data is necessary to prevent a crime or for a criminal investigation;
- the data subject has himself or herself made the personal data public;
- processing of the personal data is required for supervisory, regulatory or disciplinary activities to be carried out by public institutions and professional associations with public institution status; or
- processing of the personal data is required for the protection of the state's economic and financial interests with regard to budgetary, tax-related and financial issues.

Data accuracy

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

Personal data must be:

- processed lawfully and fairly;
- accurate and, where necessary, kept up to date;
- collected for specified, explicit and legitimate purposes;

- relevant and limited to the purposes for which they are processed; and
- retained only for the period stipulated by relevant legislation or the purpose for which they are processed.

Data minimisation

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

According to the PDPL, the amount of data processed must be proportional to the purpose of the processing, and the amount must be as small as possible. Any data processing that exceeds the scope of the purpose for which it was collected is unlawful. Data controllers must avoid processing data that is disproportionate to achieving the purpose of the processing (eg, avoid processing sensitive personal data when hiring, as the same purpose could be achieved without processing any or by only processing minimal personal data).

Data retention

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

There is no restriction on the amount of personal data that may be held. However, personal data can be preserved only for the time periods foreseen in the applicable regulations or time periods necessary for the purpose of the processing.

In addition, the amount of data and the length of time the data may be held for must be proportional to the purpose of the processing, and both the amount of PI and the length of time must be as small as possible.

While determining the maximum storage period, the following must be taken into account:

- generally accepted storage periods in the sector in which the data controller operates;
- the length of time the legal relationship with the data subject that is the basis of the processing will continue for;
- the length of time that the legitimate interest of the data controller in accordance with lawfulness and fairness principles will continue for;
- the length of time during which the risks, costs and responsibilities arising from the storage of the relevant data category will legally continue for;
- whether the intended maximum storage period is suitable to keep the relevant data category accurate and up to date;
- the length of time during which the data controller is obliged to store the data pursuant to its legal obligations; and
- the period of limitation determined by the data controller for the assertion of a right relating to personal data in the relevant data category.

Those data controllers who are obliged to register with the Data Controllers' Registry, known as VERBİS, are also obliged to prepare a data inventory, as well as data preservation and destruction policies, which set forth, among other things, the periods during which personal data will be preserved.

Data controllers who are required to prepare data preservation and destruction policies must erase, destroy or anonymise, as applicable, the relevant data in regular intervals upon the triggering of such obligation. These periods cannot exceed six months. On the other hand, for data controllers who are not required to prepare data preservation and destruction policies, this time period cannot exceed three months.

Records of all erasure, destruction and anonymisation activities must be kept and stored for at least three years (subject to any other applicable legal obligations).

Purpose limitation

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

Yes, the purposes for using the personal data must be determined and the data subject accordingly informed when obtaining the consent of the data subject. Data controllers cannot exceed or circumvent these purposes. Further, regardless of whether the processing of PI is based on the consent of the data owner or a legitimate ground not requiring consent, the processing purposes must be disclosed to the data subjects.

Data controllers are bound by the purposes stated in the relevant notification. Unless it is explicitly permitted by the PDPL, data controllers cannot use the data collected other than for the purposes clearly disclosed while collecting the data. Hence, if the collected data will be used for a new purpose requiring consent, data controllers are obliged to provide a new notification and to obtain a separate consent of the data subject. If the new purpose is based on one of the legitimate grounds under the PDPL (ie, no consent is necessary), data controllers still have to provide the data subject with a new notification that includes the new purpose.

Automated decision-making

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

There is no prohibition for using automated decision systems or making automated decisions without human intervention. The general principles of the PDPL, such as informing the data subject, shall always apply.

Additionally, as per the PDPL, data subjects can always object to the results of automated decision-making.

SECURITY

Security obligations

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

Data controllers are obliged to take all necessary technical and administrative measures to provide a sufficient level of security. Data controllers must also conduct necessary inspections or have them conducted in their own institutions. While there are no specific standards established for the technical and administrative measures to be used, the relevant guidelines of the Data Protection Board (the Board) set forth various possible data security measures. These measures include, among other things, establishing a data matrix, using closed-circuit systems, using firewalls and anti-virus programs, and implementing data security policies.

Notification of data breach

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

Under the Personal Data Protection Law, in cases where the processed data is obtained by third parties through unlawful methods, the controller must notify the data subject and the Board as quickly as possible and, in

any event, within 72 hours. Where necessary, the Board may announce such breach on its official website or through other methods it deems appropriate.

INTERNAL CONTROLS

Accountability

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

Under the Personal Data Protection Law (PDPL), data controllers are obliged to implement all necessary technical and administrative precautions to maintain data security. While the legislation does not specifically include an obligation to maintain internal controls, data controllers who are obliged to register with the Data Controllers' Registry are also obliged to prepare data preservation and destruction policies, which must contain, among other things, extensive information on how the data will be processed internally. The Data Protection Board (the Board) also recommends signing confidentiality agreements with the employees in case of a data breach.

Further, if an international company adopts binding corporate rules, and these rules are approved by the Board to transfer personal data abroad without the explicit consent of the data subject, the company and other companies in its group will be required to set up an internal compliance mechanism in accordance with the law.

Data protection officer

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

The PDPL does not foresee an obligation for appointing a data protection officer. However, the Board recently published the Communiqué on Procedures and Principles of Personnel Certification Mechanism (the Communiqué) and the Programme on Certification of Data Protection Personnel (Programme). The Communiqué and the Programme explain the certification process of data protection personnel in terms of competence and procedural requirements for accreditation. For example, data protection personnel must pass a written exam and meet the minimum requirements determined by the Board to obtain their certificates. Although the obligations of data protection personnel have not been set yet, the Board is laying the legal groundwork to implement a similar function to that of a data protection officer in the near future.

Record-keeping

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

The PDPL does not contain a provision regarding a general obligation to maintain internal records. However, data controllers and processors who process personal data by automated means are obliged to register with the Data Controllers' Registry and establish a personal data processing inventory, which must include the purpose and the legal reason for the processing, the data category, to whom the data will be transferred, the period of preservation, data to be transferred abroad, and the precautions taken for data security.

Those data controllers who are obliged to register with the Data Controllers' Registry are also obliged to prepare data preservation and destruction policies, which set forth, among other things, the periods during which personal data will be preserved.

In addition to the PDPL, the Law on Electronic Communications and related regulations oblige licensed operators within the electronic communications sector to maintain certain records relating to electronic communications. Licensed operators are also under an obligation to keep access records of personal data for two years.

Risk assessment

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

Data controllers are at all times obliged to take all necessary technical and administrative measures to provide a sufficient level of security. However, the Board particularly focuses on whether the personal data is sensitive, as well as the confidentiality level of the data and the possible damage to the data subject in the event of a security breach. While there are no specific standards established for the technical and administrative measures to be used, the relevant guidelines of the Board set forth various possible data security measures. These measures include, among other things, informing employees regarding possible security breaches, establishing a data matrix, using closed-circuit systems, using firewalls and anti-virus programs, and implementing data security policies.

Design of PI processing systems

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

The Board has issued heightened measures for the safekeeping and processing of sensitive personal data. However, there are no specific obligations as such in relation to PI processing systems outside of sensitive personal data.

REGISTRATION AND NOTIFICATION

Registration

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

As a general rule, data controllers are required to register with the Data Controllers' Registry (VERBİS). The Data Protection Board (the Board) has exempted, through various decisions, the following data controllers from the registration requirement:

- data processors who are part of a data registry system (the 'filing system' under the EU General Data Protection Regulation) and process data only in non-automated ways;
- associations, foundations and unions resident in Turkey, to the extent they process data in compliance with relevant legislation and their purposes, and in any case, limited to their areas of activity;
- political parties;
- lawyers;
- mediators;
- notaries public;
- certified public accountants;
- customs brokers; and
- employers who employ fewer than 51 people and whose annual net assets do not exceed 25 million Turkish lira, provided their primary line of business is not the processing of sensitive personal data.

Data controllers who are not exempt from the obligation to register must register with VERBİS at verbis.kvkk.gov.tr. As part of the registration process, data controllers must appoint a contact person and

complete the form provided by the Personal Data Protection Authority. If the data controller is in a foreign country, a data controller representative resident in Turkey must be appointed.

The following information must be registered with VERBİS by the data controller:

- the identity and address of the data controller and of its representative (if any);
- the purpose for which the personal data will be processed;
- explanations relating to the groups of data subjects and the relevant data categories of the subjects;
- the recipients or groups of recipients to whom the personal data may be transferred;
- the personal data envisaged to be transferred abroad;
- the measures taken concerning the security of the personal data; and
- the maximum storage period necessary for the purpose for which the personal data are processed.

Registration and renewals are not subject to any fees.

Persons who fail to comply with the obligation to register with and maintain proper entries on VERBİS may be sanctioned with a monetary fine between 50,000 Turkish lira and 2.7 million Turkish lira by the Board.

Other transparency duties

29 | Are there any other public transparency duties?

Public companies have a general duty to disclose information on events that may affect their investors' decisions. While this requirement is not specifically regulated for data processing, matters relating to data privacy will need to be disclosed if sufficiently material. There are no other transparency duties; data processors are only obliged to notify the data subjects as required by the PDPL and register with VERBİS when the applicable conditions are met.

SHARING AND CROSS-BORDER TRANSFERS OF PI

Sharing of PI with processors and service providers

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

The Personal Data Protection Law (PDPL) foresees special conditions for the domestic transfer of personal data. Personal data normally cannot be transferred without a legitimate ground specified in the PDPL or the explicit consent of the data subject. Hence, the data controller must notify the data subject that personal data will be transferred to third parties providing outsourced processing services, and obtain the data subject's consent if the transfer is not based on a legitimate ground (such as advertising purposes). If the data subject denies providing consent and the processing is not based on a legitimate ground, the applicable personal data must be destroyed (or, if applicable consent or grounds exist, used by the data processor without the involvement of the outsourced service). Further, for personal data required to be preserved pursuant to various legislation, data owners are required to establish a system for preserving such personal data without transferring it to third parties.

The PDPL also requires that data owners who use outsourced processing services provide sufficient protection with regard to the processing and preservation of personal data. In the event of a breach, data owners are jointly and severally liable with the entities providing outsourced processing services for the compensation of any damages.

Restrictions on third-party disclosure

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

As a general rule, there are no specific restrictions foreseen on the sharing of personal data apart from the general requirements on notifying and informing the data subject, obtaining the data subject's consent (except the conditions specified in the PDPL pursuant to which personal data can be transferred within Turkey without obtaining explicit consent) as to what data will be disclosed, and determining the purposes for which the data shall be disclosed.

However, for sharing sensitive personal data, the Data Protection Board (the Board) has set forth additional precautions and restrictions. These include the transfer of data in an encrypted format and for hard copies of the data to be labelled as classified. In addition, it is mandatory to obtain the data owner's consent unless the processing is required by law. In its guidelines, the Board specifically refers to the selling of sensitive personal data as a data breach, and Turkish Criminal Law states that the person who gives, distributes or seizes personal data unlawfully is punished with imprisonment from two to four years.

Cross-border transfer

32 | Is the transfer of PI outside the jurisdiction restricted?

As a general rule, personal data cannot be transferred abroad without the explicit consent of the data subject. However, personal data may be transferred abroad without the explicit consent of the data subject provided that one of the conditions specified in the PDPL is met, and that:

- adequate protection is provided in the foreign country where the data is to be transferred (the Board has the authority to determine the countries where an adequate level of protection is deemed to be provided although it has not done so yet);
- where adequate protection is not provided, the controllers in Turkey and in the relevant foreign country guarantee sufficient protection in writing, and the Board authorises such transfer (although data requiring the data subject's explicit consent in Turkey will continue to require such consent and will not be automatically covered by the approved undertaking); or
- approved binding corporate rules are followed (although data requiring data subject's explicit consent in Turkey will continue to require such consent and will not be automatically covered by such rules).

Binding corporate rules became available as an option only recently, pursuant to a Board decision. To use this method, group companies operating outside of Turkey in countries that are not listed as safe jurisdictions, must apply to the Board and submit an undertaking on their use of sufficient protection. If this undertaking is approved by the Board, then the relevant company is no longer obliged to obtain approval for each transfer.

Further transfer

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

Yes, if transfers outside of Turkey are subject to restriction or authorisation, these will also apply to transfers to service providers and onwards transfers.

Localisation

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

The PDPL does not require the PI or a copy of PI to be retained in Turkey. However, certain regulatory bodies, such as the Capital Markets Board of Turkey and Central Bank of Republic of Turkey, often require companies subject to their enforcement to have their own information systems and, therefore, keep PI in Turkey.

RIGHTS OF INDIVIDUALS

Access

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

Under the Personal Data Protection Law (PDPL), everyone has the right to:

- learn whether or not his or her personal data has been or are being processed;
- request information as to the processing if his or her data has been processed;
- learn the purpose of the processing and whether data is used in accordance with such purpose; and
- know the identity of the third parties in Turkey and abroad to whom personal data has been transferred.

Data subjects can use these by directly applying to the data controller in writing (in Turkish). Data controllers are obliged to respond to requests within 30 days. There are no limitations or fees associated with exercising these rights, except that the data controller may pass on any costs it incurs (eg, cost of a flash drive sent to the data subject).

Other rights

36 Do individuals have other substantive rights?

Each data subject has the right to apply to the controller and:

1 request the rectification of any incomplete or inaccurate data;
2 request the erasure or destruction of his or her personal data (subject to the conditions specified in the PDPL);
3 request notification of the actions listed in (1) and (2) to third parties to whom his or her personal data has been transferred;
4 object to any unfavourable result or consequence for the data subject, if such result or consequence is the result of exclusively automated means of the processing of his or her personal data; and
5 request compensation and other remedies for damages arising from any unlawful processing of his or her personal data.

Compensation

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

Yes. Despite of the fact that the PDPL does not foresee any compensation for data subjects who are affected by breaches of the PDPL, individuals can resort to general provisions of law and claim material and moral damages foreseen by the Turkish Code of Obligations. To claim material damages, the data subject must prove that a damage has occurred due to the fault of the data controller. On the other hand, to claim moral damages, the data subject must demonstrate that there was a violation of his or her individual rights and freedoms, and that violation has caused grave psychological harm.

Enforcement

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

Data subjects may demand that their rights in the PDPL, such as the right to be informed whether their PI is being processed, the purpose of the processing and whether the PI is being transferred to third parties to be enabled and enforced by the data controller. If the data controller does not comply with a data subject's request within 30 days, the data subject can request the relevant rights to be enforced by the Personal Data Protection Authority. Compensation claims are subject to the jurisdiction of civil courts and criminal complaints to the jurisdiction of criminal courts.

EXEMPTIONS, DEROGATIONS AND RESTRICTIONS

Further exemptions and restrictions

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

The Personal Data Protection Law does not include any derogations, exclusions or limitations other than those already described.

SPECIFIC DATA PROCESSING

Cookies and similar technology

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

Electronic communications, in general, are regulated by the Information and Communication Technologies Authority (ICTA), established in accordance with Law on Electronic Communications. Per the Law on Electronic Communications, the ICTA regulates and supervises the processing and protection of personal data acquired via electronic means.

Despite the fact that there is no explicit legislation on the use of cookies or equivalent technology in the Law on Electronic Communications or other legislation, because applicable legislation does not distinguish between the means of obtaining data, any personal data obtained through cookies or similar technology is under the protection of the law, and data controllers must comply with the rules applicable to the processing of personal data when using cookies or similar technology.

However, in January 2022, the Data Protection Board (the Board) published the Draft Guide Regarding Cookie Applications (the Draft Guide) and received feedback on it. The Draft Guide provides data controllers and data subjects with clarification on which types of cookies require explicit consent and how data subjects should be informed when they enter a website. Most importantly, the Draft Guide suggests that data controllers are not required to obtain explicit the consent of the data subjects for first-party analytical cookies.

Electronic communications marketing

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

The Law on the Regulation of Electronic Trade regulates the rules and conditions for marketing via electronic means.

For a data controller to use personal data for marketing by any means, the explicit consent of the data subject must be obtained. Data

subjects can always, without providing any reason, request the termination of electronic marketing communications from the data controller. Data controllers are obliged to terminate within three days all electronic communications with data subjects who require termination. Data controllers are also required to take all necessary means to preserve and protect the acquired personal data, and cannot distribute or disclose personal data without the explicit consent of the data subjects.

Further, the provision of services or sale of goods cannot be made subject to the consent to the collection of personal data that is not necessary for the provision of the relevant service or the making of the relevant sale.

The Board has also published guidance regarding electronic communications bearing personal information and deemed it necessary for data controllers to take reasonable measures to verify the contact information declared by the relevant data subjects (eg, sending a verification code or link to the person's registered phone number or email address).

Targeted advertising

42 | Are there any rules on targeted online advertising?

There are no specific rules or regulations regarding targeted online advertising. However, general principles shall always apply. As targeted online advertising does not fall under the scope of legitimate processing under the law, personal data can only be processed with the data subject's explicit consent. Likewise, this is the case for online behavioural advertising as most of the personal data is collected through cookies for targeted online advertising.

Although there are no regulations or other guidance published by the Board regarding the use of targeting and advertisement cookies, general rules require data controllers to obtain explicit consent from data subjects while the data subjects are using the data controller's website. Thus, targeted online advertising can only be done with the data subject's explicit consent.

Sensitive personal information

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

As a general rule, sensitive personal information cannot be processed without the consent of the data subject, except where permitted or required by applicable law. Further, personal data relating to health and sex lives may be processed without the explicit consent of the data subject only by persons or authorised public institutions and organisations that have confidentiality obligations, and only for the purposes of protecting public health, the administration of preventive medicine, medical diagnosis, treatment and care services, and the planning, management and financing of healthcare services.

Processing of data must be in compliance with the purposes stated in the data processing notification. If the processor decides to process the data for any reason other than those stated in the data processing notification, a new notification stating the new purpose must be provided to the data subject.

The Board has issued heightened measures for the safekeeping and processing of sensitive personal data. These measures include, among others, training programmes, encryption requirements, two-factor authentication for remote access and physical security measures such as access controls.

TURUNÇ

Esin Çamlıbel
ecamlibel@turunc.av.tr

Beste Yıldızili Ergül
byildizili@turunc.av.tr

Naz Esen
nesen@turunc.av.tr

Canberk Taze
ctaze@turunc.av.tr

Teşvikiye Caddesi 19/11
Teşvikiye 34365
Istanbul
Turkey
Tel: +90 212 259 45 36
Fax: +90 212 259 45 38

Cumhuriyet Bulvarı 140/1
Alsancak 35210
Izmir
Turkey
Tel: +90 232 463 49 07
Fax: +90 232 463 49 09

www.turunc.av.tr

Profiling

44 | Are there any rules regarding individual profiling?

There are no specific rules or regulations for individual profiling. However, general principles shall always apply for individual profiling. Thus, if the processing (profiling) is done for commercial purposes, in addition to the duty to inform the data subject regarding the purpose of processing, which data is being processed and whether the data controller is processing personal data through automated means, explicit consent of the data subject must be obtained.

Cloud services

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

Various pieces of legislation apply to the use of cloud computing services, including:

- the Universal Services Law;
- the Electronic Communications Law;
- the Regulation on Electronic Communications Infrastructure and Information Systems; and
- the Regulation on Rules on the Operations, Work and Supervision of Data Storage Institutions.

Furthermore, the ICTA regulates the use of cloud computing services.

However, the Turkish government's policy preference is the storage of personal data in Turkey.

UPDATE AND TRENDS

Key developments of the past year

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

In early 2021, the Data Protection Board (the Board) approved, for the first time, a number of applications for the transfer of data abroad through the use of written undertakings. Under this method, the controllers in Turkey and the relevant foreign country guarantee sufficient protection in writing, and the Board must approve such undertakings. This is a welcome development because the Board has yet to publish a list of safe jurisdictions (ie, foreign countries deemed to provide an adequate level of protection), another permitted (but not currently usable) method of transferring data abroad.

Binding corporate rules also became available as an option to transfer data abroad. To use this method, group companies operating outside of Turkey in countries that are not listed as safe jurisdictions must apply to the Board and submit an undertaking on their use of sufficient protection. If this undertaking is approved by the Board, then the relevant company is no longer obliged to obtain approval for each transfer.

In December 2021, the Board published the Communiqué on Procedures and Principles of Personnel Certification Mechanism and the Programme on Certification of Data Protection Personnel. Although the obligations of data protection personnel have not been set yet, we understand that the Board is laying the legal groundwork to implement a similar function to that of a data protection officer in the near future.

In January 2022, the Board published the Draft Guide Regarding Cookie Applications (the Draft Guide) and received feedback on it. The Draft Guide informs data controllers and data subjects on which type of cookies require explicit consent and how the data subject must be informed when they enter a website. Most importantly, the Draft Guide suggests that data controllers are not required to obtain explicit consent of the data subjects for first-party analytical cookies.

Other titles available in this series

Acquisition Finance
Advertising & Marketing
Agribusiness
Air Transport
Anti-Corruption Regulation
Anti-Money Laundering
Appeals
Arbitration
Art Law
Asset Recovery
Automotive
Aviation Finance & Leasing
Aviation Liability
Banking Regulation
Business & Human Rights
Cartel Regulation
Class Actions
Cloud Computing
Commercial Contracts
Competition Compliance
Complex Commercial Litigation
Construction
Copyright
Corporate Governance
Corporate Immigration
Corporate Reorganisations
Cybersecurity
Data Protection & Privacy
Debt Capital Markets
Defence & Security Procurement
Digital Business
Dispute Resolution
Distribution & Agency
Domains & Domain Names
Dominance
Drone Regulation
Electricity Regulation
Energy Disputes
Enforcement of Foreign Judgments
Environment & Climate Regulation
Equity Derivatives
Executive Compensation & Employee Benefits
Financial Services Compliance
Financial Services Litigation
Fintech
Foreign Investment Review
Franchise
Fund Management
Gaming
Gas Regulation
Government Investigations
Government Relations
Healthcare Enforcement & Litigation
Healthcare M&A
High-Yield Debt
Initial Public Offerings
Insurance & Reinsurance
Insurance Litigation
Intellectual Property & Antitrust
Investment Treaty Arbitration
Islamic Finance & Markets
Joint Ventures
Labour & Employment
Legal Privilege & Professional Secrecy
Licensing
Life Sciences
Litigation Funding
Loans & Secured Financing
Luxury & Fashion
M&A Litigation
Mediation
Merger Control
Mining
Oil Regulation
Partnerships
Patents
Pensions & Retirement Plans
Pharma & Medical Device Regulation
Pharmaceutical Antitrust
Ports & Terminals
Private Antitrust Litigation
Private Banking & Wealth Management
Private Client
Private Equity
Private M&A
Product Liability
Product Recall
Project Finance
Public M&A
Public Procurement
Public-Private Partnerships
Rail Transport
Real Estate
Real Estate M&A
Renewable Energy
Restructuring & Insolvency
Right of Publicity
Risk & Compliance Management
Securities Finance
Securities Litigation
Shareholder Activism & Engagement
Ship Finance
Shipbuilding
Shipping
Sovereign Immunity
Sports Law
State Aid
Structured Finance & Securitisation
Tax Controversy
Tax on Inbound Investment
Technology M&A
Telecoms & Media
Trade & Customs
Trademarks
Transfer Pricing
Vertical Agreements

Also available digitally

lexology.com/gtdt

ISBN XXX-X-XXXXX-XXX-X