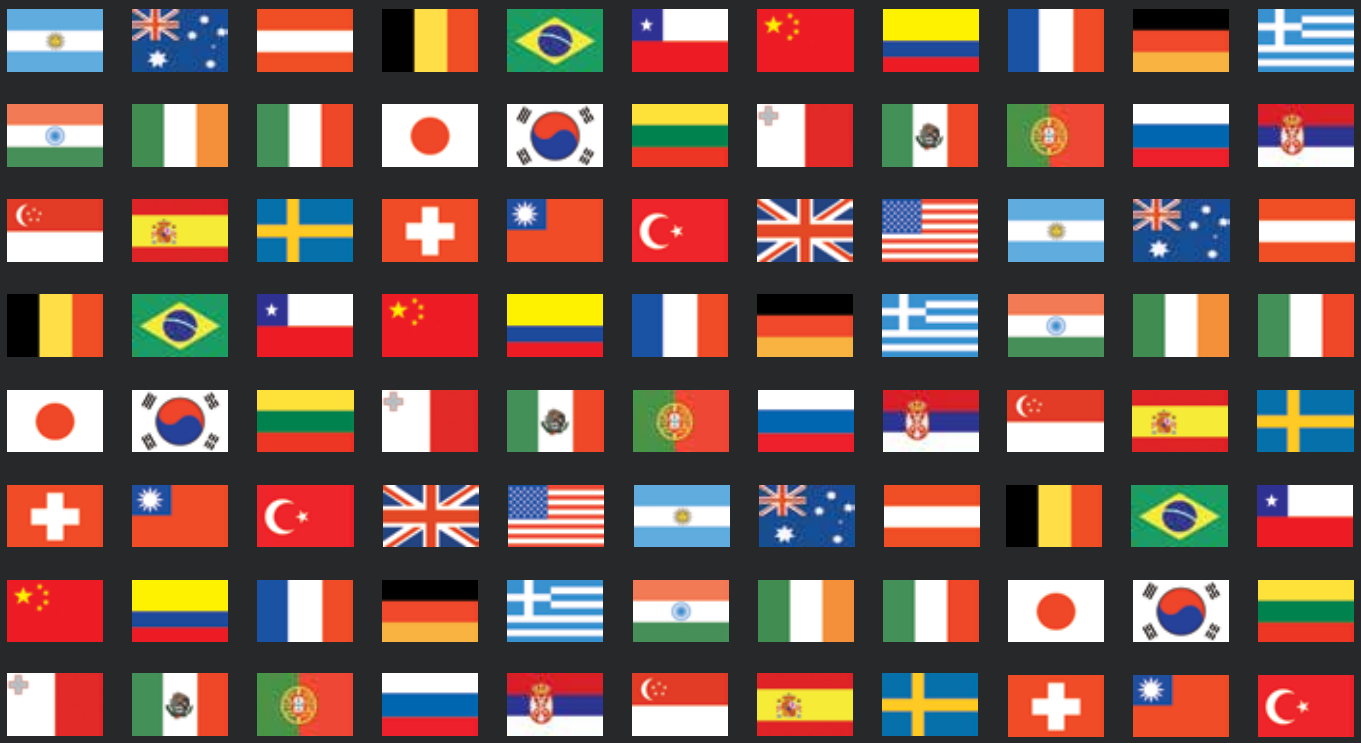
Data Protection & Privacy

Contributing editors
Aaron P Simpson and Lisa J Sotto



2019

GETTING THE DEAL THROUGH

GETTING THE DEAL THROUGH

Data Protection & Privacy 2019

Contributing editors

Aaron P Simpson and Lisa J Sotto

Hunton Andrews Kurth LLP

Reproduced with permission from Law Business Research Ltd
This article was first published in August 2018
For further information please contact editorial@gettingthedealthrough.com

Publisher
Tom Barnes
tom.barnes@lbresearch.com

Subscriptions
James Spearing
subscriptions@gettingthedealthrough.com

Senior business development managers
Adam Sargent
adam.sargent@gettingthedealthrough.com

Dan White
dan.white@gettingthedealthrough.com

Law Business Research

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

First published 2012
Seventh edition
ISBN 978-1-78915-010-0

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

CONTENTS

Preface

Data Protection & Privacy 2019

Seventh edition

Getting the Deal Through is delighted to publish the seventh edition of *Data Protection & Privacy*, which is available in print, as an e-book and online at www.gettingthedealthrough.com.

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 **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 Argentina, Colombia, Greece, Korea, Malta and Taiwan.

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.gettingthedealthrough.com.

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.

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.

GETTING THE DEAL THROUGH

London
July 2018

Turkey

Ozan Karaduman and Selin Başaran Savuran

Gün + Partners

Law and the regulatory authority

1 Legislative framework

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 protection of personally identifiable information in Turkey is regulated mainly by the Law on the Protection of Personal Data (DPL), which came into effect on 7 April 2016. The DPL is heavily modelled on Directive 95/46/EC, with many of the terms and central provisions very closely mirroring their equivalents in the Directive. Other than the DPL, there are a few other central legislative measures that constitute the framework of the protection of PII in Turkey.

The first of these is the Turkish Constitution, article 20 of which defines and enshrines the right to the protection of personal data. The Turkish Criminal Code also contains provisions relating to the unlawful recording and obtaining of personal data. In fact, before the introduction of the new DPL, the data protection regime in Turkey was based primarily on the relevant articles of the Constitution and the Turkish Criminal Code.

While the DPL provides the central framework for the general data protection regime in Turkey, there are also certain industry-specific regulatory measures that introduce further requirements. The most prominent examples of such industry-specific measures are those relating to the electronic communication and banking sectors.

Furthermore, the Turkish Data Protection Authority (Turkish DPA) issued ancillary legislation, such as the Regulation on Data Controller Registry (Regulation on Registry), the Regulation on Deletion, Destruction and Anonymisation of Personal Data, the Communiqué on Procedures and Principles for Application to Data Controllers and other guidelines and principle decisions.

In addition to these national legislative and regulatory measures, Turkey is also a signatory to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. While a signatory since 28 January 1981, Turkey only ratified the Convention on 2 May 2016.

2 Data protection authority

Which authority is responsible for overseeing the data protection law? Describe the investigative powers of the authority.

The implementation of the DPL has been granted to the Turkish DPA. The DPL contains provisions regarding both the establishment of the Turkish DPA and the scope of its powers and responsibilities. Accordingly, as per the DPL, the Turkish DPA has been granted investigative powers in order to ascertain whether data controllers and data processors are in compliance with the provisions of the DPL. To this end, the Turkish DPA may conduct investigations (either upon complaint or ex officio) in order to evaluate whether data processing is being conducted in compliance with the DPL and, if necessary, implement any temporary preventative measures. Furthermore, the Turkish DPA has been tasked with reviewing and ruling on any referred complaints alleging the violation of the fundamental data protection rights.

In light of the DPL, the Turkish DPA was established and commenced its operations in January 2017. Since that date, the Turkish DPA has issued several ancillary regulations, guidelines and principle decisions supplementing the implementation of the DPL. Furthermore, the Turkish DPA has started to investigate complaints regarding the violation of data protection legislation and issued decisions concerning these violations where it has imposed administrative fines.

3 Legal obligations of data protection authority

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

There is no data protection authority other than the DPA in Turkey. There is not an explicit obligation of the Turkish DPA to cooperate with data protection authorities in other countries. However, pursuant to the DPL, the Turkish DPA is responsible for cooperating with public institutions and organisations, non-governmental or professional organisations or universities when needed, as well as being responsible for cooperating with international organisations and participating in meetings on matters that fall under its scope of duty.

4 Breaches of data protection

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

As per the DPL, the breach of the provisions can lead to both administrative fines and criminal penalties. With regard to potential criminal penalties, the DPL itself makes reference to the relevant measures of the Turkish Criminal Code that detail unlawfully recording or accessing personal data. As per article 135 of the Turkish Criminal Code, unlawful recording of personal data can be sanctioned with a one- to three-year prison sentence; with the sanction being increased by half should the unlawfully recorded personal data be personal data of a sensitive nature. Article 136 states that unlawfully obtaining or transferring personal data is punishable by a two- to four-year prison sentence. Finally, article 138 of the Turkish Criminal Code states that those persons who have kept and not erased personal data beyond the period stipulated by DPL can be sanctioned with a prison sentence of one to two years.

In addition to criminal proceedings, the DPL also establishes administrative fines that may be applied in the situation of a breach. There are four main breaches that have been defined in the context of a potential administrative fine:

- a data controller not satisfying their obligation to inform the data subject;
- the data controller not satisfying the data security requirements;
- the data controller not implementing the decisions of the Turkish DPA; and
- the data controller not satisfying their obligation to register on the Data Controller Registry (the Registry).

These breaches can be sanctioned with administrative fines ranging from 5,000 to 1 million liras.

Depending on the nature of the breach – as in whether the breach constitutes a criminal or administrative offence – the data controller will either be referred to the prosecutor or the Turkish DPA or both.

Scope

5 Exempt sectors and institutions

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

The DPL does contain a provision that defines areas and activities of exception where the provisions of the DPL will not be applied. These areas of exception are as follows:

- use of personal data by real persons within the scope of activities relating to either themselves or their family members living in the same house; on the condition that the data is not provided to third parties and data security requirements are followed;
- processing of personal data for official statistics or – on the condition that the data is made anonymous – used for purposes such as research, planning or statistics;
- on the condition that such use is not contrary to national defence and security, public safety and order, economic security, the right to privacy and personal rights, and on the condition that it does not constitute a crime, processing for the purposes of art, history, literature or scientific pursuits or processing within the scope of the freedom of speech;
- processing within the scope of the preventive, protective and intelligence activities of the public bodies and institutions that have been authorised by law to safeguard national defence, security, public safety and order or economic security; and
- processing by judicial authorities or penal institutions in relation to investigations, prosecutions, trials or enforcement proceedings.

6 Communications, marketing and surveillance laws

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.

The DPL does not cover the issues of interception of communications, electronic marketing or the monitoring and surveillance of individuals.

The areas of interception of communications and the monitoring and surveillance of individuals are primarily regulated by the Turkish Criminal Procedure Code. The specifics of these areas are further regulated with more specific regulatory measures such as the Regulation on Inspection of Communication made via Telecommunication, Undercover Investigations and Surveillance with Technical Tools due to the Law of Criminal Procedure.

The legislative measures that regulate the electronic communication sector, primarily the Electronic Communication Law (ECL) and ancillary regulations such as the Authorization Regulation also specify that licensed operators operating within the electronic communication sector are under the obligation to establish and maintain the infrastructure that will enable such lawful interception and surveillance activities.

Electronic marketing is covered by the Law on the Regulation of Electronic Commerce (E-Commerce Law) and its ancillary regulations.

7 Other laws

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

The primary sector-specific laws and regulations that introduce further data protection rules can be found in the electronic communication and banking sectors.

With regard to the electronic communication sector, the ECL introduces specific rules regarding how licensed operators operating in this sector may use traffic and location data that they can obtain from their customer. Furthermore, the Regulation on the Processing of Personal Data in the Electronic Communication Sector and the Protection of Privacy also contains further sector-specific rules regarding data processing in the electronic communication sector.

Certain legislative measures such as the Law on Payment and Security Agreement Systems, Payment Systems and Electronic Currency Organisations, requires financial institutions to keep their primary and secondary systems within Turkey and thus prevent transfer of such data abroad. Furthermore, the Banking Law introduces specific confidentiality obligations for persons who, owing to their position and task, are in possession of secret information relating to banks or their client. The Law on Bank Cards and Credit Cards imposes a similar obligation on this industry.

8 PII formats

What forms of PII are covered by the law?

The DPL defines personal data widely as 'all information relating to an identified or identifiable real person'. Furthermore, the DPL does not make any limitations or distinctions with regard to the format that such PII is maintained or stored. Therefore, in light of the central definition of the DPL, it can be said that the forms of PII covered are extensive both in the nature of the information and in terms of the format.

9 Extraterritoriality

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

While the DPL does not have a specific geographic scope that is stated within the text of the Law, it should be noted that as a Turkish law with sanctions applied by either Turkish public bodies or Turkish courts, the application of the Law itself is practically limited to real and legal persons who are processing the PII of the persons residing in Turkey. Despite issues regarding the enforceability of sanctions against persons who are not in Turkey or do not have assets in Turkey, the content and structure of the DPL does make it clear that it is intended to establish and safeguard the data protection rights of all persons within Turkey whose personal data is being processed, regardless of the identity of the data processor. As a result, the DPL will apply to data controllers and data processors both inside and outside of Turkey that are processing the personal data of the Turkish residents.

This approach is also confirmed by the Regulation on Registry, which refers to data controllers that are based outside of Turkey. According to this Regulation, data controllers that are based outside of Turkey must be registered with the Registry established by the DPA and appoint a representative (either a legal entity based in Turkey or a Turkish citizen).

10 Covered uses of PII

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 DPL also provides a very wide scope definition for the processing of PII. As per the relevant provision, processing of personal data is defined as 'all operations performed on personal data, whether completely or partially through automated means or – on the condition that it is a part of a data recording system – through non-automated means, such as collection, recording, structuring, storage, re-structuring, disclosure, transfer, retrieval, making available, categorisation or restriction'.

The DPL also distinguishes between data controllers, who determine the purposes and methods of data processing, and data processors that process data based on the authorisation provided by the data controllers.

Data controllers and data processors have different duties under the DPL. The most important of the obligations of data controllers are the requirements to notify and inform data subjects of the processing of their data and to obtain their consents where necessary under the DPL, to implement all kinds of technical and administrative measures in order to maintain a security level that would prevent unlawful processing of and unauthorised access to personal data while also safeguarding personal data, and to register with the Registry. The data controller and the data processor that processes data on behalf of the data controller are jointly responsible for the adoption of these technical and administrative measures.

Legitimate processing of PII

11 Legitimate processing – grounds

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?

Pursuant to the DPL, in principle the personal data can be processed with the explicit and informed consent of the data subject. However, the DPL itself also provides additional conditions where this requirement of obtaining explicit and informed consent will not be required, which are set forth below:

- processing is clearly mandated by laws;
- for a person who is unable to express their explicit consent owing to a situation of impossibility, processing is required for the safeguarding of their or a third person's life or physical wellbeing;
- processing is necessary for and directly related to the formation or execution of an agreement to which the data subject is a party;
- processing is mandatory for the data controller to satisfy his or her legal obligation;
- the data to be processed has been made public by the data subject;
- processing is mandatory for the establishment, use or protection of a right; or
- on the condition that it does not harm the data subject's fundamental rights and freedoms, the processing is mandatory for the legitimate interests of the data controller.

Although the DPL specifies the explicit consent of the data subject as the main principle for processing personal data, the DPA states that if it is possible to process the personal data based on any of the additional conditions set forth above, the data controller should process the data based on the additional condition and should not obtain explicit consent.

12 Legitimate processing – types of PII

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

Yes, the DPL provides more stringent rules for the processing of personal data of a sensitive nature. Personal data of a sensitive nature is defined exhaustively as data relating to 'race, ethnicity, political views, philosophical belief, religious denomination or other beliefs, clothing and attire, membership in associations, charities or trade unions, health, sex life, convictions, security measures, biometric and genetic data'.

While the general principle for the processing of such data remains the explicit consent of the data subject, the situations of exception are a lot narrower compared to normal PII. With regard to personal data of a sensitive nature other than health and sex life data, processing without consent is allowed when such processing is clearly mandated by law. For health and sex life data, the only exception is data processed by persons or authorised institutes bound by the duty of confidentiality for the purpose of the protection of public health, the provision of medical, diagnostic and treatment services and the planning, management and financing of healthcare services.

Data handling responsibilities of owners of PII

13 Notification

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?

The DPL does include a duty of notification that requires data controllers to notify the data subjects as to the use of their data. This notification must be made at the time that the personal data is obtained and must include the following information:

- the identity of the data controller and, if applicable, its representative;
- the purposes of processing;
- to whom the processed data may be transferred and for which purposes they may be transferred;
- the method and legal grounds for the data collection; and
- information about the other rights of the data subject.

14 Exemption from notification

When is notice not required?

The conditions for exemption from the obligation of notification are when:

- the processing is required for the prevention or investigation of a crime;
- the data being processed has been made public by the data subject;
- the processing is required for disciplinary investigations or procedures by authorised public bodies and institutions, or by professional organisations with public institution status and for the inspections carried out by such parties in accordance with their statutory purview; or
- the processing is required to protect the state's economic and financial interests with regard to the issues of budget, taxation and financial issue.

15 Control of use

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

As the DPL upholds the central principle that data processing should be based on consent and that processing should be in accordance with the law and the principle of honesty, it can be said that by the very nature of the centrality of explicit consent, the data subjects are afforded a degree of control over their information. The exceptions to the requirement of consent do provide derogations from this notion of control; however, as will be further discussed in questions 37–40, data subjects have been granted substantial rights to ensure that their data is being processed in accordance with the original purpose of the processing of their PII.

16 Data accuracy

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

One of the main principles of the DPL is that the processed personal data be accurate and – when necessary – up to date. While there has not been any further guidance as to the standards of accuracy and quality of the personal data, it is expected that these principles will be further clarified by the Turkish DPA through the drafting and publication of ancillary regulatory measures.

The DPL also grants data subjects the right to demand that any personal data relating to them that has been processed in an incorrect or incomplete manner be rectified.

17 Amount and duration of data holding

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

The DPL itself does not state set and definite time limits for how long personal data may be held. However, article 7 of the DPL introduces a general principle stating that, once the grounds of processing of personal data no longer exist, the data controller is under the obligation to either delete, destroy or anonymise the personal data. While these processes may be applied upon the request of the data subject, the DPL also states that the data controller itself should also apply these processes through its own determination.

With regard to the amount of PII, as long as all processed PII is being held and processed lawfully, the DPL does not enforce any restrictions as to the amount or volume of data.

18 Finality principle

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

Article 4 of the DPL provides the fundamental principles of data processing in Turkey; one of which is that processing must be in connection with, limited to and proportional to the stated purposes of processing. Therefore, as per the DPL, processing of personal data must be limited to either the purpose for which explicit consent was provided or to the scope of the exception to obtaining explicit consent upon which the processing can be based.

19 Use for new purposes

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?

As stated above, due to the adoption of the finality principle requiring processing to be connected, limited and proportional to the stated purpose of processing, the DPL does not allow for using collected personal data for new purposes that are not covered by the obtained explicit consent or the specific grounds of exception that have been used for processing. Furthermore, the Communiqué on Procedures and Principles regarding the Obligation to Notify states that the data controller must comply with the notification obligation before starting the data processing activity if the purpose of the data processing is changed.

Security

20 Security obligations

What security obligations are imposed on PII owners and service providers that process PII on their behalf?

The DPL imposes general security obligations on data controllers to ensure that personal data is not processed unlawfully, accessed without authorisation and is safeguarded. The relevant provision stipulates a general obligation of ensuring that all technical and administrative precautions are taken by the data controller in order to ensure that such protection is provided. Furthermore, as per the provision of the DPL that establishes the conditions of processing personal data of a sensitive nature, such processing is conditioned upon implementing the sufficient measures that have been determined by the Turkish DPA.

Since the DPL itself does not provide detailed explanations as to the content of these precautions, the DPA issued the Guidelines on Personal Data Security (Technical and Administrative Measures) in January 2018 and the Decision Regarding the Adequate Measures to be Taken by Data Controllers in Processing of Personal Data of Sensitive Nature on 7 March 2018 (Decision on Adequate Measures).

Finally, pursuant to the DPL, data controllers are also under the obligation to conduct the required audits in order to ensure that they are adhering to the security provisions of the DPL. In the situation that a data controller utilises a third-party data processor to process PII on their behalf, the data controller will remain jointly liable with regard to ensuring that safety precautions are taken to ensure the protection of the PII.

21 Notification of data breach

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?

The DPL requires for any access to data by third parties through unlawful means to be notified by the data controller to both the data subject and the Turkish DPA. The DPL also stipulates that, should the Turkish DPA deem it necessary, it may publish such notified breaches either on its own website or through other appropriate means.

Currently there are no further clarifications regarding this duty of notification, particularly with regard to any set time limit within which to notify such breaches to the data subjects and the DPA. The relevant provision only states that such notifications must be made 'within the shortest possible time'. Thus, it is expected that the Turkish DPA will issue ancillary regulations to clarify this issue.

Internal controls

22 Data protection officer

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

The DPL and other sector-specific ancillary regulations do not require the appointment of a data protection officer. However, the Regulation on Registry requires data controllers that are based in Turkey to appoint a contact person, who will be responsible for communication of the requests of data subjects to the data controller and will be the contact person for the Turkish DPA. Similarly, data controllers that are based outside of Turkey are required to appoint a representative, who will be the contact person for the Turkish DPA and the Turkish Data Protection Board, for responding to the queries addressed to the data controller and conveying the responses of the data controller to data subjects and taking necessary actions concerning registration procedures to the Registry.

23 Record keeping

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

The DPL does not contain a provision regarding a general obligation to maintain internal records or establish internal processes or documentation. However, the Regulation on Deletion, Destruction and Anonymisation of Personal Data requires all data controllers to maintain data inventories, and data controllers that are responsible for enrolling in the Registry to maintain a personal data retention and destruction policy. Furthermore, the Decision on Adequate Measures requires data controllers that process personal data of a sensitive nature to adopt and maintain a systematic and sustainable policy and procedure for the safety of personal data of a sensitive nature.

On the other hand, for the time being, none of this legislation sets forth any obligation for data processors to maintain any internal records or establish internal processes or documentation. However, for evidentiary purposes, processors and controllers should maintain records to prove that they have acted in compliance with the DPL in case of an audit or conflict.

With regard to the electronic communication sector, the ECL and ancillary regulatory measures require licensed operators within the electronic communication sector to maintain certain records relating to completed and attempted electronic communications. Furthermore, licensed operators are also under an obligation to maintain records that document access made to personal data and other related systems for a period of two years.

24 New processing regulations

Are there any obligations in relation to new processing operations?

There is no explicit obligation in relation to new processing operations such as requirements to apply a privacy-by-design approach or carry out a privacy impact assessment. However, the DPL regulates the general principles of the processing of personal data, and within this scope all processing activities must comply with the laws and the rule of bona fide; be accurate and up to date; be for specific, legitimate and explicit purposes; be in connection with, limited to and proportional to the purposes of processing; and personal data must be kept only for the period required for the processing purposes or as regulated under the relevant legislation.

Registration and notification

25 Registration

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

As per the DPL, both real and legal persons processing PII must be registered on the Registry. Depending on the provision of the DPL that enables the Turkish DPA to introduce exemptions for registration to the Registry based on such considerations as the quality, amount and grounds of the processing, the Turkish DPA issued a principle decision dated 2 April 2018 that specifies the exemptions of the registration. According to the relevant decision of the Turkish DPA, data controllers that process personal data only in non-automatic ways, within the part of a data recording system; associations, foundations and unions that process personal data of their employees, members and donors only within the scope of the relevant legislation and limited with the purposes of their activities; notaries; political parties, lawyers, public accountants and sworn-in public accountants are exempted from registration.

Furthermore, article 28(2) of the DPL also introduces a more general exemption from the obligation to register for instances of

processing where, on the condition that it remains in accordance and proportional to the purpose and principles of the DPL:

- the processing is required for the prevention or investigation of a crime;
- the data being processed has been made public by the data subject;
- the processing is required for disciplinary investigations or procedures by authorised public bodies and institutions or by professional organisations with public institution status and for the inspections carried out by such parties in accordance with their statutory purview; or
- the processing is required to protect the state's economic and financial interests with regard to the issues of budget, taxation and financial issue.

These general exemptions are also repeated under article 15 of the Regulation on Registry.

26 Formalities

What are the formalities for registration?

The DPL establishes the general principles relating to registration with the Registry. As per said principles, the data controller's application for registration must include the following information:

- the identity and address of the data controller and, if applicable, his or her representative;
- the purpose of processing of the personal data;
- the data subject groups and explanations relating to the data categories belonging to these persons;
- recipients or recipient groups to whom the data may be transferred;
- the precautions taken with regard to the security of personal data; and
- the maximum time period required for the process of processing.

In order to detail the registration process, the Turkish DPA issued the Regulation on Registry on 30 December 2017. As per this Regulation, for registration to the Data Controllers Registry Information System (VERBİS), data controllers must prepare data inventories as well as data retention and destruction policies. Furthermore, data controllers that are based in Turkey must appoint a contact person and data controllers that are based outside of Turkey must appoint a data controller's representative.

27 Penalties

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

In the situation that a data controller fails to register for the Registry or fails to maintain their registration with up-to-date information, said controller can be sanctioned with an administrative fine ranging from 20,000 to 1 million liras.

28 Refusal of registration

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

Currently the DPL or the Regulation on Registry do not provide any specific grounds on which the Turkish DPA could refuse to allow an entry on the Registry. In order to register with the Registry, an individual or a legal entity must be a data controller, and thus the Turkish DPA can refuse to allow an entry only if the applicant is not a data controller or if the data controller does not provide all of the required information for registry.

29 Public access

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

Yes, the DPL and the Regulation on Registry set forth that the Registry will be open to the public. According to the Regulation, the registration of data controllers will take place electronically based on VERBİS, which will be open to the public. Currently, the Turkish DPA is working on the technical aspects of VERBIS, and VERBIS is expected to be opened soon.

30 Effect of registration

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

No. Currently, the DPL or the Regulation on Registry do not explicitly attach any specific legal effect to entry on to the Registry.

31 Other transparency duties

Are there any other public transparency duties?

No, there are no other transparency duties.

Transfer and disclosure of PII

32 Transfer of PII

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

The DPL has regulated all transfers from data controllers to third parties, without making any differentiation in terms of outsourced data processors. Therefore, there is no specific provision or exemption applicable to the transfers of PII to entities that provide outsourced processing services.

33 Restrictions on disclosure

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

Other than adhering to the requirement of obtaining explicit consent from the data subject (in cases where there is no area of exception to obtaining such explicit consent), there are no further restrictions on the disclosure of PII to third parties within Turkey.

34 Cross-border transfer

Is the transfer of PII outside the jurisdiction restricted?

The general principle with regard to transfer of personal data outside of Turkey is that the explicit consent of the data subject is required. However, in the situation that one of the general exceptions of obtaining consent for personal data or for personal data of a sensitive nature exists, said personal data may be transferred outside of Turkey if the country of the recipient provides 'sufficient safeguards'. If the country where the recipient is located does not provide 'sufficient safeguards', the personal data may only be transferred if the data controllers in Turkey and in the related foreign country undertake to ensure sufficient protection in writing and the Turkish DPA authorises such transfer. Currently, there is no list specifying the countries that provide sufficient safeguards; however, the Turkish DPA is expected to publish a decision in this regard soon.

A general restriction that applies to the transfer of personal data outside of Turkey regards considerations of national interest. Reserving the applicable provisions of international agreements, in the situation that the interests of Turkey or the data subject will be seriously harmed, said personal data may only be transferred abroad with the consent of the Turkish Data Protection Board.

35 Notification of cross-border transfer

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

As stated above, in the situation that explicit consent for transfer has not been obtained and, instead, the data controller is to transfer personal data abroad based on one of the exceptions defined in the DPL, the country where the recipient is located must provide 'sufficient safeguards'. In the situation that the Turkish DPA has not determined said country to be on the list of 'countries providing sufficient safeguards', transfer of data abroad can only be completed if both data controllers provide written undertakings to ensure sufficient safeguards and if the Turkish DPA authorises the transfer.

However, this requirement of notification and authorisation is only required for a transfer abroad based on an exception to a recipient in a country not providing 'sufficient safeguards'. For all other transfers there are no general or specific obligations to notify the Turkish DPA or obtain authorisation for transfer.

36 Further transfer

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

Currently the DPL only explicitly covers the issue of the initial transfer abroad, with no explicit provisions detailing subsequent onward transfers. Consequently, it should be accepted that the provisions relating to transfer abroad apply equally to such further transfers, and the detailed explanations provided above should be taken into consideration.

Rights of individuals

37 Access

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.

As per the DPL, individuals have been granted the right to access their personal information held by data controllers. In addition to the right to learn whether or not their personal data is being processed, individuals also have a right to know the purpose of the processing of their data and whether the current processing is in accordance with this purpose and the right to know to whom their data is being transferred, both domestically and abroad.

However, these rights of access can be limited in the following situations, on the condition that it remains in accordance and proportional to the purpose and principles of the DPL where:

- the processing is required for the prevention or investigation of a crime;
- the data being processed has been made public by the data subject;
- the processing is required for disciplinary investigations or procedures by authorised public bodies and institutions or by professional organisations with public institution status and for the inspections carried out by such parties in accordance with their statutory purview; and
- the processing is required to protect the state's economic and financial interests with regard to the issues of budget, taxation and financial issue.

38 Other rights

Do individuals have other substantive rights?

In addition to the rights explained in our response to question 37, the DPL has also granted individuals other substantive rights to exercise.

As per article 11 of the DPL, data subjects have the following substantive rights with regard to the processing of their personal data:

- the right to ask for rectification of any data that has been processed in an incomplete or wrong manner;
- the right to request the deletion or destruction of their personal data where the grounds of processing of the personal data no longer exist;
- the right to have their requests of rectification or deletion notified to any third parties to whom their personal data has been transferred; and
- the right to object to a decision made against them based solely on analysis of personal data through automated processing.

39 Compensation

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?

The DPL clearly states that individuals have the right to compensation in the situation that the unlawful processing of their personal data has caused them to suffer damage. Therefore, in the situation that a breach of the DPL causes a person damage, she or he will be able to file a compensation action seeking monetary damages against the offending data controller.

Under Turkish law, compensation claims can be filed for both pecuniary and non-pecuniary damages for pain and suffering. However, it should be noted that in Turkish practice, non-pecuniary damages are rarely granted in situations where there has not been actual damage.

40 Enforcement

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

The DPL provides that data subjects must first apply to the relevant data controller with any complaints that they have regarding the exercise of their data protection rights. Should such an application not be answered in 30 days, rejected or should the data subject be unsatisfied with the response, the data subject will then have the right to refer the complaint to the Turkish DPA.

In addition to the complaint procedure that can ultimately be referred to the Turkish DPA for resolution, data subjects may exercise their rights relating to unlawful access or transfer of their personal data through the judicial system.

Exemptions, derogations and restrictions

41 Further exemptions and restrictions

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

Other than the exemptions and derogations explained above in questions 5, 14 and 25, there are no further exemptions or limitations on the application of the provisions of the DPL.

Supervision

42 Judicial review

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

As the Turkish DPA is an administrative body, as per the general principles of Turkish administrative law, the decisions and actions of the body can be appealed through administrative courts.

Specific data processing

43 Internet use

Describe any rules on the use of 'cookies' or equivalent technology.

While there are no general legislative or regulatory measures relating to the use of cookies, the ECL does contain rules on the use of cookies that are specific to operators that have been licensed in accordance with the relevant electronic communication legislation. As per said specific rules, licensed operators may only store information on the devices of their customers, or reach stored information on these devices if they have obtained informed and explicit consent.

However, it should be noted that for any use of cookies that will involve PII, the relevant safeguards and measures of the DPL will also apply.

44 Electronic communications marketing

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

The general rules on marketing through any means of electronic communication have been defined in the E-Commerce Law. As per the E-Commerce Law, the general rule for sending any form of electronic commercial communication is that the consent of the recipient is obtained in advance. Such consent may be obtained either in writing or by using any form of electronic communication tool. Additionally, such recipients must always be provided the opportunity to opt out of receiving such communication at any time and without having to specify any reason.

Certain electronic communications can be sent without first obtaining the explicit consent of the recipient. These communications are either communications with the purpose of providing information on the changes, use and repair of the provided goods or services sent to recipients who have readily provided their contact information, or if the electronic communications are being sent to a tradesmen or merchant. However, such recipients should also be provided with the aforementioned chance to opt out of receiving such electronic communications.

Furthermore, the content of the electronic commercial communication must be in line with the consent obtained from the recipient.

45 Cloud services

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

There are currently no rules or regulatory guidance specifically relating to the use of cloud computing services. However, the Information and Communication Technologies Authority has been working on a draft guidance document relating to standards that should be adopted in this area.

Furthermore, in accordance with the aforementioned provisions of the DPL regarding the transfer of data to third parties and transfer of data abroad, it should be noted that the requirements relating to such transfers can also be applied to situations where cloud computing services are obtained from companies with servers abroad.

Getting the Deal Through

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
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
Dispute Resolution
Distribution & Agency
Domains & Domain Names
Dominance
e-Commerce
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
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
Loans & Secured Financing
Mediation
Merger Control
Mining
Oil Regulation
Outsourcing
Patents
Pensions & Retirement Plans
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-Private Partnerships
Public Procurement
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
State Aid
Structured Finance & Securitisation
Tax Controversy
Tax on Inbound Investment
Telecoms & Media
Trade & Customs
Trademarks
Transfer Pricing
Vertical Agreements

Also available digitally

Online

www.gettingthedealthrough.com

ISBN 978-1-78915-010-0