Cybersecurity

Contributing editors
Benjamin A Powell and Jason C Chipman

2019

GETTING THE DEAL THROUGH

GETTING THE DEAL THROUGH

Cybersecurity 2019

Contributing editors

Benjamin A Powell and Jason C Chipman

Wilmer Cutler Pickering Hale and Dorr LLP

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

Publisher
Tom Barnes
tom.barnes@lbresearch.com

Subscriptions
Claire Bagnall
claire.bagnall@lbresearch.com

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

Dan White
dan.white@gettingthedealthrough.com

Law Business Research

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

First published 2015
Fifth edition
ISBN 978-1-912228-87-4

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

CONTENTS

Preface

Cybersecurity 2019

Fifth edition

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

Getting the Deal Through provides international expert analysis in key areas of law, practice and regulation for corporate counsel, cross-border legal practitioners, and company directors and officers.

Throughout this edition, and following the unique **Getting the Deal Through** format, the same key questions are answered by leading practitioners in each of the jurisdictions featured. Our coverage this year includes new chapters on Denmark, Poland, Singapore and a new article on human rights and cybersecurity.

Getting the Deal Through titles are published annually in print. Please ensure you are referring to the latest edition or to the online version at www.gettingthedealthrough.com.

Every effort has been made to cover all matters of concern to readers. However, specific legal advice should always be sought from experienced local advisers.

Getting the Deal Through gratefully acknowledges the efforts of all the contributors to this volume, who were chosen for their recognised expertise. We also extend special thanks to the contributing editors, Benjamin A Powell and Jason C Chipman of Wilmer Cutler Pickering Hale and Dorr LLP, for their continued assistance with this volume.

GETTING THE DEAL THROUGH

London
January 2019

Turkey

Stéphanie Beghe Sönmez and Ceylan Necipoğlu
PAKSOY

Legal framework

1 Summarise the main statutes and regulations that promote cybersecurity. Does your jurisdiction have dedicated cybersecurity laws?

Turkey does not have any dedicated cybersecurity laws. The data protection legislation, including the Personal Data Protection Law No. 6698 (the PDPL), however, contains general requirements with regard to the security of personal data. Cybersecurity breaches can thus lead to a breach of data protection law.

The Council of Ministers has issued a decision on national cybersecurity strategy, published in the Official Gazette on 20 June 2013, in the form of an action plan aimed at ensuring the protection of services, transactions and data provided by the government through IT systems, and critical IT infrastructure operated by the public and private sectors. On that basis, the Ministry of Transport, Maritime Affairs and Communication has prepared a 2016–2019 national cybersecurity strategy and action plan, under which definitions, principles, cybersecurity risks and strategic cybersecurity purposes and actions are presented. This plan aims to shape Turkey's cybersecurity legislation in accordance with international standards and establish a public authority that ensures coordination in the field of cybersecurity.

Despite the lack of general legislation to date, certain sector-specific pieces of legislation apply. Electronic Commerce Law No. 6563 (the E-Commerce Law) and Banking Law No. 5411 (the Banking Law) and are the most important ones. In the banking sector, a draft Regulation on the Information Systems of Banks and Electronic Banking (the Draft Regulation) has been recently published, bringing a renewed focus on data protection and cybersecurity issues. The Draft Regulation is meant to repeal the Communiqué on the Principles Applicable to the Information Systems of Banks (the Communiqué) issued by the Banking Regulation and Supervision Agency (the BRSA) in 2007. The Draft Regulation contemplates at least 90 hours per year of mandatory training for bank personnel, and the annual conduct of penetration tests by independent firms.

Cybersecurity issues are also addressed under the Payment Systems Law No. 6943, which makes special certification (ISO 27001 and PCI DDS) mandatory for credit card information. In the health and insurance sectors, the data protection legislation imposes stricter requirements in terms of cybersecurity, to the extent healthcare providers and health insurers process health personal data, which qualify as a special category of data and require enhanced protection. These two sectors also have their own legislation with regard to confidentiality obligations, thus making cybersecurity even more critical. In the telecommunication sector, the Information and Communication Technologies Authority (ICTA) has detailed regulations with regard to technical precautions to be taken by telecommunications providers.

2 Which sectors of the economy are most affected by cybersecurity laws and regulations in your jurisdiction?

Since the PDPL is of general application, companies in all sectors have to comply with data protection law to the extent they process personal data. In addition, the banking, insurance, e-commerce, telecommunication and health sectors have sector-specific legislation and are thus more affected by cybersecurity issues. Owing to their data-intensive nature, these sectors have showed faster progress than other sectors in the field of cybersecurity. The issuance of additional rules specific to the telecommunication sector is also expected according to the NATO Cooperative Cyber Defence Centre of Excellence's National Cybersecurity Organization: Turkey report. Developments are also expected in the military sector: under the modernisation programme of the Cyber Defence Command, a new military-CERT and dedicated cyberdefence training laboratory has been launched. This will bring a new set of rules for cyberdefence.

3 Has your jurisdiction adopted any international standards related to cybersecurity?

For the Turkish Armed Forces, cybersecurity and defence standards are prepared in accordance with those of NATO. As Turkey is a member of the International Organization for Standardization (ISO), the requirements set out under the ISO/IEC 27001 standard have to be complied with in the field of data security. ISO/IEC 27001 is a common standard that is also applicable and mandatory under Turkish law for entities providing electronic communication services, electronic networks and infrastructure, and energy facilities. E-commerce companies and payment system providers have to comply with the Payment Card Industry Data Security Standard (PCI DSS) to keep online payment records and sensitive data, such as credit card numbers, secure. Institutions in the banking sector must comply with the Control Objectives for Information and Related Technology (COBIT) standards, that are audited by the BRSA on an annual basis to ensure data security and integrity. Although the ISO/IEC 23001 and ISO/IEC 19790 standards have been used with respect to sustainability and cryptography of the data, these are not mandatory.

4 What are the obligations of responsible personnel and directors to keep informed about the adequacy of the organisation's protection of networks and data, and how may they be held responsible for inadequate cybersecurity?

The PDPL does not regulate the concept of data protection officer. As per the DPLD and the guidelines on necessary technical and organisational measures published by the Turkish Data Protection Authority (DPA), organisations who act as a data controller or data processor have to use and implement the necessary technical and organisational measures listed therein to ensure an appropriate security level to prevent data breaches. In case of breach, if the behaviour that led to the breach can be characterised as a crime, a sanction can only be imposed on the natural person perpetrator, meaning the person who actually committed the act defined as an offence by the law. If an offence is committed upon the instruction of another person, the person who committed the act will be charged as the offender, while the person who instructed the perpetrator will be considered as an abettor. Both will be exposed to the applicable sanction for the offence at hand. Where the breach leads to an administrative penalty under the PDPL, on the other hand, the organisation itself can be fined. The liability of responsible personnel and directors will thus not be directly triggered under the provisions of the PDPL, unless they personally took part in the behaviour that led to the breach. On the other hand, directors can find themselves liable to their company under the provisions of the Turkish Commercial Code, if their failure to adequately manage and supervise the company, including by ensuring that the organisation's networks and data are adequately protected against cyberthreats, amounts to a breach of

their fiduciary duties. This could lead to their dismissal and to actions for compensation against individual directors. Responsible personnel on the company's payroll, on the other hand, could face consequences under labour law, including termination without severance.

More specific precautions in terms of cybersecurity are imposed on organisations active in regulated sectors. In the banking sector, the primary and secondary systems of banks, payment service providers and electronic money institutions should be located within the Turkish territory for data security purposes. In case of breach, a disaster recovery plan must be used to ensure data integrity. In addition, the Regulation on Bank Cards and Credit Cards states that institutions that issue credit cards must keep all personal data in confidence, refrain from using such data for marketing activities, and take all necessary precautions to keep records safe. Banks have a general obligation to supervise their information systems and ensure their secrecy, integrity and accessibility. Otherwise, administrative fines may be imposed by the BRSA. As per the Draft Regulation recently published by the BRSA, it would become mandatory to appoint a person who is responsible for cybersecurity issues and incident management. In case of data breach or cyberattack, this person would be responsible for informing the relevant departments and the BRSA immediately.

Similar rules were issued by the ICTA for the telecommunication sector.

In terms of individual liability of responsible personnel or directors in the banking and telecommunication sectors, under the current state of the legislation, the rules are the same as under the data protection legislation (ie, criminal liability would require personal involvement in the offence), while inadequate cybersecurity that leads to administrative fines for the organisation could ultimately trigger the directors' liability for breach of fiduciary duty under the Turkish Commercial Code.

5 How does your jurisdiction define cybersecurity and cybercrime?

There is no clear definition of cybersecurity under Turkish Law. Although cybersecurity as a concept is used in several regulations, it has not been specifically defined yet, whether by statute or through case law. The distinction between cybersecurity and data privacy has not been made by any authority, and cybersecurity requirements remain largely defined in terms of complying with data privacy obligations.

Various definitions have however been used by regulatory authorities. The ICTA has adopted the following definition Cybersecurity aims to ensure that the security features of institutions, organisations and users' assets are created and maintained in a way that they are able to withstand the security risks of cyber environments. The main objectives of cybersecurity are accessibility, integrity (fidelity and undeniable logs) and confidentiality.

6 What are the minimum protective measures that organisations must implement to protect data and information technology systems from cyberthreats?

Data controllers have the obligation to implement the technical and organisational measures necessary to ensure an appropriate security level to prevent personal data from being processed or accessed unlawfully, and to ensure its protection. The PDPL does not explicitly specify the technical and organisational measures to be taken, and these should be evaluated on a case-by-case basis.

The DPA has published guidelines on technical and organisational measures, which are not binding. These guidelines recommend several steps to be taken by those who process personal data. A proper firewall should be put in place. All applications and software should be protected against cyberattacks, which implies that they need to be kept up-to-date. Access to the systems that contain personal data should be limited. Employees should only be able to access information on a need-to-know basis. The use of brute-force algorithm (BFA), the requirement to use strong passwords, and limitations on the number of password entry attempts to ensure protection against most common attacks are also suggested. Anti-spam products that periodically review the system and detect malwares should be used. The integration of data leakage programs would also count as a protective measure. The guidelines further suggest pseudonymisation, micro merger, global coding, differentiated password systems, partial hiding, extraditing variables as technical methods to protect data.

Furthermore, in the banking sector, the Communiqué makes it mandatory to use a two-factor authentication method to protect data, and requires that risk analysis be carried out by the relevant department of the bank. As per the Draft Regulation, providing cybersecurity training will also become a requirement.

7 Does your jurisdiction have any laws or regulations that specifically address cyberthreats to intellectual property?

Turkey does not have any specific law addressing cyberthreats to intellectual property. Intellectual property rights are generally protected under the Intellectual Property and Artistic Works Law No. 5846, which provides for sanctions in case of infringement, regardless of the environment in which it is committed.

On the other hand, it is a crime for any person to produce, put up for sale, sell or possess for non-private use programs or technical equipment which aim to circumvent additional programs developed to prevent the illegal reproduction of a protected work. This offence is punished by six months to two years' imprisonment, which may in some cases be converted into a corresponding judicial fine.

8 Does your jurisdiction have any laws or regulations that specifically address cyberthreats to critical infrastructure or specific sectors?

Turkey does not have any specific legislation addressing cyberthreats to critical infrastructure. Yet, sector-specific regulations lead to the protection of critical infrastructure in the relevant sectors, such as financial services systems. Furthermore, the use of the ISO/IEC 27001 standard is mandatory for entities providing electronic communication services, electronic networks and infrastructure, and energy facilities.

9 Does your jurisdiction have any cybersecurity laws or regulations that specifically restrict sharing of cyberthreat information?

The Turkish Criminal Code makes it a crime to access or record telephone communications, or intercept and open private mail. While this should in principle extend to electronic communications, there are no express provisions in this respect in the legislation. It is however generally admitted that the confidentiality of electronic communications is protected as well, and this is expected to be expressly provided under the new cybersecurity law.

The only exception to the confidentiality of private communications is provided under the Turkish Code of Criminal Procedure No. 5271, under which the communications of persons suspected of illegal activities can be accessed and recorded for the needs of an investigation, with the permission of the public prosecutor. There is no law allowing access to private communications for the purpose of protecting networks or data against cyberthreats.

There are no laws governing access to metadata.

10 What are the principal cyberactivities that are criminalised by the law of your jurisdiction?

The following cyberactivities are criminalised under the Turkish Criminal Code No. 5237: providing unlawful or unauthorised access to information systems, blocking or destroying information systems and altering or destroying data; improper use of bank or credit cards; creating or putting together devices, software, passwords or other security codes to commit the abovementioned crimes; and producing, importing, delivering, transporting, storing, accepting, selling, supplying, purchasing or carrying the same. These offences can lead to sanctions ranging from one to three years' imprisonment.

The PDPL provides for a number of criminal sanctions in case of breach of its provisions. The persons who illegally collect personal data are subject to one to three years' imprisonment; if the data is sensitive personal data, the offender is subject to one-and-a-half to four-and-a-half years' imprisonment. The persons who illegally transfer personal data or make personal data available to the public are subject to two to four years' imprisonment. Finally, the persons who are responsible for the deletion of data following the expiry of the retention period, and who fail to do so, are subject to one to two years' imprisonment.

11 How has your jurisdiction addressed information security challenges associated with cloud computing?

Turkish Law has not yet specifically addressed security challenges associated with cloud computing. An informative note was issued in 2013 by the ICTA, leading to the publication of draft standards for cloud computing systems by the Turkish Standards Institution in 2014. These have not been finalised yet and are thus not binding.

The use of cloud services is indirectly regulated under the PDPL, to the extent that the storage of personal data processed by a Turkish organisation on cloud servers located outside Turkey will be considered as an international transfer of data, even if the data cannot be accessed by persons located in the third country. The PDPL rules with regard to the transfer of personal data outside Turkey will thus have to be complied with. Under the PDPL, personal data cannot be transferred to foreign countries unless the explicit consent of the data subject is obtained, or the organisation can rely on one of the exceptions set out by the law. In addition, if the recipient is located in a country that is not considered to provide adequate protection, the transfer is subject to the execution of a written undertaking by the sender and the recipient, as well as the prior approval of the DPA. The list of adequate protection countries has not been published to date.

The DPA's non-binding guidelines on technical and organisational measures also mention cloud computing systems. These mostly warn data controllers of the data protection risks associated with the use of cloud technology.

In the banking sector, the Draft Regulation provides that banks will be able to benefit from private cloud computing services only if the servers of the cloud services provider is located within the Turkish territory.

12 How do your jurisdiction's cybersecurity laws affect foreign organisations doing business in your jurisdiction? Are the regulatory obligations the same for foreign organisations?

Regulatory obligations are the same for all organisations doing business in Turkey, whether they are Turkish organisations with Turkish or foreign capital, or foreign organisations doing business through a local branch. Turkish organisations with foreign capital and foreign organisations doing business in Turkey are however more likely to need to consolidate data generated in Turkey in jurisdictions outside Turkey, for which they will face restrictions under the PDPL as explained in question 11.

Best practice

13 Do the authorities recommend additional cybersecurity protections beyond what is mandated by law?

The ICTA, as the telecommunications regulatory and supervision authority of Turkey, is authorised to regulate cybersecurity issues. While the ICTA's decisions are directly binding upon companies, the authority also publishes recommendations and guidelines. As per the recommendations of ICTA, each organisation dealing with data should conduct annual penetration tests to identify weaknesses in its information systems. The aim of the test is also to evaluate incident management methods. The same test is already required in the banking sector, but under the Draft Regulation, it would become mandatory to have such test conducted annually by an independent firm. The ICTA also recommends data classification, data governance projects and cryptology methods to be adopted to increase data security and minimise the risk of data leakage.

14 How does the government incentivise organisations to improve their cybersecurity?

The Turkish government does not currently provide any form of incentive for organisations to improve cybersecurity. It is however working on increasing cybersecurity standards and awareness within public institutions.

15 Identify and outline the main industry standards and codes of practice promoting cybersecurity. Where can these be accessed?

There are sector-based standards applicable in Turkey, the most common being ISO/IEC 27001. Regulations issued by the competent regulatory body make this standard mandatory for companies operating in certain sectors, in particular insurance companies, energy companies, banks, and information technologies companies. Companies providing payment systems must comply with the PCI DDS.

16 Are there generally recommended best practices and procedures for responding to breaches?

The DPA has not published any guidance with regard to best practices and procedures for responding to personal data breaches. Under the PDPL, the retention of third-party data forensic firms is not required, but can be useful to respond to the questions of the DPA, which is likely to request all available information related to the breach. There are no generally recommended best practices as regards communications to employees or with the media, which will be devised on a case-by-case basis.

The ICTA has published guidelines regarding general and sectoral best practices and procedures for responding to breaches in the telecommunications sector. These require operators affected by a breach to take certain technical measurements immediately in compliance with international standards. There is no requirement to retain third party forensic firms. Operators should have incident management and disaster recovery policies in place.

In the banking sector, the BRSA requires banks to comply with COBIT standards. Payment systems providers should comply with the practices and procedures set out under the PCI DSS standard.

17 Describe practices and procedures for voluntary sharing of information about cyberthreats in your jurisdiction. Are there any legal or policy incentives?

Turkey does not have any regulated practices or procedures for voluntary sharing of information about cyberthreats. The ICTA has, however, announced that it would particularly concern itself with cyberthreats listed by the Massachusetts Institute of Technology as critical cyberthreats for 2019, namely exploiting AI-generated fake video and audio, poisoning AI defences, hacking smart contracts, breaking encryption using quantum computers, and attacking from the computing cloud.

18 How do the government and private sector cooperate to develop cybersecurity standards and procedures?

The ICTA periodically convenes a meeting with cybersecurity professionals to obtain their input to determine cybersecurity standards and procedures. This is an ongoing process, and no such standards and procedures have been officially determined yet.

19 Is insurance for cybersecurity breaches available in your jurisdiction and is such insurance common?

Since cybersecurity insurance is not an obligation, there are few insurance firms offering cybersecurity insurance policies in Turkey. Due to the lack of reliable standards and parameters to detect the risk of cybersecurity breach, the actuarial risk assessment is difficult to make and insurance companies in Turkey struggle to price this type of insurance product.

For the banking sector, cybersecurity breach insurance is recommended in the Draft Regulation, and can be counted as one of the technical measures to ensure cybersecurity. Yet insurance for cybersecurity breaches will not be mandatory.

Enforcement

20 Which regulatory authorities are primarily responsible for enforcing cybersecurity rules?

The ICTA is the regulatory body authorised to take decisions and actions regarding the protection of information systems. On the other hand, since the PDPL is the only general piece of legislation that currently imposes requirements in terms of cybersecurity, the DPA is the regulatory authority competent to conduct investigations, issue binding decisions and impose administrative fines. To the extent cybercrimes are defined under the Turkish Criminal Code, public prosecutors and criminal courts are also competent to investigate, prosecute and impose sanction in relation to such crimes.

21 Describe the authorities' powers to monitor compliance, conduct investigations and prosecute infringements.

Under the PDPL, the DPA has the right to audit data controllers and processors, including the right to conduct site inspections and request documents. In the banking sector, the BRSA has right to audit the banks' information systems. Pursuant to the Regulation on Bank Information Systems and Banking Processes Audit to be Performed by External Audit Institutions, issued by the BRSA in 2010, banks have to be in compliance with COBIT standards and are subject to yearly audits conducted by certified independent firms at the request of the BRSA. The BRSA is also authorised to audit other financial institutions, including payment systems providers and e-money companies. In addition, institutions that hold a PCI DSS certification and obtain credit card information can be audited and investigated by the PCI DSS auditors.

22 What are the most common enforcement issues and how have regulators and the private sector addressed them?

The practice of regulatory is generally to afford cure periods to organisations to remedy instances of non-compliance. If the DPA identify deficiencies in the technical and organisational measures taken to protect personal data, it can give a 15-day period to cure the situation under the PDPL, and eventually issue administrative fines. The ICTA and the BRSA also have the power to request that deficiencies be cured within a certain period of time, and to issue administrative fines if the necessary measures are not taken. Where fines are indeed imposed, these can be quite substantial, especially in the banking sector where there is no statutory cap. There are market precedents in which fines well in excess of 10% of the affected bank's revenue were imposed following a failure to take necessary measures against cyberthreats, and then to report the breach immediately. On the other hand, it is difficult to have a clear picture of the enforcement environment, to the extent most regulatory decisions imposing fines are not made public; the lack of transparency in this respect is a recurrent issue in Turkey.

23 What penalties may be imposed for failure to comply with regulations aimed at preventing cybersecurity breaches?

The PDPL provides that the failure to comply with the obligation to ensure data security can result in a fine ranging from 15,000 to 1 million lira. In addition, the failure to comply with the decisions of the DPA, which can include injunctions to comply with cybersecurity requirements, can result in a fine ranging from 25,000 to 1 million lira.

In the telecommunication sector, the ICTA has broad powers to impose fines of up to 3 per cent of the operator's net revenue in the previous year for the failure to comply with laws, regulations and the ICTA's own decisions. In the banking sector, the BRSA also has the power to impose fines calculated by reference to the bank's revenue, but this is not subject to a formal cap and will be determined by the BRSA on a per breach basis.

If it determined following an inspection by ISO mandated auditors that a company fails to comply with the ISO 27001 standard, the certification may be suspended or cancelled. In the field of payment systems, if a company fails to comply with PCI DSS standards twice, the certificate is taken away from the company. For companies that are required to comply with the ISO 27001 standard by their own regulatory authority, such as the Energy Market Regulatory Authority in the energy sector, administrative fines can be directly imposed by the competent regulator in case of failure to comply.

While this would only apply in extreme cases, Turkish regulatory bodies also have the power to suspend or cancel an organisation's operating licence in case of incompliance with laws, regulations or regulatory decisions.

24 What penalties may be imposed for failure to comply with the rules on reporting threats and breaches?

Under the PDPL, the failure to report a data breach to the DPA and the data subjects can lead to administrative fines ranging from TRY15,000 to 1 million lira. In the telecommunication sector, the ICTA may impose fines of up to 3 per cent of the operator's net revenue in the previous year for the failure to report a security breach. In the banking sector, the BRSA also has the power to impose fines calculated by reference to the bank's revenue, but this is not subject to a formal cap and will be determined by the BRSA on a per incident basis.

25 How can parties seek private redress for unauthorised cyberactivity or failure to adequately protect systems and data?

Compensation lawsuits may be initiated on the basis of general principles of law, including by seeking liability in tort, or in contract if there was a contractual relationship between the parties. If the data breach affects personal data, the PDPL expressly provides for the data subjects' right to compensation if their data has been processed in breach of the law. If the data breach resulted in the infringement of intellectual property rights, compensation can also be sought on the basis of intellectual property law. If a company has suffered damages due to its directors' failure to cause the implementation of adequate cybersecurity within the organisation, this could qualify as a breach of fiduciary duties and form the basis of a liability claims against the directors under the Turkish Commercial Code.

Threat detection and reporting

26 What policies or procedures must organisations have in place to protect data or information technology systems from cyberthreats?

See question 6.

27 Describe any rules requiring organisations to keep records of cyberthreats or attacks.

There is no general legal requirement to keep cyberthreat records, although it is strongly advisable to keep records of all activity affecting personal data in the event of a DPA inspection. Most companies will also have the obligation to keep internet log records for three years under the Internet Law no. 5651 and related regulations, as long as they provide access to the internet, even if only to their own employees.

In the telecommunication sector, the Regulation on Network and Information Security in the Electronic Communications Sector, issued by the ICTA in 2008, requires that records regarding network and security breaches be kept for three years. In the banking sector, banks are obliged to keep the records of data and logs, but it is currently unclear how long the records should be retained. As per the Draft Regulation, banks will be under the obligation to keep records of all transactions for three years as well. Banks and telecom operators are also required to report breaches to the regulator in annual reports. The Internet Law also requires organisations to keep logs of all e-commerce and call centre transactions, which can be later be used for evidence purposes.

28 Describe any rules requiring organisations to report cybersecurity breaches to regulatory authorities.

If the breach affects personal data, the PDPL provides that in case personal data is illegally obtained by third parties, the data controller must inform the DPA and the relevant data subjects as soon as possible. The PDPL further states that the DPA may publish an announcement regarding the data breach on its website or by any other method it deems appropriate. The failure to comply with this obligation would expose the affected organisation to administrative fines.

In the telecommunication sector, a binding decision of the ICTA requires operators to notify any type of cybersecurity breach, including data leakage and cyberattacks, to the authority. Reports should include, among others, logs, time stamps, the identification numbers of affected devices, a description of the lost data, and the time by which the breach was discovered.

In the banking sector, banks currently have to prepare a form containing substantially the same information as listed above, as well as an identification of potential harm to end users (such as affected transactions) and submit it to the BRSA. Under the Draft Regulation, it would become mandatory to appoint a person responsible for cybersecurity issues, who would be responsible inform the departments of the bank and the relevant authorities in case of breach. Banks would also be obliged to report cyberthreats in addition to breaches.

In addition, if a public company is affected by a cyberattack, it must notify the Capital Markets Board, which will make the information publicly available. In the insurance sector, even though it is not mandatory,

Update and trends

While Turkish regulatory authorities are yet to publish an additional draft or working paper addressing future plans for cybersecurity, there has been an ever-increasing trend towards digitalisation in the country. Turkish public authorities have started to use digital platforms to increase efficiency, integrity and sustainability. One of the most recent examples would be the electronic online apostille services to be provided by the Post, Telegraph and Telephone Institution. The Istanbul Municipality has started to work on a smart cities system, and to collect data for payment systems in public transportation and vendor machines. The intent is to introduce a city card, Kent Kart, for payments in public places. This will bring about the need for increased cybersecurity precautions. Another significant development concerns the land registry system, with land registries starting to keep online records and to accept online payments for land registry transactions. A series of other formalities, such as trade registry applications or registration with the data controller registry, must now be made through online systems.

In view of this growing trend towards digitalisation, the ICTA has started to draft a code regarding cybersecurity issues, which should follow the approach taken in the Draft EU Cybersecurity Act (the Draft Cybersecurity Act) expected to be approved in 2019 to introduce a new standardised cybersecurity framework and provide an EU-wide certification system identifying resilience to cyberattacks. Since the PDPL and Payment Systems Law were largely modelled on EU legislation, Turkey's future cybersecurity code is expected to be similar to the Draft Cybersecurity Act. In the meetings convened with cybersecurity experts, ICTA officials have largely referred to the Draft Cybersecurity Act as an example.

Another expected development related to cybersecurity is the amendment of the Payment Systems Law. Since the current piece of legislation was based on the original EU Payment Services Directive, which has now been revised (PSD2), the Payment Systems Law will likely be adapted to take into account new encryption and cryptology methods set out under PSD2.

Last but not least, while Turkey does not yet have any electronic online procurement system regulation, this is definitely on the government's agenda. The electronic online procurement system recently adopted in the United Kingdom is expected to serve as a model.

it is strongly advisable for companies to notify the Undersecretariat of Treasury, which is the insurance regulator.

29 What is the timeline for reporting to the authorities?

Pursuant to the PDPL, the DPA and the relevant data subjects must be notified as soon as possible after a data breach or cyberattack is discovered. There is no requirement to report about cybersecurity on a regular basis under the PDPL.

Likewise, all regulatory authorities mentioned in question 28 should be notified as soon as the breach is discovered.

Regular reporting obligations only exist in the banking and telecommunication sectors. Banks must submit a COBIT report to the BRSA in the first month of each year, and telecommunications companies must submit a report including an assessment of cyber-risks, encountered cyberattacks and precautions taken against them, to the ICTA in the first three months of each year.

30 Describe any rules requiring organisations to report threats or breaches to others in the industry, to customers or to the general public.

The PDPL requires that data breaches affecting personal data be notified to data subjects in addition to the DPA. There are no formal requirements to report threats or breaches to others in the industry or to the general public.

Paksoy

Stéphanie Beghe Sönmez **sbeghe@paksoy.av.tr**
Ceylan Necipoğlu **cnecipoglu@paksoy.av.tr**

Orjin Maslak
Eski Büyükdere Caddesi No:27 K:11
Maslak 34485 Istanbul
Turkey

Tel: +90 212 366 47 00
Fax: +90 212 290 23 55
www.paksoy.av.tr

Getting the Deal Through

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

Also available digitally

Online

www.gettingthedealthrough.com

ISBN 978-1-912228-87-4