

CYBERSECURITY

Turkey



Cybersecurity

Consulting editors

Edward R. McNicholas, Fran Faircloth

Ropes & Gray LLP

Quick reference guide enabling side-by-side comparison of local insights, including into the applicable legal and regulatory framework; best practices, including information sharing and insurance; enforcement, including relevant regulatory authorities, notification obligations, penalties, and avenues of private redress; threat detection and reporting; and recent trends.

Generated 14 February 2022

The information contained in this report is indicative only. Law Business Research is not responsible for any actions (or lack thereof) taken as a result of relying on or in any way using information contained in this report and in no event shall be liable for any damages resulting from reliance on or use of this information. © Copyright 2006 - 2022 Law Business Research

Table of contents

LEGAL FRAMEWORK

Legislation

Scope and jurisdiction

BEST PRACTICE

Increased protection

Information sharing

Insurance

ENFORCEMENT

Regulation

Penalties

THREAT DETECTION AND REPORTING

Policies and procedures

Time frames

Reporting

UPDATE AND TRENDS

Key developments of the past year

Contributors

Turkey



Stéphanie Beghe Sönmez
sbeghe@paksoy.av.tr
Paksoy



Mert Karakaşlar
mkarakaşlar@paksoy.av.tr
Paksoy

Paksoy

LEGAL FRAMEWORK**Legislation**

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 (PDPL), however, contains general requirements with regard to the security of personal data. Cybersecurity breaches can therefore lead to a breach of data protection law.

Following the previous version for the periods between 2013–2014 and 2016–2019, the Ministry of Transport, Maritime Affairs and Communication prepared the 2020-2023 National Cybersecurity Strategy and Action Plan (the National Action Plan), under which definitions, principles, cybersecurity risks and strategic cybersecurity purposes and actions were presented. This plan aimed to shape Turkey's cybersecurity legislation in accordance with international standards and establish a public authority that ensures coordination in the field of cybersecurity.

The 11th Development Plan of the Turkish Republic for the 2019–2023 period (the Strategy Plan for 2019–2023) states that to mitigate national security and ensure technological transformations in primary sectors (eg, chemical industry, medicine and medical equipment, electronics, automotive and rail system equipment), Turkey must enhance its ability to develop cybersecurity and data privacy technologies, fill the gap in the number of qualified persons, further develop its administrative structures and keep its legislation in pace with ever-developing technology. Various plans and strategies are expected to be implemented within the period covered by the Strategy Plan for 2019–2023, including the establishment of new public organisations and committees dealing with cybersecurity. On the other hand, the Turkish Presidency's Digital Transformation Office (DTO), which was established in 2018, has been carrying out a series of studies and projects in the area of cybersecurity and data security for the purpose of ensuring digitalisation in public services and increasing public awareness thereof.

The Presidential Circular on Information and Communication Security Measures (the Circular), which was published by the Presidency on 6 July 2019, sets forth a series of measures aimed at increasing the security of critical data, including requirements for the domestic localisation of data and limitations on the use of cloud services. The Circular primarily concerns public institutions and organisations, but also private organisations that provide services in critical infrastructure sectors, namely banking and finance, electronic communications, transportation, energy, water management and critical public services. The Circular also provided that the DTO had to prepare an Information and Communication Security Guide (the Guide) to be implemented by public institutions and organisations, as well as organisations providing critical infrastructure services. The current information systems of these institutions shall be gradually aligned with the principles determined in the Guide. The Guide, which entered into force on 24 July 2020, lists a series of security measures to be implemented by institutions within the scope of the Circular and provides a 24-month timeline for actions to be taken. In addition, the DTO addressed some of the issues arising under the Circular in the form of frequently asked questions published on its website. On 27 October 2021, the DTO published the Information and Communication Security Audit Guide (the Audit Guide), which provides the methodology to be followed in planning the audits, implementing the audit procedures and reporting the audit results within the scope of mandatory annual periodic audits.

Despite the lack of general legislation to date, certain sector-specific pieces of legislation apply. The Electronic Commerce Law No. 6563 and the Banking Law No. 5411 are the most important. In the banking sector, the Regulation on the Information Systems of Banks and Electronic Banking (the Electronic Banking Regulation), published on 15 March 2020, brought a renewed focus on data protection and cybersecurity issues. The Electronic Banking Regulation contemplates at least 90 hours per year of mandatory training for bank personnel and the carrying out of annual penetration tests by independent firms. It puts in place a gradual transition system, with most provisions becoming effective on 1 July 2020, while six provisions in relation to identity authentication came into force on 1

January 2021. The Electronic Banking 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 (BRSA) in 2007.

In the health and insurance sectors, the data protection legislation imposes stricter requirements in terms of cybersecurity to the extent that healthcare providers and health insurers process health personal data, which qualifies as a special category of data and requires enhanced protection. These two sectors also have their own legislation with regard to confidentiality obligations, thus making cybersecurity even more critical. In the telecommunications sector, the Information and Communication Technologies Authority (ICTA) has detailed regulations with regard to technical precautions to be taken by telecommunications providers.

Law stated - 13 January 2022

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

As 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, telecommunications and health sectors have sector-specific legislation and are thus more affected by cybersecurity issues. Owing to their data-intensive nature, these sectors have shown faster progress than other sectors in the field of cybersecurity.

In the telecommunications sector, for instance, the ICTA published a decision on 28 March 2019 with regard to localisation requirements for remote programmable SIM technologies (eg, eUICC, e-SIM) used in devices that are manufactured to be used in Turkey, imported into the country or brought by passengers from abroad. The decision sets forth that where remote programmable SIM technologies are used in Turkey, SIM modules embedded in these devices must be programmed in such a way that they can be managed by authorised operators, and that only local operator profiles must be installed on the devices. One of the grounds for this decision is to maintain cybersecurity and prevent possible security breaches.

The issuance of additional rules specific to the telecommunications sector is also expected according to the NATO Cooperative Cyber Defence Centre of Excellence's National Cybersecurity Organisation: Turkey report . Developments are also expected in the military sector. The DTO has numerous projects in this field and is soon expected to become more active. On the other hand, under the modernisation programme of the Cyber Defence Command, a new military computer emergency response team and dedicated cyber defence training laboratory has been launched. This will bring a new set of rules for cyber defence.

Law stated - 13 January 2022

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 must 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.

Pursuant to the Regulation on Independent Audit of Information Systems and Business Processes issued by the BRSA on 31 December 2021, institutions in the banking sector must comply with control objectives in accordance with the principles determined by the BRSA to ensure data security and integrity. The previous issue of this regulation made reference to COBIT standards, but these have been removed in the new version. Although the ISO/IEC 23001 and ISO/

IEC 19790 standards have been used with respect to sustainability and cryptography of data, they are not mandatory.

In practice, payment system providers that support the e-commerce industry comply with the Payment Card Industry Data Security Standard, imposed by international credit card institutions to keep online payment records and sensitive data, such as credit card numbers, secure.

Law stated - 13 January 2022

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. Although the Turkish Data Protection Authority (DPA) has issued rules for the certification of data protection officers on 10 December 2021, these are solely aimed at certifying a level of knowledge in data protection law and do not define any position with specific duties or responsibilities under the PDPL. As per the PDPL and the guidelines on necessary technical and organisational measures published by the DPA, organisations that act as a data controller or data processor must use and implement the necessary technical and organisational measures listed therein to ensure an appropriate security level to prevent data breaches. In the event of a 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 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, 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 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 the event of a 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 Electronic Banking Regulation, it is mandatory to establish a cyber incident response team that is responsible for cybersecurity issues and incident management, and to ensure that the contact details of the team members are notified to the BRSA. In the event of a data breach or cyberattack, this team will be responsible for informing the relevant departments and the BRSA immediately. If such a breach or cyberattack results in the breach or disclosure of sensitive data or personal data, banks must notify their customers following an internal assessment.

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

In terms of individual liability of responsible personnel or directors in the banking and telecommunications 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.

Law stated - 13 January 2022

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'. In the National Action Plan, cybersecurity is defined as 'activities that consist in protecting the information systems that shield the cyber space from attacks, securing the confidentiality, integrity and accessibility of the information/data processed in this environment, detecting attacks and cyber incidents, activating reaction mechanisms against these detections, and then returning the systems to their pre-existing state before cyber events'; and cybercrime is defined as 'crimes targeting the security of an information system and/or the data and/or user connected to it and committed by using the information system'.

Law stated - 13 January 2022

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 that 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 algorithms, the requirement to use strong passwords and limitations on the number of password entry attempts to ensure protection against the most common attacks are also suggested. Anti-spam products that periodically review the system and detect malware should be used. The integration of data leakage programs would also count as a protective measure. The guidelines further suggest pseudonymisation, micro merging, global coding, differentiated password systems, partial hiding and 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 Electronic Banking Regulation, providing cybersecurity training is also a requirement.

Law stated - 13 January 2022

Scope and jurisdiction

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 that aim to circumvent additional programs developed to prevent the illegal reproduction of a protected work. This offence is punishable by six months to two years' imprisonment, which may in some cases be converted into a corresponding judicial fine.

Law stated - 13 January 2022

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

While Turkey does not have any specific legislation addressing cyberthreats to critical infrastructure, the Circular sets forth a general framework for security measures applicable to such infrastructures. Although the Circular does not expressly specify its scope of application, it primarily concerns public institutions and organisations. It also extends to private organisations that provide services in the following critical infrastructure sectors: banking and finance, electronic communications, transportation, energy, water management and critical public services. In addition, sector-specific regulations lead to the protection of critical infrastructure in the relevant sectors, such as financial services systems. Finally, the use of the ISO/IEC 27001 standard is mandatory for entities providing electronic communication services, electronic networks and infrastructure, and energy facilities.

Law stated - 13 January 2022

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.

Law stated - 13 January 2022

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 :

1. providing unlawful or unauthorised access to information systems, blocking or destroying information systems and altering or destroying data;
2. improper use of bank or credit cards;
3. creating or putting together devices, software, passwords or other security codes to commit the crimes listed in points (1) and (2); and
4. 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 the event of a breach of its provisions. 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. Persons who illegally transfer personal data or make personal data available to the public are subject to two to four years' imprisonment. Finally, persons who are responsible for deleting data following the expiry of the retention period but fail to do so are subject to one to two years' imprisonment.

Law stated - 13 January 2022

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 Strategy Plan for 2019–2023 prepared by the ICTA mentions that necessary legal and administrative arrangements will be made for the development and expansion of cloud computing services.

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 Electronic Banking Regulation provides that banks are obliged to have their primary and secondary systems within Turkish territory. Likewise, they will be able to benefit from private cloud computing services only if the servers of the cloud services provider are located within Turkish territory.

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.

Law stated - 13 January 2022

BEST PRACTICE

Increased protection

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

The Information and Communication Technologies Authority (ICTA), as the telecommunications regulatory and supervisory 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 the 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. This test is already required in the banking sector, but under the Regulation on the Information Systems of Banks and Electronic Banking, it is mandatory to have the test be 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.

Furthermore, a series of security measures to be implemented by institutions within the scope of the Presidential Circular on Information and Communication Security Measures (ie, public institutions and organisations, as well as private organisations that provide services in critical infrastructure sectors) are provided in the Guide to ensure network and system securities, application and data security, portable device and platform security, internet of things device security, personnel security and physical place security.

Law stated - 13 January 2022

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. In this respect, the Turkish Cyber Security Cluster was established in 2017 to develop the Turkish cybersecurity ecosystem with the contribution of all public agencies, academia and private sector representatives under the leadership of the Presidency of Defence Industries. This platform has a number of objectives, which include: increasing the number of cybersecurity companies in Turkey; supporting the development of the member companies' technical, administrative and financial capabilities; improving the branding of products and services; improving the standards of the cybersecurity ecosystem; increasing the competitiveness of member companies in the national and global market; increasing human capital in the field of cybersecurity; and increasing awareness of cybersecurity throughout society.

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. It is a legal requirement for energy companies, licensed operators in accordance with ICTA regulations and certified operators in accordance with customs law to obtain ISO/IEC 27001 certification. Companies providing payment systems services must comply with the Payment Card Industry Data Security Standard (PCI DSS), which is imposed in practice by international credit card institutions. At points where classified information is processed by public institutions and organisations, dissemination security (TEMPEST) or similar security measures must be taken.

Law stated - 13 January 2022

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

The Turkish Data Protection Authority (DPA) has not published any guidance with regard to best practices and procedures for responding to personal data breaches. Under the Personal Data Protection Law No. 6698, the retention of third-party data forensic firms is not required but may 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 measures 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 Banking Regulation and Supervision Agency requires banks to comply with control objectives in accordance with the principles determined by the BRSA. Payment systems providers should comply with the practices and procedures set out under the PCI DSS.

Law stated - 13 January 2022

Information sharing

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. According to the 11th Development Plan of the Turkish Republic for the 2019–2023 period and the Strategy Plan for 2019–2023 issued by the ICTA, coordination and bidirectional information flow should be ensured between the National Cyber Incidents Response Centre (established under the ICTA) and public authorities, the private sector, universities, NGOs and cybersecurity volunteers to ensure coordination on cyberthreat intelligence with national and international stakeholders and to fight cyberthreats through rapid detection and early intervention.

Law stated - 13 January 2022

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.

Law stated - 13 January 2022

Insurance

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

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

Law stated - 13 January 2022

ENFORCEMENT

Regulation

Which regulatory authorities are primarily responsible for enforcing cybersecurity rules?

The Information and Communication Technologies Authority (ICTA) is the regulatory body authorised to take decisions and actions regarding the protection of information systems. However, as the Personal Data Protection Law No. 6698 (PDPL) is the only general piece of legislation that currently imposes requirements in terms of cybersecurity, the Turkish Data Protection Authority (DPA) is the regulatory authority competent to conduct investigations, issue binding decisions and impose administrative fines. To the extent that cybercrimes are defined under the Turkish Criminal Code, public prosecutors and criminal courts are also competent to investigate, prosecute and impose sanctions in relation to such crimes.

The Digital Transformation Office (DTO), established in 2018, is the main body responsible for the digital transformation of public institutions and cybersecurity. As per Presidential Decree No. 1 on the organisation of the Presidency (of which the DTO is a department), the DTO is authorised to implement strategies and policies regarding cybersecurity and to coordinate the regulatory activities necessary for digital transformation and the harmonisation of national regulation with international standards.

Law stated - 13 January 2022

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 Banking Regulation and Supervision Agency (BRSA) has the right to audit the banks' information systems. Pursuant to the Regulation on Independent Audit of Information

Systems and Business Processes issued by the BRSA on 31 December 2021, banks must comply with control objectives in accordance with the principles determined by the BRSA and are subject to yearly audits conducted by certified independent firms at the request of the BRSA in accordance with the rules and principles set forth under the aforementioned regulation. The BRSA is also authorised to audit other financial institutions, including payment systems providers and e-money companies. In addition, institutions that hold a Payment Card Industry Data Security Standard (PCI DSS) certification and obtain credit card information can be audited and investigated by the PCI DSS auditors.

Law stated - 13 January 2022

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

The practice of regulators is generally to afford cure periods to organisations to remedy instances of non-compliance. If the DPA identifies 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 imposed, they 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 per cent of the affected bank's revenue were imposed following a failure to take necessary measures against cyberthreats and report the breach immediately. On the other hand, it is difficult to have a clear picture of the enforcement environment because most regulatory decisions imposing fines are not made public; the lack of transparency in this respect is a recurrent issue in Turkey.

Law stated - 13 January 2022

What regulatory notification obligations do businesses have following a cybersecurity breach? Must data subjects be notified?

In the event of a cybersecurity breach potentially affecting personal data, the data controller must notify the DPA without undue delay and, where feasible, no later than 72 hours after becoming aware of the data breach. Data subjects must also be notified via appropriate methods as soon as possible after determination of the persons affected by the data breach.

The following elements must be included in the notification made to the data subjects:

- date of the breach;
- information on the categories of personal data affected by the breach;
- possible consequences of the breach;
- measures taken or proposed to be taken to reduce or eliminate possible adverse effects; and
- the names and contact details of the persons who can provide information about the breach or the full contact details of the data controller.

Law stated - 13 January 2022

Penalties

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 40,179 Turkish lira to 2,678,863 Turkish lira (for 2022). In addition, failure to comply with the decisions of the DPA, which may include injunctions to comply with cybersecurity requirements, can result in a fine ranging from 66,965 Turkish lira to 2,678,863 Turkish lira (for 2022).

In the telecommunications 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 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 is determined, following an inspection by mandated auditors of the International Organization for Standardization (ISO), that a company has failed to comply with the ISO 27001 standard, the company's certification may be suspended or cancelled. In the field of payment systems, if a company fails to comply with the PCI DSS 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 non-compliance with laws, regulations or regulatory decisions.

Law stated - 13 January 2022

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

Under the PDPL, failure to report a data breach to the DPA and the data subjects can lead to administrative fines ranging from 40,179 Turkish lira to 2,678,863 Turkish lira (for 2022). In the telecommunications 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 case-by-case basis.

Law stated - 13 January 2022

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 damage as a result of its directors' failure to implement adequate cybersecurity measures within the organisation, this could qualify as a breach of fiduciary duties and form the basis of liability claims against the directors under the Turkish Commercial Code.

Law stated - 13 January 2022

THREAT DETECTION AND REPORTING

Policies and procedures

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

The Regulation on Deletion, Destruction and Anonymisation of Personal Data provides that data controllers that are obliged to register with the data controller registry should prepare a data retention and disposal policy based on the personal data processing inventory, and should include the technical and organisational measures to be provided by data controllers.

Organisations acting as 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 Personal Data Protection Law No. 6698 (PDPL) does not explicitly specify the technical and organisational measures to be taken, and these should be evaluated on a case-by-case basis.

As per Decision No. 2019/10 of the Turkish Data Protection Authority (DPA), dated 24 January 2019, data controllers should prepare and periodically review a data breach intervention plan. This plan should include matters such as the internal reporting line, responsible persons for disclosures and assessments of possible outcomes of data breaches.

The Information and Communication Technologies Authority (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 measures 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 Banking Regulation and Supervision Agency (BRSA) requires banks to comply with control objectives in accordance with the principles determined by the BRSA. Payment systems providers should comply with the practices and procedures set out under the Payment Card Industry Data Security Standard. At points where classified information is processed by public institutions and organisations, dissemination security (TEMPEST) or similar security measures must be taken.

Law stated - 13 January 2022

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 an inspection by the DPA. Most companies will also have an obligation to keep internet log records for two 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 telecommunications sector, the Regulation on Network and Information Security in the Electronic Communications Sector, issued by the ICTA in 2014, requires that records regarding network and security breaches be kept for two years. In the banking sector, banks are obliged to keep records of data and logs, but it is currently unclear how long the records should be retained. In accordance with the Regulation on the Information Systems of Banks and Electronic Banking (the Electronic Banking Regulation), banks are under the obligation to keep records of all transactions for three years. Banks and telecoms operators are also required to report breaches to the regulator in annual reports. The Internet Law also requires internet access providers to keep records of traffic information for one year, and organisations to keep logs of all e-commerce and call centre transactions, which can be later be used for evidence purposes.

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

If the breach affects personal data, the PDPL provides that if 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 telecommunications 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 other things, logs, time stamps, the identification numbers of affected devices, a description of the lost data and the time at 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 identification of potential harm to end users (such as affected transactions) and submit it to the BRSA. Under the Electronic Banking Regulation, it is mandatory to appoint a team responsible for cybersecurity issues, whose duties would include informing the departments of the bank and the relevant authorities in the event of a breach. Banks would also be obliged to report cyberthreats as well as 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, it is strongly advisable for companies to notify the Undersecretariat of the Treasury, which is the insurance regulator.

Law stated - 13 January 2022

Time frames

What is the timeline for reporting to the authorities?

In the event of a cybersecurity breach potentially affecting personal data, the data controller must notify the DPA without undue delay and, where feasible, no later than 72 hours after becoming aware of the data breach. Data subjects must also be notified via appropriate methods as soon as possible after determination of the persons affected by the data breach. There is no requirement to report on cybersecurity on a regular basis under the PDPL.

Likewise, all the relevant regulatory authorities should be notified as soon as the breach is discovered. This could mean the ICTA, the BRSA and any other competent authority depending on the sector in which the affected entity operates.

Regular reporting obligations only exist in the banking and telecommunications sectors. Banks must submit an information system audit report to the BRSA in accordance with the rules and principles to be determined by the BRSA, 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.

Law stated - 13 January 2022

Reporting

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.

Law stated - 13 January 2022

UPDATE AND TRENDS

Key developments of the past year

What are the principal challenges to developing cybersecurity regulations? How can companies help shape a favourable regulatory environment? How do you anticipate cybersecurity laws and policies will change over the next year in your jurisdiction?

Together with the publication of various strategy and development plans that set promising goals for the government and regulatory authorities to develop cybersecurity and information technologies in several sectors, there has been an increasing trend towards digitalisation in the country. Turkish public authorities have started to use digital platforms to increase efficiency, integrity and sustainability. One example is the electronic online apostille services to be provided by the Post, Telegraph and Telephone Institution.













The Ministry of Environment and Urbanisation published its smart cities strategy and action plan for 2020–2023, which introduces various enhancements in the areas of data security, information technologies, smart infrastructures and so on. The Istanbul Municipality is working on a smart cities system and on the collection of data for payment systems in public transportation and vendor machines. The intent is to introduce a city card, the Kent Kart, for payments in public places. This will bring about the need for increased cybersecurity precautions. The establishment of an Istanbul Cyber Security Platform is also on the agenda. However, no official announcement has been made to date regarding the implementation of these projects. 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 Information and Communication Technologies Authority (ICTA) has started to draft a code regarding cybersecurity issues that should follow the approach taken in the EU Cybersecurity Act to introduce a new standardised cybersecurity framework and provide an EU-wide certification system identifying resilience to cyberattacks. Since the Personal Data Protection Law No. 6698 and the Payment Systems Law are largely modelled on EU legislation, Turkey's future cybersecurity code is expected to be similar to the EU Cybersecurity Act. In the meetings convened with cybersecurity experts, ICTA officials have largely referred to the EU Cybersecurity Act as an example.

Overall, the cybersecurity ecosystem in Turkey is developing as more strategies, plans and projects are being drawn up, in particular in the public sector and in critical private sectors, such as banking, health, telecommunications and energy. One obvious challenge for authorities devising legislation in this field is to keep up with fast-paced technological developments and the changing needs of private sector players. Turkish public authorities dealing with cybersecurity issues have, however, shown themselves to be quite open to seeking feedback from market players and involving them in the process to shape the new regulations. In this area, more than others, it is in the interest of market players to engage with regulatory authorities as early as possible in the process, make their needs known to these authorities and provide constructive feedback as to the proposed regulations.

Law stated - 13 January 2022

Jurisdictions

	Austria	MGLP Rechtsanwälte Attorneys-at-Law
	Belgium	Keller and Heckman LLP
	China	Fangda Partners
	European Union	Taylor Wessing
	France	ADSTO
	India	AZB & Partners
	Italy	ICT Legal Consulting
	Japan	TMI Associates
	Singapore	Drew & Napier LLC
	Switzerland	Walder Wyss Ltd
	Turkey	Paksoy
	USA	Ropes & Gray LLP