Data Protection & Privacy

In 31 jurisdictions worldwide

Contributing editor
Rosemary P Jay

2015

GETTING THE DEAL THROUGH

GETTING THE DEAL THROUGH

Data Protection & Privacy 2015

Contributing editor

Rosemary P Jay

Hunton & Williams

Publisher
Gideon Roberton
gideon.roberton@lbresearch.com

Subscriptions
Sophie Pallier
subscriptions@gettingthedealthrough.com

Business development managers
George Ingledew
george.ingledew@lbresearch.com

Alan Lee
alan.lee@lbresearch.com

Dan White
dan.white@lbresearch.com

Law Business Research

THE QUEEN'S AWARDS FOR ENTERPRISE: 2012

Published by
Law Business Research Ltd
87 Lancaster Road
London, W11 1QQ, UK
Tel: +44 20 7908 1188
Fax: +44 20 7229 6910

First published 2012
Third edition
ISSN 2051-1280

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

CONTENTS

Turkey

Gönenç Gürkaynak and İlay Yılmaz

ELIG, Attorneys-at-Law

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? Have any international instruments on privacy or data protection been adopted in your jurisdiction?

Turkey does not currently have a dedicated data protection law in force, but there is draft legislation awaiting ratification, entitled the 'Draft Law on the Protection of Personal Data' (the Draft Law). Turkey is a party to United Nations Universal Declaration of Human Rights and Convention for the Protection of Human Rights and Fundamental Freedoms and has signed the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, but has not yet ratified it.

The legislative framework for the protection of PII in Turkey can be defined under four legal and legislative dimensions: rights on personal data under public law rules, rights on personal data under private law rules, rights on personal data under criminal rules and rights under the Draft Law.

Rights on personal data under public law rules

These rights are stipulated in the Turkish Constitution of 1982. The applicable legislation is section 5 of the Turkish Constitution entitled 'Privacy and protection of private life' and, in particular, article 20, which regulates the act of processing – without any definitions – and states that personal data may only be processed in cases where it is stipulated by law or with the owner's explicit consent and article 22, which regulates the privacy of communication and states that communication cannot be hindered and its privacy cannot be violated.

Similarly, the same protection is provided under article 12 of the United Nations Universal Declaration of Human Rights of 10 December 1948 and article 12 of the Convention for the Protection of Human Rights and Fundamental Freedoms of 4 November 1950, both of which Turkey is party to, as indicated above.

Rights on personal data under private law rules

These rights are stipulated in the Turkish Civil Code (the TCC). Article 23 et seq of the TCC includes provisions regulating the protection of personal rights in general. The TCC does not provide either a comprehensive or numerus clausus list in respect of personal rights and leaves the matter to the discretion of judges. Therefore, the question of whether such data will be qualified as a personal right within the meaning of the TCC will depend on the judicial precedents on the matter.

To give an example of judicial precedent, in its decision dated 15 May 2006, No. 2005/6811E,2006/1959K, the 12th Chamber of State Council defined personal data as 'any information that belongs to an identified person or any information that directly or indirectly leads to identification of a person, especially with respect to any ID number or physical, psychological, intellectual, economic, cultural or social status'. The relevant jurisprudence and academic research give weight to the will of the data owner (ie, whether the data owner considers the collected data to be personal). Since personal data is generally defined as the 'data which relate to a person who is identifiable from such data', there should be no doubt that such would be deemed as a personal right. Consequently, collecting, publishing and communicating personal data without the prior consent of such person may obviously be deemed a violation of personal rights under the TCC.

Rights on personal data under criminal rules

These rights are stipulated in the Turkish Criminal Code (the Criminal Code). Unlike the TCC, the Criminal Code adopts a definition of 'personal data', which is similar to the definition provided in the Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, details of which can be explained below in question 3. On this basis, the rationale of the Criminal Code makes reference to the penal code of France and states that 'information relating to and sufficient enough to identify an individual' would qualify as 'personal data' within the meaning of section 9 of the Criminal Code.

Pursuant to section 9 of the Criminal Code dealing with 'crimes against private life and privacy', recording or acquisition of personal data amounts to a crime which, depending on the circumstances, may trigger imprisonment of up to four years.

Rights on personal data under criminal rules and the Draft Law

Turkey signed the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (Convention No. 108) in 1981 but has not yet ratified it. The Turkish Ministry of Justice has been working on the draft legislation and the Draft Law was completed and sent to the Prime Ministry to be later referred to the Grand National Assembly of Turkey for ratification. The Draft Law was sent to the Grand National Assembly of Turkey by the prime minister on 22 April 2008 for the first time and it is still pending before the Grand National Assembly of Turkey. The Draft Law is based on the Convention No. 108 and the European Data Protection Directive (1995/46/EC).

One should stress in advance that Turkish law gives effect to the general principle of lex specialis, according to which a special rule dealing with a specific matter prevails over a general rule on the same matter. As a result, the Draft Law, when entered into force, would be the primary legal source for and apply in priority to the matters regarding PII. Nevertheless, if an individual seeks legal remedies against a legal entity regarding data privacy, he or she may always rely on and have recourse to the actions provided under the general rules, in particular those provided under article 23 et seq of the TCC and article 135 et seq of the Criminal Code.

The Draft Law defines personal data as any 'information relating to an identified or identifiable individual' and provides that data owners should be informed of and consent to the data collection and storing. Except as required by law, any objection by the data owner to the data collection will invalidate such data collection.

2 Data protection authority

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

There is no specific data protection authority in Turkey. Currently, Turkish courts are entitled to stop the distribution, publication etc. of any personal data that are used without the owner's permission and/or against the law. To give an example, in a precedent of the Supreme Court Assembly of Chambers (2001/4-926E and 2001/742K) dated 17 October 2001, a photograph of a person was published without permission, and the court of first instance decided to stop the publication and distribution of the photograph as injunctive relief.

Pursuant to article 139 of the Criminal Code, crimes stipulated under section 9 of the Criminal Code are ex officio investigated by the public prosecutor and are not subject to the complaint by the injured party, as will be explained in detail under question 3.

Under the Draft Law, a supervisory authority will be established, called the Council of Protection of Personal Data, with the authority to supervise the compliance of the data processing systems.

Additionally, article 6 of the Electronic Communications Law entitled 'Competencies of the Authority' states that the Information and Communication Technologies Authority is responsible for making the necessary arrangements and supervisions pertaining to the rights of subscribers, users, consumers and end users, as well as the processing of personal data and protection of privacy. The Information and Communication Technologies Authority exercises its authority through the Information and Communication Technologies Board (Board). There are a significant number of Board decisions imposing general data protection principles on operators in the electronic communications sector. Furthermore, pursuant to article 51 of the Electronic Communications Law Information and Communication Technologies Authority is entitled to determine the procedures and principles towards the processing of personal data and the protection of its privacy regarding the electronic communications sector.

3 Breaches of data protection

Can breaches of data protection lead to criminal penalties? How would such breaches be handled?

Breaches of data protection might lead to criminal penalties. Rights on personal data under criminal rules are stipulated in section 9 of the Criminal Code. The relevant provisions of section 9 of the Criminal Code are as follows:

- Article 135(1) of the Criminal Code reads as follows: 'He whoever unjustly records personal data shall be imprisoned from six months up to three years.'
- Article 136 of the Criminal Code reads as follows: 'He whoever unjustly acquires or disseminates personal data or gives personal data to somebody else shall be imprisoned from one year up to four years.' Article 136, without making a distinction between international and domestic data transfers, states that anyone who unlawfully transfers personal data shall be sentenced.
- Article 138 of the Criminal Code provides that any person who fails to destroy any personal data even after the storage periods set out in the law have been passed shall be imprisoned from six months up to one year.
- In case such crimes are committed by a legal entity, the entity will be subject to the security measures set out under article 60 of the Criminal Code. Such security measures are, as the case may be, (i) if the entity carries out its commercial activities by virtue of a permit granted by a public institution, cancellation of such permit of activity, and (ii) seizure of the relevant goods and objects that were used in committing the crime.

It is of significant importance for a legal entity and its managers to ensure compliance with these criminal provisions, as failure to do so would have serious negative consequences on the part of both the legal entity and its managers.

The Draft Law also defers to the provisions of the Criminal Code, defined above, if the matter within the scope of the Draft Law constitutes a crime.

Scope

4 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?

As will be further explained in question 5, data protection law covers all sectors and types of organisations with the exception of some areas of activity that relate to:

- national security matter;
- organised crime regarding drug trafficking or manufacturing;
- organised crime regarding illegal profit and crimes committed via threat and violence; and
- crimes committed against the government.

In addition to the foregoing exceptions, article 22 of the Draft Law adds the exception of matters related to budget, tax and economic issues that hold important interest and benefit to the government.

5 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.

Pursuant to article 5 of the Regulation on the Authorisation for Electronic Communications (Regulation), telecommunication services may be provided by obtaining the authorisation of Information and Communication Technologies Authority (Authority). Pursuant to article 19 of the Regulation, operators are obliged to establish the necessary technical infrastructure, even before they start to provide any services, and keep them up to date in order to fulfil the requests of competent authorities under the relevant laws. Operators are obliged to provide any and all information, document and data to these authorised authorities in a timely manner.

Pursuant to paragraph (u) of article 19 of the Regulation, the authorities (ie, courts, public prosecutors, Telecommunications Presidency, General Directorate of Security and Police Intelligence Department) may request user data or relevant information regarding user data, from the operators, in case of a national security matter and under the relevant provisions of Law No. 5397 on Amendments to be Made to Various Laws (Law No. 5397) and Law No. 5651 on Regulation of Broadcasts via Internet and Prevention of Crimes Committed Through Such Broadcasts (Law No. 5651).

According to these laws, the authorities may request such information from the operator, including but not limited to the following cases:

- with respect to the amendment made by Law No. 5397 (ie, the additional article 7 of Law No. 2559 on Police Powers), competent authorities may request such information from operators, in case of:
  - national security matters;
  - organised crime regarding drug trafficking or manufacturing;
  - organised crime regarding illegal profit and crimes committed via threat and violence; or
  - crimes committed against the government; and
- Pursuant to the additional article 7, the competent authorities are the courts, but in urgent matters, by written order of the director of General Directorate of Security or Head of Police Intelligence Department, communication via telecommunication can be located, monitored, recorded and signal information can be evaluated.

Article 5 of the Regulation on the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector stipulates that communications and the related traffic data are confidential in principle and any kinds of interception (including but not limited to listening, tapping or storage) or surveillance of communications without the consent of the parties of communication is prohibited. However, the same provision allows exceptions in circumstances where the interception or surveillance of communication is required by relevant legislation or a judicial decision.

6 Other laws

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

'Regulation on the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector' (Regulation on Electronic Communications) has been published in the Official Gazette of 24 July 2012 and entered into force as of 24 July 2013. This regulation sets out the procedures and principles to be followed by operators (ie, any legal entity authorised to provide electronic communications services or to provide an electronic communications network and to operate the infrastructure) performing activity in the electronic communications sector for the processing and retention of PII and the protection of privacy in the electronic communications sector. The Regulation on Electronic Communications stipulates certain obligations for these operators, such as taking necessary preventive measures for the protection of personal data, notifying the

users or subscribers of violation risks or of existing violations of personal data protection. Furthermore the main principles for processing personal data, stipulated under the Regulation on Electronic Communications, are quite similar to the principles set out in the Convention for the Protection of Individuals with Regard to the Automatic Processing of Personal Data (Convention No. 108) for personal data subject to automatic processing. The Regulation on Electronic Communications encompasses the retention of data including PII, traffic data and location data. However, the retention of the communication's content is not included in the scope of the Regulation, and moreover it is expressly excluded with a specific provision.

Article 73 of Banking Law No. 5411 (Law No. 5411) stipulates that personal, and therefore confidential, information must not be disclosed by banks and real persons who had acquired such information because of their role or duties, even after they leave their role or duties, except when requested by the competent authorities. In addition to the authorisation of public prosecutors and courts, article 95 of Law No. 5411 also entitles the Banking Regulation and Supervision Agency (the Agency) to audit banks and to request any information (including those classified as confidential). The banks, their subsidiaries, associations, branches, representative offices and outsourcing institutions, as well as any other real or legal persons, are obliged to provide any and all necessary systems, passwords, documents, records and information upon such request.

Pursuant to article 23 of the Bank Cards and Credit Cards Law, member merchants cannot disclose, keep or copy the information they acquired from consumers without their consent, except to the competent authorities. Member merchants cannot share, sell, buy or trade such information, and may only do so with the affiliated bank card issuer. Bank card issuers may also be held liable with this article; they are responsible for supervising member merchants to ensure that they comply with law or bank card issuers and member merchants might be subject to imprisonment for up to three years.

Another provision in this respect is governed under the Turkish Labour Law. Article 75 of the Labour Law stipulates that the employers are obliged to keep personal files on their employees but are obliged to use this information in good faith, consistent with the law.

Under the Medical Deontology Bylaw and Patient Rights Regulation, information obtained during medical procedures cannot be disclosed unless required by law.

Besides, the Regulation on Security and Sharing of General Health Insurance Data became effective as of 11 July 2012. This regulation sets out the principles and procedures regarding protection and sharing of health data stored in the database related to the Social Security Authority and contracted health service providers.

Additionally the Ministry of Health announced a draft regulation, entitled 'The Draft Regulation on Processing of Personal Medical Data and Maintaining Data Privacy'. This regulation is at its initial legislative stage as it is only available for public opinion at present. The purpose of this regulation is expressed as to maintain the privacy of personal medical data, regulate the processing of such data and to set out the principles and procedures to be followed by the persons (including both real persons and legal entities) processing such data.

7 PII formats

What forms of PII are covered by the law?

As the form of PII is not explicitly defined under the foregoing legislation, and rather broad and varying definitions of PII are given, it may be concluded that all forms of PII are covered by the legislations, as applicable.

8 Extraterritoriality

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

It is not explicitly stated in the Draft Law whether the law only applies in Turkey, or also applies to data owners and data processors abroad. Transfer of PII to data owners and data processors abroad is, however, separately stipulated, and by way of analogy it can be concluded that the Draft Law's reach is limited to data owners and data processors established or operating in Turkey.

On criminal issues the Draft Law defers to the Criminal Code. Article 8 of the Criminal Code states that 'Turkish law is applied to the offences that are committed in Turkey'. Where the act constituting an offence is partially or entirely committed in Turkey or the result is felt in Turkey, the offence is assumed to have been committed in Turkey.

9 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 services to owners?

The Draft Law draws a distinction between PII owners and PII processors. In article 15 of the Draft Law, it is stipulated that PII owners are obliged to make sure PII processors take the necessary technical and administrative precautions, should they provide them with PII.

Notwithstanding the foregoing, the Draft Law does not draw any distinction between PII owners and processors in terms of liability, as the relevant provisions are governed in a manner such that the important point is the violating act rather than the person who carried it out.

Legitimate processing of PII

10 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?

Article 20 of the Constitution deals with the act of processing PII – without any definitions – and states that personal data may only be processed in cases where it is stipulated by law or with the owner's explicit consent.

Similar to the provisions of Turkish Constitution, prior consent of the data owner is considered as a legitimising factor in terms of the provisions of TCC. The TCC, except for cases where there is a higher private or public interest, or the exercise of legal authority, does not require the data owner's consent.

The valid consent of the data owner is required to ensure that data collection, publishing and communicating is in compliance with law.

Similarly, the Draft Law provides that data owners should be informed of and should consent to the data collection and storage. Except as required by law, any objection by the data owner to the data collection will invalidate such collection. The data may only be stored for specific and legitimate purposes and not reprocessed in a way incompatible with those purposes. The data must be preserved in a way so as to enable identification of the data owner and shall be kept for no longer than storage purposes require.

Furthermore, article 4 of the Regulation on Electronic Communications requires personal data to be processed fairly and lawfully; processed upon the consent of the data subject; processed adequately, relevantly and not excessively in relation to the purposes for which the data were collected; accurate and, where necessary, kept up to date and kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which it is further processed.

11 Legitimate processing – types of data

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

Article 7 of the Draft Law prohibits, with certain exceptions, the data processor from processing personal data on the data owner's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health or private life, and convictions.

Regarding personal and family life, such data as described above may be processed with the consent of the person or as required by law (ie, public interest, criminal and administrative prosecutions, and medical issues).

Data handling responsibilities of owners of PII

12 Notification

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

Currently, legislation on the protection of PII does not cover such an obligation. Having said that, articles 4 et seq and 12 of the Draft Law oblige the data processor to process personal data for -legitimate and specified purposes only, and not to reprocess it in a way incompatible with those purposes, and inform the data owner of any personal data being processed.

During the data collection, the data processor must provide the data owner with:

- its identity;
- the purposes of the data collection;
- the recipients of the personal data;
- the method, legal grounds and possible outcomes of the data collection; and
- the right of access to and the right to rectify the collected data, as they may relate to the data owner.

A definite time period is not stipulated herein as the Draft Law only refers to the time period of notification as 'during the data collection'.

13 Exemption from notification

When is notice not required?

Pursuant to article 12 of the Draft Law, an individual might not be notified in a case of national security, intelligence issue or if a crime is to be prevented. An individual might also not be notified so as not to hinder a criminal prosecution.

14 Control of use

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

Pursuant to article 12 of the Draft Law, the data owner has the right to request (i) confirmation on whether his or her personal data are being processed, (ii) any such personal data undergoing processing, (iii) correction of such date if the content of the data is inaccurate or false, (iv) erasure or blocking of such data, if the content of the data is unlawful, or (v) notification of any correction, erasure or blocking to third parties to whom the data have been disclosed.

Article 6 of the Draft Law stipulates that PII cannot be processed without consent of the individual, unless required or permitted by law.

15 Data accuracy

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

Pursuant to the Draft Law, data must be adequate, relevant and not excessive in relation to the purposes for which they are stored. The data must be accurate and, where necessary, kept up to date.

16 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?

Article 138 of the Criminal Code provides that any person who fails to destroy any personal data after the storage periods set out in the law have been passed will be imprisoned for between six months and one year. Article 138 does not define the storage periods but defers to the legislation under which personal data-related provisions are governed.

To give an example regarding storage periods set out in the law, under article 42 of the Law No. 5411 and pursuant to article 17 of the Regulation on the Procedures and Principles for Accounting Practices and Retention of Documents by Banks, banks are obliged to keep the originals of any documents concerning their operations within their own premises for a period of 10 years (or if keeping originals is not possible, copies of any letters sent to customers or private or public entities, including any letters, telegrams, e-mails, notices and notifications and any other letters received from their customers or public or private entities and organisations) for presentation to the competent authorities whenever requested.

17 Finality principle

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

As previously stated, the Draft Law stipulates that the data may be stored for specific and legitimate purposes only and not reprocessed in a way incompatible with those purposes. The data must be adequate, relevant and not excessive in relation to the purposes for which they are stored.

18 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?

During the data collection, the data controller must provide the data owner with the purposes of the data collection. The provisions of the Draft Law are not explicit in defining the limits of such purpose.

Security

19 Security obligations

What security obligations are imposed on data owners and entities that process PII on their behalf?

Such obligations are governed under the Draft Law. Although the security obligations are not specified explicitly, article 15 of the Draft Law states that technical and administrative precautions must be taken in order to prevent destruction, loss, altering of data not consistent with the law or with imprudence, or disclosure of such data without authorisation.

20 Notification of security breach

Does the law include obligations to notify the regulator or individuals of breaches of security?

The Draft Law does not include any explicit provisions regarding the obligation to notify the regulator or individuals of breaches of security.

On the other hand, the Regulation on Electronic Communications obliges the operators to inform the Information and Communication Technologies Authority and its subscribers or users concerning the risks of a breach in an efficient manner and without undue delay. According to article 6 of the Regulation on Electronic Communications, if a personal data breach occurs, the operator shall inform the Information and Communication Technologies Authority in relation to details of the notification to be made to subscribers or users concerning the nature and consequences of the mentioned breach and measures taken for addressing the breach.

Internal controls

21 Data protection officer

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

Article 20 of the Draft Law entitles the PII owners or processors to appoint an independent audit institution. These independent audit institutions are obliged to keep the personal data register (the Register) as stipulated in article 16 of the Draft Law and audit the PII owners or processors within the scope of the Draft Law.

22 Record keeping

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

Pursuant to article 17 of the Draft Law, any changes made related to the criteria for being registered will need to be notified to the High Council of Protection of Personal Data at the end of each year.

The Draft Law is not explicit about any records or documentation but it is stated in article 33 of the Draft Law that the PII owner is obliged to provide any and all information and documents at the request of the High Council. By way of analogy, it might be concluded that the PII owner is required to maintain internal records and documentation.

Registration and notification

23 Registration

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

Pursuant to article 16 and 17 of the Draft Law, an application is required to be submitted to the Council of Protection of Personal Data before putting a system in place regarding the collection of personal data. The Council of Protection of Personal Data will establish a database thereof (ie, the Register).

24 Formalities

What are the formalities for registration?

The application filing must contain, inter alia; (i) the identity of the legal entity and – if any – of its representative; (ii) the purposes of the processing for which the data are intended; (iii) explanatory statements as to the data owners, categories of data owners and the respective data categories; (iv) the recipients or categories of recipients of the data; and (v) a general explanation regarding the precautions taken pursuant to article 15, regulating technical and administrative precautions to be taken in order to prevent destruction, loss, altering of data contrary to the law or with imprudence, or disclosure of such data without authorisation. These requirements are not stated in the applicable legislation but in article 17 of the Draft Law.

25 Penalties

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

Article 37 of the Draft Law stipulates an administrative fine to be paid if a data owner or processor fails to make an entry into the Register, and a separate administrative fine if it fails to maintain such entry. Furthermore, the Draft Law defers to provisions of the Criminal Code if the reason of such failure to make an entry or maintain the entry in the Register also constitutes a crime.

26 Refusal of registration

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

Any changes or modifications in items listed in article 17 of the Draft Law (ie, necessary information such as purposes of processing personal data, the groups subject to the data and the explanations with respect to data categories that belong to them, to be submitted into the Register) must be notified to the Council of Protection of Personal Data at the end of each year. Should the Council find that the data processing system subject to application does not fulfil the foregoing conditions, it can ban the proposed system.

27 Public access

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

The Draft Law, in article 16, stipulates that the Register will be publicly available, but it does not explain how it will be accessed.

28 Effect of registration

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

The application filing, pursuant to article 17 of the Draft Law, must contain, inter alia, the purposes of the processing for which the data are intended and the recipients or categories of recipients of the data.

Transfer and disclosure of PII

29 Transfer of PII

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

The applicable laws require explicit consent of individuals to collect their PII, so it is possible to interpret by analogy that the transfer of PII to entities providing outsourced processing services will also be subject to explicit consent. Article 8 of the Draft Law stipulates that PII cannot be transferred to third persons, without consent or unless required by law.

30 Restrictions on disclosure

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

There is no specific restriction on the disclosure of PII as article 8 of the Draft Law is drawn up in such a manner that the general rule is non-disclosure of PII, and it is exceptional that PII be disclosed. Furthermore, pursuant to the applicable legislation, there is no provision restricting disclosure of PII to other recipients, but it regulates legal remedies that might be applied against the disclosure.

31 Cross-border transfer

Is the transfer of PII outside the jurisdiction restricted?

Article 14 of the Draft Law permits the transfer to a third country of personal data only if the third country of destination ensures an adequate level of protection to the rights of personality. Pursuant to article 14, the issue of whether any given third country ensures an adequate level of protection will be assessed by the Council of Protection of Personal Data on the basis of the international treaties between Turkey and the destination country in question and the de facto reciprocity between Turkey and the destination country regarding data transfer.

In addition, article 14 will not apply in cases where:

- the data owner (the employee) has given his or her unambiguous consent to the proposed transfer;
- the transfer is necessary for either the performance of a contract between the data owner and the data processor or the implementation of the pre-contractual relation between the parties;
- the transfer is necessary or legally required on prevention of crime, or for the establishment, exercise or defence of legal claims;
- the transfer is necessary in order to protect the vital interests of the data owner; or
- the transfer is made from a register that, according to laws or regulations, is intended to provide information to the public and that is open to consultation either by the public in general or by any person who can demonstrate legitimate interest.

On the basis of the foregoing, the system adopted by the Draft Law is very similar to the one under the European Data Protection Directive (1995/46/EC).

32 Notification of transfer

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

For the transfer of PII, authorisation is required from the Council of Protection of Personal Data, a body established pursuant to article 14 of the Draft Law.

33 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?

There no provisions governing restriction of or obtaining authorisation for transfer of PII outside the jurisdiction. In light of the possible interpretation of applicable legislation, however, it would be wise to obtain explicit consent for every step to be taken with respect to PII.

Rights of individuals

34 Access

Do individuals have the right to see a copy of their personal information held by PII owners? Describe any limitations to this right.

This matter is also regulated under the Draft Law. Article 12 states that anybody can apply to the PII owner and question whether data related to him or her is recorded and request such data if recorded. The PII owner is obliged to disclose the whole data and the processed data upon such request.

It is not explicitly stated in the Draft Law whether the applicant may obtain a physical copy of such data.

35 Other rights

Do individuals have other substantive rights?

A supervisory authority called the 'Council of Protection of Personal Data' will be established with the authority to supervise the compliance of the data processing systems with the Draft Law.

The data owner will be entitled to file objections with the High Council against any data processing involving him or her.

36 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?

Monetary damages or compensation in case of a breach of the Draft Law is not regulated therein. Therefore, from a legal perspective, any individual who suffers damages and losses may apply to the general provisions regulated under the applicable legislation. Under article 23 of the TCC, an individual whose personal rights are violated unjustly is entitled to file a claim for pecuniary and non-pecuniary damages.

Under Turkish law, an actual damage is required in order to file a claim for pecuniary damages whereas there is no such requirement for the claims for non-pecuniary damages.

37 Enforcement

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

Individuals who suffer damages and losses due to violation of PII protection may exercise their rights through the judicial system.

Exemptions, derogations and restrictions

38 Further exemptions and restrictions

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

No. The main exclusions and limitations are already described above.

Supervision

39 Judicial review

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

Pursuant to article 32 of the Draft Law, persons that apply to the Council of Protection of Personal Data may object its decisions to the competent administrative court. The subsequent provisions of the same article stipulate that PII owners are obliged to comply with the decisions and instructions of the Council of Protection of Personal Data. The Draft Law does not govern the right to appeal the decisions of the Council. Under general Turkish administrative law provisions, however, all owners are entitled to appeal such decisions before the competent administrative courts.

Update and trends

In a recent decision, the Turkish Constitutional Court annulled article 51 of the Electronic Communications Law, which entitles the Information and Communication Technologies Authority to regulate the principles and procedures for processing of and protecting privacy of personal data in the electronic communications sector (including the provision imposing the obligation of keeping the data in Turkey on the electronic communication service providers). The Turkish Constitutional Court's decision is expected to become effective six months after its publication in the Official Gazette. The decision has not yet been published by the Turkish Constitutional Court. Since the Constitutional Court deemed the authority of the Information and Communication Technologies Authority for regulating data protection and privacy void, the previously issued regulations (eg, the Regulation on Electronic Communications) and other regulatory transactions previously conducted by the Information and Communication Technologies Authority are expected to become null and void when the decision becomes effective. This would change the scope of the data protection and privacy environment in the electronic communications sector in Turkey.

40 Criminal sanctions

In what circumstances can owners of PII be subject to criminal sanctions?

Owners of PII might be subject to criminal sanctions pursuant to article 135 et seq of the Criminal Code.

41 Internet use

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

There is no specific rule on the use of 'cookies' under Turkish law.

42 Electronic communications marketing

Describe any rules on marketing by e-mail, fax or telephone.

Neither the applicable legislation nor the Draft Law regulates any provision with respect to marketing by e-mail, fax or telephone. Therefore, any marketing activity in this respect would be subject to the provisions already outlined.

ELİG
Attorneys at Law

Gönenç Gürkaynak **gonenc.gurkaynak@elig.com**
İlay Yılmaz **ilay.yilmaz@elig.com**

Çitlenbik Sokak No: 12
Yıldız Mahallesi
Beşiktaş
34349 Istanbul
Turkey

Tel: +90 212 327 1724
Fax: +90 212 327 1725
www.elig.com

Getting the Deal Through

Acquisition Finance
Advertising & Marketing
Air Transport
Anti-Corruption Regulation
Anti-Money Laundering
Arbitration
Asset Recovery
Aviation Finance & Leasing
Banking Regulation
Cartel Regulation
Climate Regulation
Construction
Copyright
Corporate Governance
Corporate Immigration
Data Protection & Privacy
Debt Capital Markets
Dispute Resolution
Domains and Domain Names
Dominance
e-Commerce
Electricity Regulation
Enforcement of Foreign Judgments
Environment
Foreign Investment Review
Franchise
Gas Regulation
Government Investigations
Insurance & Reinsurance
Insurance Litigation
Intellectual Property & Antitrust
Investment Treaty Arbitration
Islamic Finance & Markets
Labour & Employment
Licensing
Life Sciences
Mediation
Merger Control
Mergers & Acquisitions
Mining
Oil Regulation
Outsourcing
Patents
Pensions & Retirement Plans
Pharmaceutical Antitrust
Private Antitrust Litigation
Private Client
Private Equity
Product Liability
Product Recall
Project Finance
Public-Private Partnerships
Public Procurement
Real Estate
Restructuring & Insolvency
Right of Publicity
Securities Finance
Ship Finance
Shipbuilding
Shipping
State Aid
Tax Controversy
Tax on Inbound Investment
Telecoms and Media
Trade & Customs
Trademarks
Transfer Pricing
Vertical Agreements

Also available digitally

Online

www.gettingthedealthrough.com

iPad app

Available on iTunes

Law Business Research

Data Protection & Privacy
ISSN 2051-1280

THE QUEEN'S AWARDS FOR ENTERPRISE: 2012

LACCA
LATIN AMERICAN CORPORATE COUNSEL ASSOCIATION

Official Partner of the Latin American Corporate Counsel Association

ABA Section of International Law
Your Gateway to International Practice

Strategic Research Partner of the ABA Section of International Law