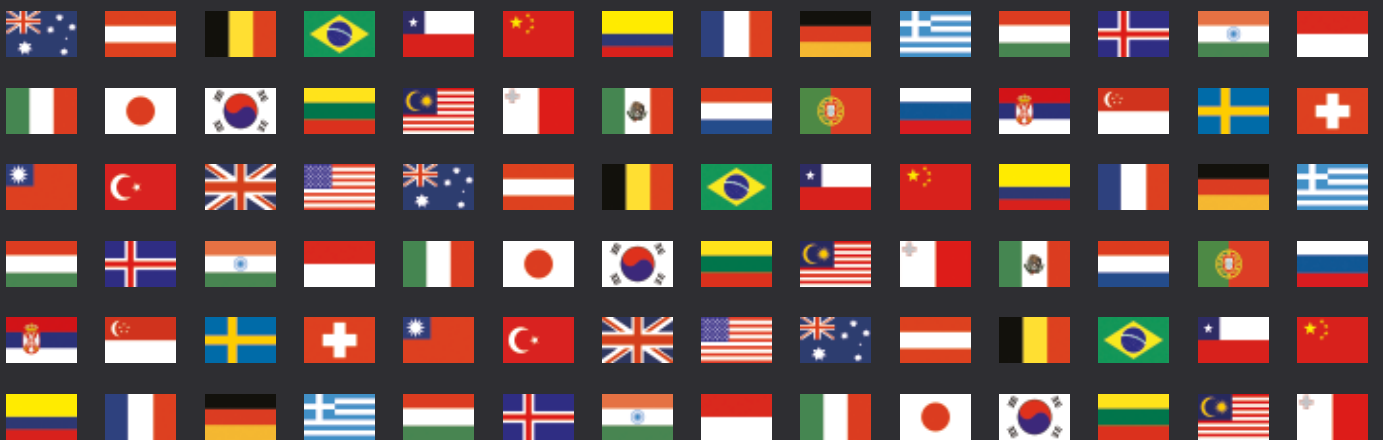


Data Protection & Privacy 2020

Contributing editors
Aaron P Simpson and Lisa J Sotto



Publisher

Tom Barnes
tom.barnes@lbresearch.com

Subscriptions

Claire Bagnall
claire.bagnall@lbresearch.com

Senior business development managers

Adam Sargent
adam.sargent@gettingthedealthrough.com

Dan White

dan.white@gettingthedealthrough.com

Published by

Law Business Research Ltd
87 Lancaster Road
London, W11 1QQ, UK
Tel: +44 20 3780 4147
Fax: +44 20 7229 6910

The information provided in this publication is general and may not apply in a specific situation. Legal advice should always be sought before taking any legal action based on the information provided. This information is not intended to create, nor does receipt of it constitute, a lawyer-client relationship. The publishers and authors accept no responsibility for any acts or omissions contained herein. The information provided was verified between June and July 2019. Be advised that this is a developing area.

© Law Business Research Ltd 2019
No photocopying without a CLA licence.
First published 2012
Eighth edition
ISBN 978-1-83862-146-9

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



Data Protection & Privacy

2020

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

Lexology Getting The Deal Through is delighted to publish the eighth edition of *Data Protection and 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 Hungary, Iceland, Indonesia and Malaysia.

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.



London
July 2019

Reproduced with permission from Law Business Research Ltd
This article was first published in August 2019
For further information please contact editorial@gettingthedealthrough.com

Contents

Introduction	5	Greece	90
Aaron P Simpson and Lisa J Sotto Hunton Andrews Kurth LLP		Vasiliki Christou Vasiliki Christou	
EU overview	9	Hungary	97
Aaron P Simpson, Claire François and James Henderson Hunton Andrews Kurth LLP		Endre Várady and Eszter Kata Tamás VJT & Partners Law Firm	
The Privacy Shield	12	Iceland	104
Aaron P Simpson and Maeve Olney Hunton Andrews Kurth LLP		Áslaug Björgvinsdóttir and Steinlaug Högnadóttir LOGOS legal services	
Australia	16	India	112
Alex Hutchens, Jeremy Perier and Meena Muthuraman McCullough Robertson		Stephen Mathias and Naqeeb Ahmed Kazia Kochhar & Co	
Austria	24	Indonesia	119
Rainer Knyrim Knyrim Trieb Attorneys at Law		Abadi Abi Tisnadisastra, Prihandana Suko Prasetyo Adi and Filza Adwani AKSET Law	
Belgium	32	Italy	126
David Dumont and Laura Léonard Hunton Andrews Kurth LLP		Rocco Panetta and Federico Sartore Panetta & Associati	
Brazil	43	Japan	136
Fabio Ferreira Kujawski, Paulo Marcos Rodrigues Brancher and Thiago Luís Sombra Mattos Filho		Akemi Suzuki and Tomohiro Sekiguchi Nagashima Ohno & Tsunematsu	
Chile	50	Korea	144
Carlos Araya, Claudio Magliona and Nicolás Yuraszeck Magliona Abogados		Young-Hee Jo, Seungmin Jasmine Jung and Kwangbok Kim LAB Partners	
China	56	Lithuania	153
Vincent Zhang and John Bolin Jincheng Tongda & Neal		Laimonas Marcinkevičius Juridicon Law Firm	
Colombia	66	Malaysia	159
María Claudia Martínez Beltrán and Daniela Huertas Vergara DLA Piper Martínez Beltrán Abogados		Jillian Chia and Natalie Lim Skrine	
France	73	Malta	166
Benjamin May and Farah Bencheliha Aramis		Ian Gauci and Michele Tufigno Gatt Tufigno Gauci Advocates	
Germany	83	Mexico	174
Peter Huppertz Hoffmann Liebs Partnerschaft von Rechtsanwälten mbB		Abraham Díaz Arceo and Gustavo A Alcocer OLIVARES	

Netherlands	182
Inge de Laat and Margie Breugem Rutgers Posch Visée Endedijk NV	
Portugal	188
Helena Tapp Barroso and Tiago Félix da Costa Morais Leitão, Galvão Teles, Soares da Silva & Associados	
Russia	196
Ksenia Andreeva, Anastasia Dergacheva, Anastasia Kiseleva, Vasilisa Strizh and Brian Zimble Morgan, Lewis & Bockius LLP	
Serbia	204
Bogdan Ivanišević and Milica Basta BDK Advokati	
Singapore	212
Lim Chong Kin Drew & Napier LLC	
Sweden	229
Henrik Nilsson Wesslau Söderqvist Advokatbyrå	
Switzerland	236
Lukas Morscher and Nadja Flühler Lenz & Staehelin	
Taiwan	245
Yulan Kuo, Jane Wang, Brian, Hsiang-Yang Hsieh and Ruby, Ming-Chuang Wang Formosa Transnational Attorneys at Law	
Turkey	252
Esin Çamlıbel, Beste Yıldızılı and Naz Esen TURUNÇ	
United Kingdom	259
Aaron P Simpson, James Henderson and Jonathan Wright Hunton Andrews Kurth LLP	
United States	268
Lisa J Sotto and Aaron P Simpson Hunton Andrews Kurth LLP	

Turkey

Esin Çamlıbel, Beste Yıldızlı and Naz Esen

TURUNÇ

LAW AND THE REGULATORY AUTHORITY

Legislative framework

- 1 Summarise the legislative framework for the protection of personally identifiable information (PII). Does your jurisdiction have a dedicated data protection law? Is the data protection law in your jurisdiction based on any international instruments on privacy or data protection?

The Turkish Constitution specifically protects, since 2010, PII. Protection of PII 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 General Data Protection Regulation (GDPR), the PDPL is generally based on and follows the GDPR.

Turkey is 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 become 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? Describe the investigative powers of the authority.

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, NGOs, professional associations and universities.

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

- ensuring that PII is 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;
- 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 sole authorised institution under the PDPL. The PDPL tasks the Authority with monitoring and evaluating the 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 into account when investigating cases. However, there is no mechanism to prevent the Board from taking decisions diverging from the European Data Protection Board.

Breaches of data protection

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

Breach of the PDPL can lead to both administrative fines and criminal penalties. The Board is responsible for ensuring that personal data are 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 registration of personal data, unlawful acquisition of personal data and non-destruction of personal data when required may be subject to criminal penalties under the Turkish Criminal Code.

SCOPE

Exempt sectors and institutions

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

The PDPL applies to all natural persons whose personal data is processed. It also applies to all natural and legal persons who (i) process such data using fully or partially automated means and (ii) provided that they are part of a data registry system ('filing system' under the

GDPR), through non-automated means. There is no distinction foreseen between private sector institutions and state institutions. As such, the PDPL is applicable to all types of entities and persons.

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

- processing by real 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 are 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/enforcement proceedings.

Communications, marketing and surveillance laws

6 | Does the data protection law cover interception of communications, electronic marketing or monitoring and surveillance of individuals? If not, list other relevant laws in this regard.

No, the PDPL does not directly cover interception of communications, electronic marketing or monitoring and surveillance of the individuals. Having said that, the Board has issued a decision regarding the regulation of contacting individuals via e-mail, 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 cover 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. In addition, the Criminal Code and Criminal Procedural Law regulate the sanctions in case of breach of applicable legislation.

Other laws

7 | Identify any further laws or regulations that provide specific data protection rules for related areas.

There are specific rules setting forth data protection rules for various areas. As an example, Turkish Labour Law holds that employers are obliged to use the personal data of employees in good faith and in accordance with applicable law, and not to disclose any personal data in which an employee has 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.

PII formats

8 | What forms of PII are covered by the law?

The PDPL does not limit the scope of protection by format. All information relating to an identified or identifiable real person maintained and stored in any format is covered by the PDPL and secondary legislation promulgated thereunder.

Extraterritoriality

9 | Is the reach of the law limited to PII owners and processors of PII established or operating in the jurisdiction?

The PDPL does not make any differentiation between data subjects who are nationals or not. The PDPL is applicable to all natural persons whose personal data are processed.

Having said that, 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:

- either adequate protection is provided in the foreign country where the data are to be transferred (the Board determines and announces the countries where adequate level of protection is deemed to be provided); or
- where adequate protection is not provided, the controllers in Turkey and in the related foreign country guaranteeing sufficient protection in writing, and the Board has authorised such transfer.

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

Covered uses of PII

10 | Is all processing or use of PII covered? Is a distinction made between those who control or own PII and those who provide PII 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 with respect to their duties and liabilities.

LEGITIMATE PROCESSING OF PII

Legitimate processing – grounds

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

In the eye of the PDPL, holding personal data is deemed as processing such data. As a general rule under the PDPL, 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 party;
- the processing is necessary in order to comply with a legal obligation to which the data controller is subject;
- the data have been made public by the data subject;
- the processing is necessary in order 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.

There are also specific rules for processing sensitive personal data. See question 12.

Legitimate processing – types of PII

12 | Does the law impose more stringent rules for specific types of PII?

Under the PDPL, personal data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, clothing choices/habits, trade-union membership, health or sex life, criminal conviction 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. Furthermore, personal data relating to health and sex life 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, administration of preventive medicine, medical diagnosis, treatment and care services, and the planning, management and financing of healthcare services.

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

DATA HANDLING RESPONSIBILITIES OF OWNERS OF PII

Notification

13 | Does the law require owners of PII to notify individuals whose PII they hold? What must the notice contain and when must it be provided?

When collecting 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 of its representative, if any;
- the purpose of 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 PDPL (see questions 37 and 38).

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.

Exemption from notification

14 | When is notice not required?

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 him 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 having the status of public institution; or
- processing of the personal data is required for protection of the state's economic and financial interests with regard to budgetary, tax-related and financial issues.

Control of use

15 | Must owners of PII offer individuals any degree of choice or control over the use of their information? In which circumstances?

Data controllers are obliged to request for consent of the data subject at the time of acquiring data. Data subjects can freely decide whether to grant consent or not. Data subjects are entitled to withdraw their consent at any time. Having said that, in the cases detailed in question 11, data controllers can process the data based on legitimate reasons under the PDPL.

Also, data subjects can demand their personal data to be erased, destructed or anonymised upon the disappearance of reasons which require the processing. Data subjects have also been granted with substantial rights to ensure that their personal data continue to be processed in accordance with the original purpose of the processing (for which consent was granted).

Data accuracy

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

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.

Amount and duration of data holding

17 | Does the law restrict the amount of PII that may be held or the length of time it may be held?

There is no restriction on the amount of personal data that may be held.

Having said that, personal data can only be preserved for the time periods foreseen in the applicable regulations or time periods necessary for the purpose of processing.

Data controllers, who are obliged to register with the data controllers registry known as VERBİS (see question 26), 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.

Data controllers who are required to prepare data preservation and destruction policies must erase, destruct 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).

Finality principle

18 | Are the purposes for which PII can be used by owners restricted? Has the 'finality principle' been adopted?

Yes, the purposes for using the personal data must be determined during obtaining the consent of the data subject. Data controllers cannot exceed or circumvent these purposes.

Use for new purposes

19 | If the finality principle has been adopted, how far does the law allow for PII to be used for new purposes? Are there exceptions or exclusions from the finality principle?

Data controllers are limited with the purpose(s) stated in the consent or notification, as applicable. Unless it is explicitly permitted by the PDPL, data controllers cannot use the data collected other than for the purposes that are clearly expressed while collecting the data. Hence, data controllers are obliged to obtain additional consent of the data subject and to provide a new notification if the collected data will be used for a new purpose requiring consent. 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.

SECURITY

Security obligations

20 | What security obligations are imposed on PII owners and service providers that process PII 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 conduct necessary inspections or have them conducted in their own institutions.

Notification of data breach

21 | 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 PDPL, 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 promptly 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

Data protection officer

22 | Is the appointment of a data protection officer mandatory? What are the data protection officer's legal responsibilities?

The PDPL does not foresee an obligation for appointing a data protection officer.

Record keeping

23 | Are owners or processors of PII required to maintain any internal records or establish internal processes or documentation?

The PDPL does not contain a provision regarding a general obligation to maintain internal records or establish internal processes or documentation. Having said that, data controllers and processors who process personal data by automated means are obliged to 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.

Data controllers, who are obliged to register with the data controllers registry VERBİS, 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.

New processing regulations

24 | Are there any obligations in relation to new processing operations?

No, there are no specific obligations as such in relation to new processing operations.

REGISTRATION AND NOTIFICATION

Registration

25 | Are PII owners or processors of PII required to register with the supervisory authority? Are there any exemptions?

As a general rule, data controllers are required to register with VERBİS. The Board has exempted, through various decisions, the following data controllers from the registration requirement:

- data processors that are part of a data registry system ('filing system' under the GDPR) and process data only in non-automated ways;
- associations, foundations and unions (to the extent they process data of their employees); and members and donors (limited to their areas of activity);
- political parties;
- lawyers;
- mediators;
- notaries public;
- certified public accountants;
- customs brokers; and
- employers that 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.

Formalities

26 | What are the formalities for registration?

Data controllers must register with VERBİS at verbis.kvkk.gov.tr. If the data controller is in a foreign country, a data controller representative resident in Turkey must be appointed before registering.

Data controllers must appoint a contact person and complete the form provided by the Authority.

There is no fee for registration or renewals.

Penalties

27 | What are the penalties for a PII owner or processor of PII for failure to make or maintain an entry on the register?

Persons who fail to comply with the obligation to register with and maintain proper entries on VERBİS may be sanctioned to a monetary fine between 20,000 Turkish lira and 1,000,000 Turkish lira by the Board.

Refusal of registration

28 | On what grounds may the supervisory authority refuse to allow an entry on the register?

All data controllers must register except for the exempted persons listed in question 25.

Public access

29 | Is the register publicly available? How can it be accessed?

Yes, the VERBİS system is publicly available and individuals can make online enquiries through the system and can view the information registered.

Effect of registration

30 | Does an entry on the register have any specific legal effect?

The registry records, thus the purpose of processing, are open to public. The registry aims to provide transparency for the records.

Other transparency duties

31 | Are there any other public transparency duties?

There are no other transparency duties; data processors are only obliged to notify the data subjects and register with VERBİS when the applicable conditions are met.

TRANSFER AND DISCLOSURE OF PII

Transfer of PII

32 | How does the law regulate the transfer of PII to entities that provide outsourced processing services?

The PDPL foresees special conditions for transferring personal data. Personal data normally cannot be transferred without explicit consent of the data subject, unless the conditions described in questions 11 and 12 are applicable. 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. In the event that the data subject denies providing consent, 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). With regard to personal data that is required to be preserved pursuant to various legislations, 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 the 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 disclosure

33 | Describe any specific restrictions on the disclosure of PII to other recipients.

As a general rule, there are no specific restrictions foreseen on the disclosure of personal data apart from the general requirements detailed above as to notifying and informing the data subject, obtaining the data subject's consent as to what data will be disclosed, and determining the purposes for which the data shall be disclosed.

Having said that, for disclosing sensitive personal data, 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.

Cross-border transfer

34 | Is the transfer of PII 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:

- either adequate protection is provided in the foreign country where the data are to be transferred (the Board determines and announces the countries where an adequate level of protection is deemed to be provided); or
- where adequate protection is not provided, the controllers in Turkey and in the related foreign country guaranteeing sufficient protection in writing, and the Board has authorised such transfer.

Notification of cross-border transfer

35 | Does cross-border transfer of PII require notification to or authorisation from a supervisory authority?

Yes. As described in question 34, transfer of personal data to a foreign jurisdiction may be made if that jurisdiction is on the Board's safe list or a specific authorisation granted by the Board.

In deciding whether to approve a foreign jurisdiction, the Board will take into account the following:

- international treaties to which Turkey is a party;
- reciprocity by the foreign jurisdiction;
- for each proposed transfer, the nature of the personal data proposed to be transferred, the purpose of the processing and retention policies;
- relevant legislation and practice of the foreign jurisdiction; and
- the measures undertaken to be implemented by the relevant data controller in that jurisdiction.

The Board may also obtain the opinion of relevant public institutions; subject to any applicable international treaties, it must do so if Turkey's or the data subject's interests are likely to be materially prejudiced.

Further transfer

36 | 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.

RIGHTS OF INDIVIDUALS

Access

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

Under the PDPL everyone has the right to:

- learn whether or not his or her personal data has been or is 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 thirty 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

38 | Do individuals have other substantive rights?

In addition to the rights described in question 37, each data subject has the right to apply to the controller and:

- request the rectification of any incomplete or inaccurate data;
- request the erasure or destruction of his or her personal data (subject to the conditions specified in the PDPL);
- request notification of the actions listed in the first two bullet points above to third parties to whom his or her personal data has been transferred;
- 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
- request compensation and other remedies for damages arising from any unlawful processing of his or her personal data.

Compensation

39 | 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. In order 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 a grave psychological harm.

Enforcement

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

Data controllers may demand the rights described in question 38 to be enforced by the 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

41 | Does the law include any derogations, exclusions or limitations other than those already described? Describe the relevant provisions.

The PDPL does not include any derogations, exclusions or limitations other than those already described.

SUPERVISION

Judicial review

42 | Can PII owners appeal against orders of the supervisory authority to the courts?

Data subjects can appeal to administrative courts against the orders of the Authority.

SPECIFIC DATA PROCESSING

Internet use

43 | Describe 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.

Electronic communications marketing

44 | Describe any rules on marketing by email, fax or telephone.

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

In order 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 the electronic marketing communications from the data controller. Data controllers are obliged to terminate electronic communications with data subjects who require termination within three days. 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.

Furthermore, 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.

Cloud services

45 | Describe any rules or regulator guidance on the use of cloud computing services.

Various pieces of legislation apply to the use of cloud computing services: 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, among others. Furthermore, the ICTA regulates the use of cloud computing services.

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?

The PDPL is a relatively new piece of legislation, which entered into force in 2016. The Board was formed in early 2017 and since its formation has issued only 13 decisions. Accordingly, much of the interpretation (and application) of the PDPL is either very new or yet to be formed. Having said that, there is significant awareness about the PDPL in the country and the Board is in close cooperation with practitioners, academia and other stakeholders to implement the best practices, make improvements to the legislation, and further raise awareness on data protection and privacy issues.

TURUNÇ

Esin Çamlıbel

ecamlibel@turunc.av.tr

Beste Yıldızlı

byildizili@turunc.av.tr

Naz Esen

nesen@turunc.av.tr

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

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

www.turunc.av.tr

Other titles available in this series

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

Also available digitally

[lexology.com/gtdt](https://www.lexology.com/gtdt)