The Privacy, Data Protection and Cybersecurity Law Review

Second Edition

Editor
Alan Charles Raul

Law Business Research

The Privacy, Data Protection and Cybersecurity Law Review

The Privacy, Data Protection and Cybersecurity Law Review
Reproduced with permission from Law Business Research Ltd.

This article was first published in The Privacy, Data Protection and Cybersecurity Law Review - Edition 2
(published in November 2015 – editor Alan Charles Raul)

For further information please email
Nick.Barette@lbresearch.com

The Privacy, Data Protection and Cybersecurity Law Review

Second Edition

Editor

Alan Charles Raul

Law Business Research Ltd

PUBLISHER
Gideon Roberton

SENIOR BUSINESS DEVELOPMENT MANAGER
Nick Barette

SENIOR ACCOUNT MANAGERS
Katherine Jablonowska, Thomas Lee, Felicity Bown, Joel Woods

ACCOUNT MANAGER
Jessica Parsons

PUBLISHING MANAGER
Lucy Brewer

MARKETING ASSISTANT
Rebecca Mogridge

EDITORIAL ASSISTANT
Sophie Arkell

HEAD OF PRODUCTION
Adam Myers

PRODUCTION EDITOR
Robbie Kelly

SUBEDITOR
Gina Mete

MANAGING DIRECTOR
Richard Davey

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

www.TheLawReviews.co.uk

ISBN 978-1-909830-75-2

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 INTERNATIONAL 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

www.TheLawReviews.co.uk

ACKNOWLEDGEMENTS

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

ADVOKATFIRMAET SIMONSEN VOGT WIIG AS

ALLENS

ASTREA

BOGSCH & PARTNERS LAW FIRM

CMS CAMERON MCKENNA GRESZTA I SAWICKI SP.K.

DUNAUD CLARENC COMBLES & ASSOCIÉS

ELIG, ATTORNEYS-AT-LAW

JUN HE LAW OFFICES

LEE & KO

MATHESON

MATTOS FILHO, VEIGA FILHO, MARREY JR E QUIROGA ADVOGADOS

NNOVATION LLP

PEARL COHEN ZEDEK LATZER BARATZ

SANTAMARINA Y STETA, SC

SIDLEY AUSTIN LLP

SUBRAMANIAM & ASSOCIATES

URÍA MENÉNDEZ ABOGADOS, SLP

VIEIRA DE ALMEIDA & ASSOCIADOS, RL

WALDER WYSS LTD

WINHELLER RECHTSANWALTSGESELLSCHAFT MBH

CONTENTS

Chapter 25

TURKEY

Gönenç Gürkaynak and İlay Yılmaz[1]

I OVERVIEW

As of 2015, Turkey does not currently have a dedicated and specific data protection law in force, but there is draft legislation that has been awaiting ratification since 2003, entitled the Draft Law on the Protection of Personal Data (the Draft Law). The Draft law is drawn up in accordance with the EU approach to data protection. On the other hand, 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. The Draft Law was eventually submitted to the Turkish Grand National Assembly (TGNA) on 26 December 2014 .

Moreover, Turkey is one of the signatories of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (the Processing Convention) of 1981. On 1 August 2014, the Processing Convention was submitted to the TGNA and is currently awaiting ratification.

Along with a draft law on the regulation of the general principles of data protection, there are certain sector-specific regulations.

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, and which 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.

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

Privacy and data protection are treated as coextensive concepts in the Draft 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 Draft Law has been in train since 2007 and is pending before the TGNA. Moreover, the Processing Convention has been awaiting approval and was brought before the TGNA very recently, in August 2014. Therefore, while the implementation process for data protection policy in Turkey remained very slow for a long time, the beginning of 2015 saw a significant acceleration in this area. However, given that there are still to be parliamentary elections in 2015, we do not expect ratification of the Draft Law before 2016.

The right to privacy and protection of an individual's private life is enshrined in the Turkish Constitution of 1982. 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 Turkish Civil Code (TCC). Articles 23 et seq. of the TCC include 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 the 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 from one to four years.

The privacy of corporations and business secrets, on the other hand, are protected under '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 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]

2 The TPC provides that a punitive fine will be payable to the state Treasury and 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

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 Turkish Constitution[7] provides the principle of proportionality. Therefore, there must be a logical bond between the precautions 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.

II THE YEAR IN REVIEW

The notable recent developments pertaining to data protection are the introduction of the new Article 51 of Law No. 5809 (the previous version of the Article was annulled

---

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: http://freedomhouse.org/country/turkey?gclid=CjwKEAjwkMWgBRCJ1L_wypbX0wkSJAC3Xio2aBFjuFTFBu9_pjSrQYeaeta3ksxFK6zddIF1rjxKcBoCV4Lw_wcB#.VBGhpMJ_tcR; for European Commission evaluations see: http://ec.europa.eu/enlargement/pdf/key_documents/2013/wbt_media_study.pdf; and for the EU's 2013 progress report on Turkey, see: http://ec.europa.eu/enlargement/pdf/key_documents/2013/package/brochures/turkey_2013.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.

by the Constitutional Court) covering data protection in the electronic communications sector, and enactment of the E-Commerce Law and the secondary legislation of the E-Commerce Law regarding electronic commercial communications.

The enactment of Article 51 of Law No. 5809 on Electronic Communications (the ECL) was a significant development in 2015. Article 51 regulates the principles and procedures for processing and protecting privacy of personal data in the electronic communications sector (including a provision imposing an obligation on electronic communication service providers to keep data in Turkey), and was previously annulled by Turkish Constitutional Court decision No. 2014/74 of 9 April 2014. The annulment decision was rendered following the Turkish Council of State's application to the Constitutional Court. The Constitutional Court stated in its reasoned decision that 'Pursuant to inalienability of legislative power, authorisation of rule-making cannot be directly and at first hand transferred on the matters that are explicitly stated in the Constitution. The provision which delegates the power to regulate the principles and procedures on processing and protection of privacy of personal data in the electronic communications sector to the authority which is also the subject of the case is against Article 20 of the Constitution.' The Constitutional Court clearly emphasised that protection of personal data may only be regulated by a law, and not by a regulation or other secondary legislation issued by the public authorities. The Constitutional Court's decision became effective as of 26 January 2015 and Article 51 of Law No. 5809 was annulled accordingly.

The new Article 51 of Law No. 5809 replaced the annulled article and is drafted in a way to comply with the Constitutional Court's decision and the requirements of the Turkish Constitution. The framework for processing personal data in the electronic communication sector might be established through this Article and it does not appear to result in arbitrary implications being drawn by the administration.

The amendment entered into force retroactively, as of 26 January 2015, which was the date that the Constitutional Court's decision on the annulment of the previous version of the Article became effective.

Another significant development for 2015 was the enactment of Law No. 6563 on the Regulation of Electronic Commerce (the E-Commerce Law), which was published in the Official Gazette on 5 November 2014. The E-Commerce Law aims to regulate procedures and principles regarding electronic commerce and became effective on 1 May 2015. The E-Commerce Law actually focuses on (1) the obligation to provide information regarding contracts that are entered into via electronic means, and the liabilities and obligations of online service providers; and (2) unsolicited commercial electronic marketing. The E-Commerce Law and its secondary legislation includes certain data protection obligations for electronic communication service providers and intermediaries.

The secondary legislation of the E-Commerce Law, namely the Regulation on Commercial Communication and Commercial Electronic Communications (the Regulation) entered into force on 15 July 2015. Article 12 of the Regulation states that service providers and intermediary service providers are responsible for the protection of personal data and should take necessary steps to prevent the unlawful use of personal data. Data owners' consent should be obtained to share the personal data with third parties, process or use the data for other purposes.

III REGULATORY FRAMEWORK

i Privacy and data protection legislation and standards

Key definitions

Personal data

Under Turkish law, all information relating to identified or identifiable natural persons or legal entities may be deemed personal data. There are two types of data regulated under the Draft Law: 'personal data' and 'special categories of personal data'. Personal data is defined as any information pertaining to identified or identifiable persons (including both natural persons and legal entities). In contrast, special categories of personal data are data regarding a person's race, political opinion, philosophical belief, religion, sect or other beliefs, association, foundation and trade union membership, health, private life and any type of conviction.

Processing

The Draft Law covers all kinds of personal data 'processing', which is defined as a transaction or group of transactions on the data, such as acquisition of personal data, recording, storing, modifying, deleting or destroying, rearrangement of personal data or making it available through other means, transferring to third parties, marking to limit its use or classifying or preventing use of personal data.

On the other hand, the general provisions that are currently in effect and applicable to data protection do not distinguish between the types of acts related to data processing, although the TPC does provide that some types of processing are criminal acts.

Anonymising

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 of preventing 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: (1) rights on personal data under public law rules; (2) rights on personal data under private law rules; (3) rights on personal data under criminal rules and (4) rights under the Draft Data Protection Law.

Public law

Rights on personal data under public law rules are stipulated under the Turkish Constitution of 1982. The applicable legislation is Section V of the Turkish Constitution titled 'Privacy and the Protection of Private Life' and in particular Article 20 of the

Turkish 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 Turkish Civil Code. TCC includes provisions[8] regulating protection of personal rights in general. The Turkish Civil Code does not provide either a comprehensive or *numerus clausus* list in respect of personal rights and leaves 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 Turkish Civil Code 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 respect to any ID number or physical, psychological, intellectual, economic, cultural or social status'. The relevant jurisprudence and the 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 Turkish Civil Code.

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, birthdate, birthplace, phone number, licence plate number, social security number, passport number, CV, images, visuals and recordings related to the person, his or her fingerprints, genetic information, IP address, email 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.

The Constitutional Court also categorises personal data – as 'sensitive data' and 'non-sensitive data'. These phrases are not used under the applicable legislation. The Constitutional Court considers that all of a person's health information, including all records regarding physical and mental health, as well as data related to that person's race, political views, philosophical thought, religion, sect or other beliefs, memberships of associations and unions, private life and any convictions, as 'sensitive data'. The decision states that this type of data requires a higher level of protection. Identification and residence information and information as to diagnoses, medical examinations and medical treatment are also included within the sensitive data category.

8 Article 23 et seq.

9 Decision Nos. 2005/6811E and 2006/1959K, dated 15 May 2006.

In another Constitutional Court decision, the reasoning of a dissenting vote of a member of the Court states that information as to a person's alcohol or drug addiction is also deemed sensitive data, by referring to EU Directive 95/46/EC.

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. The Section 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 Draft Data Protection Law

The Draft Data Protection Law is based on the Processing Convention and the European Data Protection Directive (1995/46/EC). It is expected that the Draft Data Protection Law will soon be enacted, since it has been included in the government's short-term action plan.

Sector-specific regulations

There are also sector-specific regulations. With respect to the telecommunications sector, the 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 ECL and its secondary regulations. The ICTA, considering the factors such as 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 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 permission given to the operator by the subscriber or user also involves the processing of personal data by parties that are authorised by the operator. The process should be carried out within the purposes of the service provided to the subscriber or

user. If a third party is authorised by the operator to process the personal data of the user or subscriber, the operator is liable for ensuring the personal data's privacy, security and compliance of the data use with the purpose of the service, including any violation of the Regulation on Data Protection in the Electronic Communications Sector by the third parties.

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.

The Regulation on Data Protection in the Electronic Communications Sector also sets out the permitted storage periods for personal information collected during electronic communication services. In accordance with Article 14 of the Regulation on Data Protection in the Electronic Communications Sector, personal data that is subject to investigations, evaluations, inspections or disputes shall be stored until the relevant processes are concluded. In any case, records regarding the accessing of personal data and relevant systems shall be stored for four years.

ii General obligations for data handlers

According to the Draft Law, the following information should be provided to data subjects by the owner of the data file or the data controller when obtaining personal data:

a the identity of the controller and of his or her representative, if any;
b the purposes of the processing;
c to whom and with what purpose the personal data can be transferred;
d the method and legal reason for collection; and
e other rights of the data subject referred to in Article 10.

The data controller must also inform the data subject when the personal data are erased, destroyed or anonymised.

The 'data subject' is defined as the natural person whose personal data is processed under the Draft Law. The Draft Law provides exceptions to certain of its provisions under certain circumstances. According to the Draft Law, the data subject's consent is not required and the notification and registration obligations do not apply in the following situations:

a where personal data is processed by a natural person in the course of a purely personal or household activity;
b where personal data is processed for purposes of research, planning or statistical operations after being anonymised;
c where personal data is processed within the framework of freedom of press and in line with the general principles set forth in this Law, the general measures relating to data security and professional codes of conduct;
d where personal data is processed within the framework of the provisions relating to intellectual activities laid down in the Law on the Duties and Powers of the Police; Law on the Organisation, Duties and Powers of the Gendarmerie; and Law on the State Intelligence Services and National Intelligence Organisation; and
e personal data is processed for the purposes of making financial research, collecting data, receiving, analysing, evaluating, studying and sharing with related institutions

notifications relating to suspicious transactions and other notifications within the framework of the Law on the Prevention of the Laundering of Crime Revenues, and the Law on the Prevention of the Financing of Terrorism.

Pursuant to the Draft Law, natural or legal persons processing personal data must register with the Data File Registry before commencing processing.

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 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 is a particular provision imposing certain obligations on the 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

The Regulation on Security and Sharing of General Health Insurance Data sets out the principles and procedures regarding the protection and sharing of health data stored in the databases of the Social Security Authority and contracted health service providers.

Also, 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 and 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 to 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, are obliged to provide any and all necessary systems, passwords, documents, records and information upon such a request.

Under the Bank Cards and Credit Cards Law, enterprises cannot disclose, keep or copy the information they acquired from consumers without their consent, except for requests by authorised authorities. 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 the 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 Draft Law provides an exception for personal data processed for research, planning or statistical purposes. Personal data are processed for research, planning and statistical operations after being anonymised. Such anonymised data and the results may be transferred to third parties or published without being subject to the restrictions under the Draft Law.

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

Turkey does not have a particular regulation in effect with respect to international data transfers. Pursuant to the Draft Law, personal data cannot be transferred to third persons or to a foreign country, in principle.

According to the Draft Law, personal data may be transferred abroad without the data subject's consent, provided that the foreign country provides equivalent and effective protection with respect to personal rights. If there is no equivalent or effective protection in the foreign country, personal data may nonetheless be transferred to such a country if:

a the data subject provides explicit consent;

b the controllers in Turkey and in the foreign country to which the data are to be transferred provide a written commitment about adequate protection and that the ICTA gives its authorisation.

However, a significant amendment made by the Regulation on Data Protection in the Electronic Communications Sector in 2013 concerns the transfer of personal information abroad. 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 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 transfer of personal data abroad. Further, this provision might affect the free flow of data of within

or between multinational companies. Although the ICTA states that this article is merely intended to ban the transfer of data abroad for commercial purposes, the wording of the article 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

There are no specific policies and practices that an organisation that processes personal information is required to comply with under Turkish law. However, pursuant to Supreme Court decisions, personal data must:

a be processed in accordance with the law and rules of honesty;
b be processed based on the consent of the respective person;
c fit the purpose for the collection of the data and be sufficient and proportionate to that purpose;
d be accurate and updated when necessary; and
e be stored in a manner indicating the identities of the respective persons, and stored as long as it is necessary for the purpose of its reprocessing.

Therefore individuals whose personal rights are violated because of a data protection breach have the right to claim damages or to make complaints.

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

In Turkey there is no data protection or privacy authority for enforcement. However, the ICTA is entitled to supervise and audit data protection breaches in electronic communications services.

ii Recent enforcement cases

In 2013, the ICTA declared that it was investigating operators regarding the recording of data obtained while providing electronic communications services. In 2011, the ICTA in its decision of 11 December fined TTNet AS – one of the major ISPs in Turkey – 975,336 liras for not taking necessary measures for the protection of subscribers' data.

Turkcell Iletisim Hizmetleri AS, a Turkish GSM operator, was fined 11.22 million liras by ICTA in its decision of 19 April 2011, on the grounds that an employee of the company shared billing details with third parties. Another GSM operator, Vodafone Telekomunikasyon AS, was also fined 1.27 million liras, which was 0.05 per cent of the firm's 2009 net sales. The fine was imposed by the Presidency in its February 2011 decision regarding a security loophole in the 'My Vodafone' service, which enabled the billing details of subscribers to be seen.

VIII CONSIDERATIONS FOR FOREIGN ORGANISATIONS

A major compliance issue for organisations based or operating outside Turkey is 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 does not have an adequate level of protection for personal data, and transfer of personal data to Turkey is therefore 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, the 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 the operators all the information and documents concerning the systems in which personal data is 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

In light of the Constitutional Court's significant decision of 2014 regarding data protection regulations in Turkey and the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, which has been sent to the TGNA for ratification, it appears that the near future will bring new regulations on data protection. Moreover, as mentioned above, Turkish data protection laws are based on EU legislation. Therefore, it is likely the new EU General Data Protection Regulation will affect the Turkish data protection regime as well.

If Turkey enacts the Processing Convention and the Draft Law, in accordance with the EU data protection measures, harmonisation on data protection and cybersecurity matters would be more feasible. Considering the borderless nature of technology and threats to cybersecurity, international cooperation is essential and such cooperation can only maintained by the harmonisation of regulations.

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 60 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 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 34349
Beşiktaş, 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