The Privacy, Data Protection and Cybersecurity Law Review

Third Edition

Editor
Alan Charles Raul

Law Business Research

The Privacy, Data Protection and Cybersecurity Law Review

Third Edition

Editor
Alan Charles Raul

Law Business Research Ltd

PUBLISHER
Gideon Roberton

SENIOR BUSINESS DEVELOPMENT MANAGER
Nick Barette

BUSINESS DEVELOPMENT MANAGER
Thomas Lee

SENIOR ACCOUNT MANAGERS
Felicity Bown, Joel Woods

ACCOUNT MANAGERS
Jessica Parsons, Jesse Rae Farragher

MARKETING COORDINATOR
Rebecca Mogridge

EDITORIAL ASSISTANT
Gavin Jordan

HEAD OF PRODUCTION
Adam Myers

PRODUCTION EDITOR
Anne Borthwick

SUBEDITOR
Anna Andreoli

CHIEF EXECUTIVE OFFICER
Paul Howarth

Published in the United Kingdom
by Law Business Research Ltd, London
87 Lancaster Road, London, W11 1QQ, UK

www.TheLawReviews.co.uk

ISBN 978-1-910813-32-4

Printed in Great Britain by
Encompass Print Solutions, Derbyshire
Tel: 0844 2480 112

THE LAW REVIEWS

THE MERGERS AND ACQUISITIONS REVIEW

THE RESTRUCTURING REVIEW

THE PRIVATE COMPETITION ENFORCEMENT REVIEW

THE DISPUTE RESOLUTION REVIEW

THE EMPLOYMENT LAW REVIEW

THE PUBLIC COMPETITION ENFORCEMENT REVIEW

THE BANKING REGULATION REVIEW

THE INTERNATIONAL ARBITRATION REVIEW

THE MERGER CONTROL REVIEW

THE TECHNOLOGY, MEDIA AND
TELECOMMUNICATIONS REVIEW

THE INWARD INVESTMENT AND
INTERNATIONAL TAXATION REVIEW

THE CORPORATE GOVERNANCE REVIEW

THE CORPORATE IMMIGRATION REVIEW

THE INTERNATIONAL INVESTIGATIONS REVIEW

THE PROJECTS AND CONSTRUCTION REVIEW

THE INTERNATIONAL CAPITAL MARKETS REVIEW

THE REAL ESTATE LAW REVIEW

THE PRIVATE EQUITY REVIEW

THE ENERGY REGULATION AND MARKETS REVIEW

THE INTELLECTUAL PROPERTY REVIEW

THE ASSET MANAGEMENT REVIEW

THE PRIVATE WEALTH AND PRIVATE CLIENT REVIEW

THE MINING LAW REVIEW

THE EXECUTIVE REMUNERATION REVIEW

THE ANTI-BRIBERY AND ANTI-CORRUPTION REVIEW

THE CARTELS AND LENIENCY REVIEW

THE TAX DISPUTES AND LITIGATION REVIEW

THE LIFE SCIENCES LAW REVIEW

THE INSURANCE AND REINSURANCE LAW REVIEW

THE GOVERNMENT PROCUREMENT REVIEW

THE DOMINANCE AND MONOPOLIES REVIEW

THE AVIATION LAW REVIEW

THE FOREIGN INVESTMENT REGULATION REVIEW

THE ASSET TRACING AND RECOVERY REVIEW

THE INSOLVENCY REVIEW

THE OIL AND GAS LAW REVIEW

THE FRANCHISE LAW REVIEW

THE PRODUCT REGULATION AND LIABILITY REVIEW

THE SHIPPING LAW REVIEW

THE ACQUISITION AND LEVERAGED FINANCE REVIEW

THE PRIVACY, DATA PROTECTION AND CYBERSECURITY LAW REVIEW

THE PUBLIC-PRIVATE PARTNERSHIP LAW REVIEW

THE TRANSPORT FINANCE LAW REVIEW

THE SECURITIES LITIGATION REVIEW

THE LENDING AND SECURED FINANCE REVIEW

THE INTERNATIONAL TRADE LAW REVIEW

THE SPORTS LAW REVIEW

THE INVESTMENT TREATY ARBITRATION REVIEW

THE GAMBLING LAW REVIEW

THE INTELLECTUAL PROPERTY AND ANTITRUST REVIEW

THE REAL ESTATE, M&A AND PRIVATE EQUITY REVIEW

THE SHAREHOLDER RIGHTS AND ACTIVISM REVIEW

www.TheLawReviews.co.uk

ACKNOWLEDGEMENTS

The publisher acknowledges and thanks the following law firms for their learned assistance throughout the preparation of this book:

ALLENS

ASTREA

BAKER & MCKENZIE - CIS, LIMITED

BOGSCH & PARTNERS LAW FIRM

CMS CAMERON MCKENNA GRESZTA I SAWICKI SP.K

DUNAUD CLARENC COMBLES & ASSOCIÉS

ELIG, ATTORNEYS-AT-LAW

GIANNI, ORIGONI, GRIPPO, CAPPELLI & PARTNERS

JUN HE LAW OFFICES

LEE & KO

MATHESON

NNOVATION LLP

SANTAMARINA Y STETA, SC

SIDLEY AUSTIN LLP

SIQUEIRA CASTRO – ADVOGADOS

SK CHAMBERS

SUBRAMANIAM & ASSOCIATES

URÍA MENÉNDEZ ABOGADOS, SLP

VIEIRA DE ALMEIDA & ASSOCIADOS, SP RL

WALDER WYSS LTD

WINHELLER RECHTSANWALTSGESELLSCHAFT MBH

CONTENTS

Chapter 26

TURKEY

Gönenç Gürkaynak and İlay Yılmaz[1]

I OVERVIEW

The Data Protection Law (DP Law), which has been pending since 2003, was published in the Official Gazette of 7 April 2016. This is the first separate and dedicated legislation covering general data protection in Turkey. The DP Law is based on the EU Data Protection Directive 95/46/EC (EU Data Protection Directive), although it differs from the Directive in certain aspects.

A number of provisions applicable to data protection and privacy can also be found in a variety of other Turkish laws, including the Constitution of the Republic of Turkey of 9 November 1982 (Constitution), and there are certain sector-specific regulations on this matter as well. The general provisions that are applicable to data protection and privacy are as follows:

a Article 20 (Privacy of Private Life) and Article 22 (Freedom of Communication) of the Constitution;

b Article 24 (Protection of Personality against Violations) of the Turkish Civil Code (TCC); and

c Article 135 (Recording of Personal Data), Article 136 (Unlawfully Disseminating or Capturing Data), Article 138 (Failure to Destroy Data) and Article 244 (Preventing and Impairing the System, Altering or Destroying Data) of the Turkish Criminal Law, which regulate unlawful storage of, transmission, reception or alteration of, and destruction of or failure to destroy personal data, respectively.

Moreover, the Regulation on Security of Electronic Communications, effective as of 13 July 2014, contains certain provisions on data security in the context of electronic communications.

1 Gönenç Gürkaynak is managing partner and İlay Yılmaz is a partner at ELIG, Attorneys-at-Law.

Turkey also has a regulation on electronic commerce, entitled the Law on Regulation of Electronic Commerce (Law on E-Commerce), which regulates the principles and procedures regarding electronic commerce and imposes certain obligations on the main actors in electronic commerce with respect to the protection and processing of personal data. The Law on E-Commerce came into effect on 5 December 2014.

In addition, there are some sector-specific regulations particular to data protection and privacy, including:

a the Regulation on Processing and Protection of Privacy of Personal Data in the Electronic Communications Sector;

b the Regulation on Protection and Sharing of the General Health Insurance Data; and

c the Regulation on Data Privacy and Principles and Procedures Regarding Security of Confidential Data in the Official Statistics.

Turkey is a party to the United Nations Universal Declaration of Human Rights and the 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. The Law on Ratification of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of the Council of Europe (Convention 108) is published in the Official Gazette of 18 February 2016 and came into force on the same date.

Cybersecurity is not regulated by specific legislation in Turkey, but cybersecurity provisions are found in incidental regulations. A governmental step to maintain cybersecurity in Turkey was taken with a decision regarding conducting, managing and coordinating national cybersecurity activities that came into force on 20 October 2012. On 20 June 2013, another decision on the National Cyber Security Strategy and 2013–2014 Action Plan came into force. Under the decision of 20 October 2012, a Cyber Security Board was established in Turkey.

Privacy and data protection are treated as coextensive concepts in the DP Law. However in sector-specific regulations, privacy and data protection are regulated distinctly, such as privacy of private life, which is regulated under the Turkish Penal Code (TPC). Articles 134–140 of the TPC regulate the protection of privacy and define violation of the confidentiality of private life as a crime punishable by imprisonment.

The right to privacy and protection of an individual's private life is enshrined in the Constitution. Accordingly, everyone has freedom of communication, and privacy of communication is a fundamental right.

Rights on personal data under private law rules are stipulated in 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. The question of whether data will be qualified as a personal right within the meaning of the TCC will depend on the judicial precedents on the matter. See Section III.i, *infra* regarding recent judicial precedents defining 'personal data'.

Rights on personal data under criminal rules are separately governed under the TPC. The definition of 'personal data' under criminal law is similar to the definition provided in the Processing Convention.

Governmental privacy is also the subject of separate measures under Turkish law. Breach of government privacy is set out under the 'crimes against the government' section of

the TPC. Pursuant to Article 258, any public officer who discloses or publicises confidential documents, decisions and orders and other notifications delivered to him or her by virtue of office, or facilitates access to such information and documents by third parties, will be punished with imprisonment for a period from one to four years.

The privacy of corporations and business secrets, on the other hand, are protected under the 'crimes related to the economy, industry and trade' section of the TPC. Pursuant to Article 239, any person who passes on information or documents that he or she holds by virtue of office, or discloses business secrets, banking secrets or customer secrets to unauthorised persons, shall be sentenced to imprisonment for a period from one to three years and also subject to a punitive fine,[2] upon complaint. Turkish judicial authorities make a distinction between trade secrets and personal information.[3]

Therefore, Turkish law regulates personal data, government information and business information separately, and Turkish judicial authorities confirm this separation in their precedents.

Under Turkish law, freedom of expression is a highly debated issue, and this is also stated in the international evaluation reports regarding Turkey.[4] The definition of privacy is too broad and the concept of 'personal data' is not yet well established. Therefore, Turkish authorities tend to vote in favour of privacy and personal data, and free speech is what is left after all the sensitivities are ironed out.

As highlighted by a Turkish High Court decision, judicial authorities must be even more careful while applying the limitation to fundamental rights and freedoms.[5] Moreover, the European Court of Human Rights clearly highlights that freedom of expression 'constitutes one of the essential foundations of a democratic society and one of the basic conditions for its progress and each individual's self-fulfilment'.[6] Article 13 of the Constitution[7] provides the principle of proportionality. Therefore, there must be a logical bond between the precautions

2 The TPC provides that a punitive fine will be payable to the State Treasury that is calculated by multiplying the duration of the offence – up to 5,000 days – by an amount to be decided by the judge. The amount for each day should be between 20 and 100 liras.

3 Decision of Criminal Department No. 12 of the Turkish Supreme Court of 10 June 2013 No. 2013/15772 states that 'information regarding real persons should be defined as "personal data", whereas financial information and programs of a corporation cannot be accepted as personal data'.

4 For Freedom House's evaluations, see freedomhouse.org/report/freedom-press/2016/turkey; for United Nations evaluations, see www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=17172&LangID=E; and for the EU's 2015 progress report on Turkey, see ec.europa.eu/enlargement/pdf/key_documents/2015/20151110_report_turkey.pdf.

5 Decision of the General Criminal Assembly of the Supreme Court of 11 July 2006, File No. 2006/9-169, Decision No. 2006/184.

6 *Vogt v. Germany*, ECHR (1996) 21 EHRR 205, (17851/91).

7 Article 13 of the Constitution: 'Fundamental rights and freedom may be limited without interfering with their nature and only for the reasons stated in relevant articles of the Constitution and only by the Law. These limitations may not be contrary to the wording and spirit of the Constitution, to the requirements of the democratic public order and the secular Republic and to the principle of proportionality.'

taken that limit fundamental rights such as freedom of speech and freedom and the intended purpose of the precaution and the tools used to achieve it to give the minimum harm to the fundamental rights and freedom subject to limitation.

NGOs have an important role in collecting public opinion and monitoring regulations. Although there are a significant number of NGOs operating in the data protection and cybersecurity area, they still do not have much effect on the regulatory bodies. The Turkish Industrialists' and Businessmen's Association played an active role during the legislative process of the DP Law by way of contributing to legislative meetings and drafting proposals.

II THE YEAR IN REVIEW

2016 is expected to be the year for the regulation of data protection measures in Turkey. The DP Law, which is based on the EU Data Protection Directive, recently entered into force on 7 April 2016.

The DP Law was first introduced to the Turkish Grand National Assembly by the government in April 2003 as a part of Turkey's Accession Partnership Document signed between the Council of Europe and Turkey. The Data Protection Law has been mentioned various times by several members of the Cabinet as a law 'soon to be ratified' between 2008 and 2016.

The current version of the DP Law is more compatible with the EU Data Protection Directive than its previous versions. That said, the DP Law still differs from the EU data protection regime at certain points. Moreover, the DP Law may need to be amended following the adoption of the General Data Protection Regulation for full harmonisation, since the Law is prepared based on the EU Data Protection Directive.

The DP Law aims to protect the fundamental rights and freedoms of people with respect to the processing of personal data, particularly privacy of private life, and to regulate the procedures and principles along with obligations to be followed by real persons and legal entities that are processing personal data. The DP Law is applicable to real persons whose data is processed, and to real persons or legal entities that process personal data.

The secondary legislation relating to the implementation of the DP Law will enter into force within one year following the publication of the Law (i.e., within one year after 7 April 2016).

III REGULATORY FRAMEWORK

i Privacy and data protection legislation and standards

Key definitions

Personal data

Under the DP Law, personal data means any information relating to an identified or identifiable real person. There are two types of data regulated under the DP Law: 'personal data' and 'special categories of personal data'. Data concerning racial or ethnic origin, political opinions, philosophical beliefs, religion, sect or other beliefs, appearance and clothing, association, foundation or trade-union membership, health or sex life, and criminal conviction and security measures regarding a person, along with their biometric and genetic information, are special categories of personal data.

Processing
The DP Law states that the processing of personal data means any operation performed on personal data, wholly or partly, whether through automatic means, or if the data is part of a data filing system, through non-automatic means, such as collection, recording, storage, preservation, alteration, retrieval, disclosure, transfer, acquisition, making available, categorising or blocking.

Anonymising
As per the DP Law, anonymisation means rendering personal data anonymous in such a way that it cannot be related to an identified or identifiable real person even through linking that data to another data.

The term 'anonymising' is described under Article 1 of the Regulation on Data Protection in the Electronic Communications Sector as processing data in a way that they cannot be associated with any real person or legal entity who is identified or identifiable, or in a way that prevents the identification of the source.

Key legislation
There are certain provisions under various laws with respect to privacy and data protection, and sector-specific regulations. The legislative framework for the protection of data or personally identifiable information in Turkey may be defined under four main legislative prongs:

a rights on personal data under public law rules;
b rights on personal data under private law rules;
c rights on personal data under criminal rules; and
d rights under the DP Law.

Public law
Rights on personal data under public law rules are stipulated under the Constitution. The applicable legislation is Section V of the Constitution titled 'Privacy and the Protection of Private Life', and in particular Article 20 of the Constitution, which regulates the act of processing and states that personal data may only be processed in cases where it is stipulated by law or with the owner's explicit consent.

Private law
Rights on personal data under private law rules are regulated in the TCC. The TCC includes provisions[8] regulating protection of personal rights in general. The TCC does not provide either a comprehensive or *numerus clausus* list in respect of personal rights, leaving the matter to the discretion of the judge. 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 the judicial precedents, the 12th Chamber of the Council of State defined personal data[9] as 'any information that belongs to an identified person or any information that directly or indirectly leads to identification of a person, especially with

8 Article 23 et seq.

9 Decision No. 2005/6811E and Decision No. 2006/1959K, of 15 May 2006.

respect to any ID number or physical, psychological, intellectual, economic, cultural or social status'. The relevant jurisprudence and scholarly writings highlight the will of the data subject, namely whether the data subject considers the collected data personal or not. Hence, collecting, publishing and communicating personal data without the prior consent of such a person would constitute a violation against personal rights under the TCC.

Rights on personal data under criminal rules are regulated in the TPC, and it adopts a definition of 'personal data' that does not fall far from the definition provided in the Processing Convention.

The Constitutional Court states that 'personal data' means all the information related to a person, if the person or his or her identity is identifiable through such information – such as given name, surname, birth date, birthplace, telephone number, licence plate number, social security number, passport number, curriculum vitae, images, visuals and recordings related to the person, his or her fingerprints, genetic information, IP address, e-mail address, hobbies, preferences, associates, affiliates, group memberships or family members. Apparently, personal data has a broad scope, and any information that makes a person identifiable is considered personal data.

Criminal law

Breaches of data protection may lead to criminal penalties. Rights on personal data under criminal rules are stipulated in Section 9 (Crimes against Private Life and Privacy) of the TPC. Section 9 provides that any person unjustly recording personal data, unjustly acquiring or disseminating personal data or giving personal data to somebody else, unlawfully transferring personal data or failing to destroy any personal data after the waiting periods set forth in law have been passed shall be liable for criminal prosecution.

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 consequences for both the legal entity and its managers.

The DP Law

The DP Law, which will be explained in detail below, is based on the EU Data Protection Directive, although it differs from the Directive in certain aspects.

Sector-specific regulations

There are also sector-specific regulations. With respect to the telecommunications sector, the Information and Communication Technologies Authority (ICTA) supervises the rights of subscribers, users, consumers and end users, as well as the processing of personal data and privacy protection in the telecoms sector. The above-mentioned duties and authorities of the ICTA are regulated under the Electronic Communications Law (ECL) and its secondary regulations. The ICTA, considering factors such as the requirements of the sector, international regulations and technological developments, is entitled to impose obligations on operators to protect personal data and privacy.

The Regulation on Data Protection in the Electronic Communications Sector, which is based on the ECL, sets forth certain protective measures for the personal information of subscribers or users of electronic communication services, such as traffic data required for marketing of electronic communication services and providing value-added electronic communication services, may be processed only by anonymising the data or obtaining the consents of subscribers or users after they are properly informed, and such processing may

only be performed in accordance with the consent obtained from the user or subscriber and in the amount and for the time required by the electronic communication services, marketing activities and similar services.

Location data and the identity of the relevant persons may only be processed in the absence of consent by the subscriber or user in the event of a disaster, a state of emergency or an emergency call, other than in the cases designated under relevant legislation and judicial decisions.

The traffic data processed and stored shall be deleted or anonymised after the completion of the activity required for the processing and storage in the first place.

ii General obligations for data handlers

A data controller, or any person authorised by the data controller, is obliged to provide the relevant data subjects with information. The data subject should be informed during the collection of the personal data.

The data controller, or any person authorised by the data controller, is obliged to provide the data subjects with the following information:

a the identity of the data controller, and of his or her representative (if any);
b the purposes of the processing;
c to whom and for what purpose the processed personal data can be transferred;
d the method and legal ground of the collection; and
e the data subjects' rights.

Pursuant to the Regulation on Processing and Protection of Privacy of Personal Data in the Electronic Communications Sector, operators providing electronic communications also have certain obligations to inform subscribers and users.

iii Technological innovation and privacy law

Pursuant to the Electronic Communications Data Protection Regulation, personal data cannot, in principle, be transferred abroad (although Article 51 of the ECL allows the transfer of traffic and location data abroad under certain conditions). This provision may affect the development of information technologies such as cloud computing (see Section IV, *infra*).

iv Specific regulatory areas

Employment

There are no specific laws governing the processing of personal data in employment relationships. However, there is a particular provision imposing certain obligations on employers with respect to their employees' personal information. Pursuant to Article 75 of the Turkish Labour Law, employers are obliged to keep personnel files on their employees, but are obliged to use this information in good faith and in accordance with the law.

Health

As per Article 78 of the Law on Social Security and General Health Insurance, in principle, the health information of an insured person and the ones he or she is obliged to look after are confidential. The Medical Deontology By-law and the Patient Rights Regulation stipulate that information obtained during medical procedures cannot be disclosed unless required by law.

Finance

Article 73 of the Banking Law stipulates that personal information must not be disclosed by banks or persons who have 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, the Banking Law also entitles the Banking Regulation and Supervision Agency to audit banks and request any information (including that classified as confidential). The banks, their subsidiaries, associations, branches, representative offices and outsourcing institutions, as well as any other natural or legal persons related to those banks, are obliged to provide any and all necessary systems, passwords, documents, records and information upon such request. Under the Bank Cards and Credit Cards Law, member enterprises cannot disclose, keep or copy the information they acquired from consumers without their consent, except for requests by authorised authorities. Member enterprises cannot share, sell, buy or trade such information, and may only do so with the affiliated bank card issuer.

Telecommunications

The ECL is the primary law applicable to telecommunications and telecoms companies. The Regulation on Processing and Protection of Privacy of Personal Data in the Electronic Communications Sector, which is based on the ECL, sets out the procedures and principles to be followed by operators (i.e., any legal entity authorised to provide electronic communications services or to provide electronic communications network and to operate the infrastructure) active in the electronic communications sector with respect to the processing and the retention of personal data and the protection of privacy in the electronic communications sector.

Historical, statistical and scientific research purposes

The DP Law provides an exception for personal data processed for scientific and statistical purposes. In particular, if personal data are processed for the purposes of research, planning or statistical operations after being anonymised as official statistics, the Law will not apply. Moreover, if personal data are processed for artistic, historical, literary or scientific purposes or within the scope of freedom of speech, and provided that national defence, national security, public safety, public order, economic safety, privacy of private life or personal rights are not violated, and the processing does not constitute a crime, the Law will not apply either. The Regulation on Data Privacy and Principles and Procedures Regarding Security of Confidential Data in the Official Statistics sets out the principles and procedures with respect to data privacy and the maintenance of security of confidential information in official statistics.

IV INTERNATIONAL DATA TRANSFER

The DP Law regulates the transfer of personal data abroad. In principle, personal data cannot be transferred abroad without the explicit consent of a data subject, except in specific circumstances.

The exceptions under which personal data can be transferred abroad without the explicit consent of a data subject are if the country to which the personal data is to be transferred provides an adequate level of protection; or, if the protection is not adequate

in such country, the data controllers in Turkey and in such country may provide a written undertaking guaranteeing an adequate level of protection, which should be authorised by the Data Protection Board (Board).

The Board determines which countries have an adequate level of protection and announces them publicly. The Board determines whether a foreign country can afford an adequate level of protection, and whether data transfers will be authorised after consulting with the relevant public administrations and agencies (if necessary), by evaluating:

a the international agreements to which Turkey is a party;

b the reciprocity in place relating to data transfers between Turkey and the country where the personal data will be transferred;

c the category of the personal data, as well as the purpose and period of processing for each specific data transfer;

d the relevant legislation and practice in the foreign country to which the data will be transferred; and

e the measures that the controller in the foreign country to which the data will be transferred commits to provide.

Without prejudice to the provisions of international treaties, if the interests of Turkey or a data subject will be seriously undermined, personal data may only be transferred abroad upon the authorisation of the Board, having ascertained the relevant public institution's or authority's opinion.

In accordance with the Regulation on Data Protection in the Electronic Communications Sector, personal data cannot, in principle, be transferred abroad (although Article 51 of the ECL allows the transfer of traffic and location data abroad under certain conditions). This provision may have certain side effects on the development of information technologies. As an example, this provision may constitute an obstacle to the use of cloud computing services, which sometimes require the transfer of personal data abroad. Further, this provision might affect the free flow of data within or between multinational companies. Although the ICTA states that Article 51 is merely intended to ban the transfer of data abroad for commercial purposes, its wording does not include this provision.

On the other hand, traffic and location data may be transferred abroad, provided that the data subject explicitly consents to such a transfer, according to the recently enacted Article 51 of the ECL, which constitutes the basis of the foregoing regulation.

V COMPANY POLICIES AND PRACTICES

In principle, personal data may not be disclosed to a third party without the explicit consent of the data subject. According to the DP Law, a data controller is obliged to take the appropriate technical and administrative measures to protect the personal data. There are currently no specific technical requirements described under the Law. However, the International Organization for Standardization (ISO) already has a set of standards with respect to technical data security measures entitled ISO/IEC 27000, although it is not clear whether these ISO standards are sufficient to comply with the information security requirement set forth under the Law.

The breach notification obligation is incumbent on data controllers, data processors and operators. In the event that processed personal data is unlawfully obtained by others, the data controller shall notify the issue to the data subject and the Board. If necessary, the Board may announce the issue on its own website or via any other means it deems appropriate.

The Regulation on Processing and Protection of Privacy of Personal Data in the Electronic Communications Sector obliges operators to effectively inform their subscribers and users of risks violating the security of personal data and the network, or of the existing violations of personal data protection, or both, provided that the ICTA and the Board deem it necessary.

VI DISCOVERY AND DISCLOSURE

The Electronic Communications Data Protection Regulation sets out the period for which personal information may be stored. In accordance with the Electronic Communications Data Protection Regulation, personal data that is subject to investigations, evaluations, inspections or disputes shall be stored until the relevant process is concluded. In any case, records regarding the accessing of personal data and relevant systems shall be stored for four years.

VII PUBLIC AND PRIVATE ENFORCEMENT

i Enforcement agencies

Currently, there is no specific data protection authority in Turkey. However, the DP Law stipulates the establishment of a supervisory authority, called the Personal Data Protection Authority, which has the authority to supervise the compliance of data processing systems with the Law. Moreover, the ICTA is entitled to supervise and audit data protection breaches in electronic communications services.

VIII CONSIDERATIONS FOR FOREIGN ORGANISATIONS

A major compliance issue for organisations based or operating outside Turkey was the absence of a specific data protection law in Turkey. This compliance issue is particularly acute for organisations in EU Member States, as the EU Data Protection Directive states that personal data may only be transferred to countries outside the EU and the European Economic Area if an adequate level of protection is guaranteed in the relevant country. In this respect, Turkey would be considered to have an adequate level of protection for personal data, and transfer of personal data to Turkey would not therefore be problematic.

There is no specific regulation forcing localisation requirements for data servers or cloud computing, human resources and internal investigations in terms of data protection unless the service of relevant multinational organisations falls within the scope of electronic communications service under the ECL. If this were the case, and such companies were to provide electronic communications services, the major issue for these multinational organisations would be transferring personal data outside Turkey, as this is currently forbidden in the electronic communications sector in Turkey.

IX CYBERSECURITY AND DATA BREACHES

Turkey is a signatory to the Council of Europe's Convention on Cybercrime, and ratified and adopted the Convention in 2014.

Cybersecurity provisions for electronic communications services are more detailed than general data security provisions. Technical, administrative, organisational and physical safeguards are regulated under the Regulation on Security of Electronic Communications.

On the other hand, Turkey is still far beyond satisfying the EU cybersecurity legislation, as cybersecurity measures under Turkish law are still being regulated under secondary legislation. The Turkish cybersecurity regime needs a law to cover the basic principles of cybersecurity, and the secondary legislation should be updated to reflect technological developments and new threats to cybersecurity.

As regards data breaches, since January 2014, operators have been obliged to inform the ICTA in the event of a network security and personal data violation risk, and should the ICTA deem it necessary, operators must also inform their subscribers or users about this risk in an effective and prompt manner. The ICTA also has the right to request from operators all the information and documents concerning the systems in which personal data are kept and the security measures taken by the operators to protect that data. The ICTA may then request changes to the security measures. The Regulation on Data Protection in the Electronic Communications Sector has not set out the circumstances in which the ICTA may find informing users to be 'necessary'; therefore, this provision is criticised for granting such broad discretion and power to the ICTA.

X OUTLOOK

Turkey enacted the Processing Convention and the DP Law in accordance with the EU data protection measures, and harmonisation of data protection and cybersecurity matters should be expected to be more feasible. Considering the borderless nature of technology and threats to cybersecurity, international cooperation is essential, and such cooperation can only be maintained by the harmonisation of regulations. It is clear that Turkey welcomes new data protection measures and practices, and at the same time offers great potential for user penetration and an increasing thirst for technology consumption.

Appendix 1

ABOUT THE AUTHORS

GÖNENÇ GÜRKAYNAK

ELIG, Attorneys-at-Law

Gönenç Gürkaynak is the managing partner and a founding partner of ELIG, Attorneys-at-Law, a leading law firm of 70 lawyers in Istanbul, Turkey. He holds an LLM from Harvard Law School, and is qualified to practise in Istanbul, New York, Brussels, and England and Wales. Before joining ELIG, Attorneys-at-Law, Mr Gürkaynak worked as an attorney at the Istanbul, New York and Brussels offices of a global law firm for more than eight years. He also holds a teaching position at undergraduate and graduate levels at two universities in the fields of law and economics, competition law and Anglo-American law, and he frequently gives lectures and speeches in numerous universities and academic platforms on internet law, freedom-of-speech issues and anti-corruption law. He has had more than 100 articles published, internationally and locally, in English and Turkish, and two books, one published by the Turkish Competition Authority, and the other, *Fundamental Concepts of Anglo-American Law*, published by Legal Publishing.

İLAY YILMAZ

ELIG, Attorneys-at-Law

İlay Yılmaz is a partner at ELIG, Attorneys-at-Law in Istanbul, Turkey. She graduated from Dokuz Eylül University's Faculty of Law in 2003 and is admitted to the Istanbul Bar. She holds an LLM degree from Istanbul Bilgi University. She has represented various multinational and national companies before the Turkish authorities. İlay Yılmaz's practice focuses on IT and telecoms, media and entertainment, internet, data protection, contracts, energy market and general corporate law. She has authored and co-authored numerous articles and essays pertaining to these practice areas, in addition to speaking at conferences and symposia on similar matters. İlay Yılmaz is fluent in English.

ELIG, ATTORNEYS-AT-LAW
Çitlenbik Sokak No. 12
Yıldız Mahallesi
Beşiktaş
34349 Istanbul
Turkey
Tel: +90 212 327 17 24
Fax: +90 212 327 17 25
gonenc.gurkaynak@elig.com
ilay.yilmaz@elig.com
www.elig.com