Chambers AND PARTNERS

CHAMBERS GLOBAL PRACTICE GUIDES

Cybersecurity 2025

Definitive global law guides offering comparative analysis from top-ranked lawyers

Türkíye: Law and Practice & Trends and Developments

Bora Yazıcıoğlu, Kübra İslamoğlu Bayer, Aslı Rabia Savaş and Yağmur Yaren Özdabakoğlu
YAZICIOGLU Legal

TÜRKIYE

Law and Practice

Contributed by:
Bora Yazıcıoğlu, Kübra İslamoğlu Bayer, Aslı Rabia Savaş and Yağmur Yaren Özdabakoğlu
YAZICIOGLU Legal

Contents

Contributed by: Bora Yazıcıoğlu, Kübra İslamoğlu Bayer, Aslı Rabia Savaş and Yağmur Yaren Özdabakoğlu, **YAZICIOGLU Legal**

YAZICIOGLU Legal is an Istanbul-based boutique technology law firm. The firm focuses on legal matters related to technology, media & telecommunications and data protection/cybersecurity. It also has solid expertise in cross-border transactions, corporate and commercial matters, intellectual property, regulatory compliance, e-commerce, consumer protection and dispute resolution. YAZICIOGLU Legal has a dedicated team of 16 lawyers working on data protection and cybersecurity. The majority of the firm's workload involves data protection-related matters. In particular, the firm is known for successfully representing its clients on investigations and data breaches before the Turkish Data Protection Authority. It also provides assistance to several clients, both local and international, including, but not limited to, Acer, Reddit, and Workday, in ensuring compliance with data protection legislation, particularly in cross-border data transfers. The firm is ranked in several legal directories for TMT and is also a Bronze Corporate Member of the International Association of Privacy Professionals (IAPP).

Authors

Bora Yazıcıoğlu is the managing partner at YAZICIOGLU Legal. He has significant experience in advising national and international clients on several aspects of data protection, cybersecurity, and e-commerce law. Bora has represented several major clients on data breaches and investigations before the Turkish Data Protection Authority. He is one of the founding members and the current President of the Data Protection Association of Türkiye. Bora acts as the data controller representative for Zoom, Acer, Cerus, and Ookla in Türkiye.

Aslı Rabia Savaş is a senior associate at YAZICIOGLU Legal. She primarily focuses on data protection law, cybersecurity, e-commerce, and contracts law. Aslı holds an advanced master's degree specialising in data law, and a CIPP/E certificate from the International Association of Privacy Professionals.

Kübra İslamoğlu Bayer is a senior managing associate at YAZICIOGLU Legal. She advises clients on data protection, e-commerce, and cybersecurity laws. She is an active member of the Istanbul Bar Association's IT Law Commission: Artificial Intelligence Study Group and the Data Protection Commission. Kübra gives speeches on data protection on several platforms. She holds a CIPP/E certificate from the International Association of Privacy Professionals.

Yağmur Yaren Özdabakoğlu is an associate at YAZICIOGLU Legal. She focuses on various areas of law, including data protection, cybersecurity, e-commerce, contracts law and consumer protection law.

Contributed by: Bora Yazıcıoğlu, Kübra İslamoğlu Bayer, Aslı Rabia Savaş and Yağmur Yaren Özdabakoğlu, **YAZICIOGLU Legal**

YAZICIOGLU Legal

NidaKule – Goztepe
Merdivenköy Mahallesi Bora Sokak No: 1
Kat: 7 34732 Kadıköy
Istanbul
Türkiye

Tel: +90 216 468 8850
Fax: +90 216 468 8801
Email: info@yazicioglulegal.com
Web: www.yazicioglulegal.com

1. General Overview of Laws and Regulators

1.1 Cybersecurity Regulation Strategy

Cybersecurity has been at the forefront of Türkiye's strategic policies since the last decade as an integral part of its national security. The results are showcased in the Global Cybersecurity Index 2024 published by the International Telecommunication Union, which ranked Türkiye as a Tier-1 Role-modelling country in Europe and awarded a full score in all five areas of strength (eg, legal, technical, organisation, capacity development, and co-operation measures).

The National Cybersecurity Strategy for 2024–2028 (the *"NCS 2024"*)

Since 2012, the Ministry of Transport and Infrastructure (the MTI) has published four mid-term strategic plans for cybersecurity, the most recent being the NCS 2024. According to the NCS 2024, Türkiye's cybersecurity strategy for the next four years is based on six objectives:

- cyber-resilience;
- proactive cyber-defence and deterrence;
- human-centred cybersecurity approach;
- secure use of technology and its contribution to cybersecurity;
- use of domestic and national technologies for combating cyber threats; and
- international reputation.

The 12th Development Program (2024–2028)

The 12th Development Program sets out the following general policy goals for information technologies, as well as sector-specific policies (eg, financial markets, education and health):

- strategic, regulatory, and technological efforts to ensure national cybersecurity and strengthen institutional structures;
- updating the National Cyber Security Strategy and Action Plan in the context of new-generation cyber-threats and technological developments;
- enacting regulations in line with the EU's *"NIS2 Directive"* and the best international practices;
- administrative structuring for high-level co-ordination of national cybersecurity activities;
- strengthening cybersecurity threat intelligence through the development of AI and big data analytics applications;

- strengthening the national cybersecurity infrastructure;
- enacting and implementing procedures and principles on the establishment of an information security system in critical infrastructures;
- introducing cybersecurity standards in the required fields;
- improving the domestic cybersecurity ecosystem, spreading national solutions, and boosting competitiveness on an international scale;
- supporting the global competitiveness of domestic solutions;
- developing test infrastructures for cybersecurity;
- increasing the use of domestic cybersecurity products, primarily in public institutions;
- raising cybersecurity awareness and training a competent workforce and making new business models for maintaining the same;
- building programmes aimed at cybersecurity training and bettering career opportunities; and
- improving the content, quality, and environment for training personnel fit for the sectoral needs.

The Medium-Term Program (2025–2027)

Medium-Term Program provides the following policy objectives:

- utilising digital technologies to the fullest extent to strengthen nationwide cybersecurity through comprehensive policies, enhance the efficiency of public administration, and develop public services;
- enacting dedicated legislation on cybersecurity and the necessary secondary regulations in compliance with the EU *acquis* (the collection of common rights and obligations that constitute the body of EU law, incorporated into the legal systems of EU member states – according to the official website of the EU);
- implementing public–university–private sector co-operation programmes to train qualified personnel in strategic fields, including cybersecurity; and
- taking measures to increase the level of resilience in payment and electronic institutions' cybersecurity.

The Presidency Program for 2025

Lastly, the Presidency Program for 2025 sets out more specific plans that are based upon the six objectives set out in the NCS 2024, including:

- legislative works in line with the EU legal framework (eg, the EU's NIS2 Directive and the EU Cyber Resilience Act);
- review of critical infrastructure sectors;
- awareness-raising activities for the public; and
- cybersecurity training for public servants.

1.2 Cybersecurity Laws

There have been significant developments in cybersecurity legislation of Türkiye recently. On 19 March 2025, the Cybersecurity Act was published in the official gazette and entered into force. According to the Cybersecurity Act, secondary regulations will be made within one year. Until then, current regulations that are not contrary to the Cybersecurity Act will continue to be in force.

General Regulations

The Constitution of the Turkish Republic (the "Constitution")

The Constitution does not directly set out any provision on cybersecurity. However, as cybersecurity is an umbrella term also covering data protection – whether it is personal or non-personal data – it can be considered that cyberse-

curity is partly and indirectly covered by Article 20(3) of the Constitution, which provides for the right to protection of personal data. Furthermore, Article 22 recognises freedom of communication as an individual right to any person.

The Cybersecurity Act

The Cybersecurity Act provides a dedicated legal framework for the responsibilities of institutions and persons who operate in cyberspace and the powers and duties of the recently established Cybersecurity Directorate (*"Directorate"*). It also establishes the Cybersecurity Board and determines its duties.

Additionally, certain actions are now criminalised, such as:

- failure to provide information, documents and data to the Directorate's audit personnel;
- distributing, sharing or selling leaked data; and
- creating and disseminating false content regarding data breaches in cyberspace, with the intent to incite anxiety, fear and panic among the public or to target institutions or individuals.

There are also specific requirements for companies producing cybersecurity products and services.

For more information on the Cybersecurity Act, see **1.3 Cybersecurity Regulators**, **2.1 Scope of Critical Infrastructure Cybersecurity Regulation**, **2.2 Critical Infrastructure Cybersecurity Requirements**, **4.1 Cyber-Resilience Legislation**, **4.2 Key Obligations Under Legislation**, and **5.1 Key Cybersecurity Certification Legislation**.

The Law on Regulation of Publications via the Internet and Combating Crimes Committed by Means of Such Publications No 5651 (the "Internet Law")

The Internet Law aims to regulate the obligations and responsibilities of content providers, hosting providers, internet service providers, social network providers, and access providers to combat crimes committed via the internet.

The Internet Law directs the Turkish Information and Communication Technologies Authority (the ICTA) to establish co-ordination between the relevant public institutions, law enforcement agencies, above-mentioned providers and other related institutions and organisations to ensure the safe use of the internet, raise public awareness, and carry out necessary activities (eg, taking necessary measures within the scope of national cybersecurity policies). However, according to the Cybersecurity Act, the ICTA will no longer be able to carry out these duties when the Directorate's organisation is completed.

The Law on Electronic Communication No 5809 (the "E-Communication Law")

Information security is among the basic principles in the E-Communication Law, which provides the main framework for network security, the confidentiality of communication, and personal data protection. Detailed provisions concerning each may be found under several secondary pieces of legislation enacted based thereon.

While the ICTA is the authorised regulatory body in the e-communications sector, its authority in cybersecurity measures has now been transferred to the Directorate. However, the ICTA will continue to exercise these powers until the latter becomes operational.

The Council of Ministers Decision on Carrying Out, Managing and Co-ordinating National Cybersecurity Activities, dated 11 June 2012 (the "Council of Ministers Decision on Cybersecurity")

This decision is one of the landmarks of Türkiye's cybersecurity legislation. It defines national cybersecurity as: *"security of all services, transactions, and data provided via information and communications technologies as well as systems used for the provision thereof"*.

The Cybersecurity Act transfers the MTI's cybersecurity-related duties and powers to the Directorate; however, it does not explicitly annul this decision.

The Presidential Decree No 177 on the Cybersecurity Directorate

On 8 January 2025, the Presidential Decree No 177 on the Cybersecurity Directorate established the Directorate as a public legal entity affiliated with the Presidency with financial autonomy. The decree grants the Directorate general regulatory power on cybersecurity matters. Refer to **1.3 Cybersecurity Regulators** for further explanations on the duties of the Directorate.

The Communiqué on Procedures and Principles of the Establishment, Duties and Activities of Cyber-Incidents Response Teams (CERTs) (the "Communiqué on CERTs")

The purpose and scope of this *communiqué* are to ensure CERTs carry out their services effectively and efficiently by determining the procedures and principles of their establishment, duties and work.

The Guideline for Establishment and Management of Institutional CERTs (the "Institutional CERT Guideline") and the Guideline for Establishment and Management of Sectoral CERTs (the "Sectoral CERT Guideline")

These guidelines, published by the National Cyber Incidents Response Centre (TR-CERT), provide guidance on:

- establishing and managing institutional CERTs and sectoral CERTs in relevant organisations;
- their relationship with each other and the TR-CERT;
- capacity planning;
- qualifications of the personnel (education level and experience);
- mandatory training; and
- the steps that personnel must take before, during and after a cybersecurity incident.

They also include the principles for communication with internal/external stakeholders and establishing institutional and sectoral CERTs.

The Decree No 2019/12 on Information and Communication Security Measures issued by the Presidency of Türkiye (the "Presidency Decree")

The Presidency Decree sets specific measures deemed appropriate to diminish and neutralise security risks – in particular, ensuring the security of critical data that may jeopardise national security or deteriorate public order when its confidentiality, integrity, or accessibility is compromised. It provides an obligation to securely store critical data (eg, population, health and communication records, genetic and biometric data) within Türkiye.

The Presidency Decree applies to public institutions and organisations as well as businesses providing critical infrastructure services (ie, energy, electronic communications, banking and finance, critical public services, water management, and transportation). See **2.1 Scope of Critical Infrastructure Cybersecurity Regulation** for further details.

The Turkish Data Protection Law No 6698 (the "DP Law") and its secondary legislation

The DP Law covers all personal data-processing activities in Türkiye. From a cybersecurity perspective, it also regulates the security of personal data and full or partly automated and non-automated data-processing systems. According to the DP Law, controllers are obliged to take all necessary technical and organisational measures to provide a sufficient level of security to:

- prevent unlawful processing and accessing of personal data; and
- ensure the safekeeping of personal data.

See **6.1 Cybersecurity and Data Protection** for further information.

The Turkish Criminal Code (the TCrC) No 5237

The TCrC criminalises several actions in connection to cybersecurity and sets out criminal sanctions of imprisonment between six months and eight years for these actions. Some are as follows:

- unlawful access to a cyber-system;
- blocking or bricking the cyber-system or destroying, modifying, or making inaccessible the data within a cyber-system;
- misuse of debit or credit cards;
- manufacturing, importing, dispatching, transporting, storing, accepting, selling, offering for sale, purchasing, giving to others or keeping forbidden devices and software that are used to break a computer program's password or a code as such in order to commit a crime described in the bullet points above;
- committing theft or fraud via cyber-systems;
- unlawful recording of personal data;
- unlawful transfer, publication or acquisition of personal data; and
- failure to destroy personal data after the retention period set forth in the applicable laws.

The Law on Intellectual and Artistic Works No 5846

The Law on Intellectual and Artistic Works (focusing on the protection of copyright) also criminalises the following actions with sanctions of imprisonment between six months and two years:

- circumventing technological measures such as access control or encryption;
- breach of the protected rights of the database manufacturer; and
- continuous violation of copyrights and related rights by service and information content providers via transmission tools for signs, sounds and/or images, including digital transmission.

The Communiqué on the Procedures and Principles for Connecting to and Auditing the KamuNet Network (The "Communiqué on KamuNet")

KamuNet (loosely translated as PublicNet) is a closed-circuit, virtual network infrastructure isolated from the private network and internet environment and utilised by public institutions and organisations in their service, transaction, and data traffic transfers. Hence, it is more secure against physical and cyber-attacks. Per the Prime Ministry Decree No 2016/28 on Inte-

grating Public Institutions and Organisations into KamuNet, all public institutions and organisations must utilise the KamuNet network.

The *Communiqué* on KamuNet sets the requirements for public institutions and organisations integrated into KamuNet, such as having a TS ISO/IEC 27001 certificate for their information security management systems. In addition, it authorises the MTI to determine the public institutions and organisations to be integrated into KamuNet and assess their suitableness before the integration.

1.3 Cybersecurity Regulators

Regulators

The Cybersecurity Directorate

The Directorate has been designated as a general authority on cybersecurity matters. The main duties and powers of the Directorate are as follows:

- conducting operations to increase cyber-resilience (eg, by penetration tests or risk analysis);
- determining critical infrastructures;
- ensuring keeping of the asset inventory for public institutions and critical infrastructures;
- establishing and auditing CERTs;
- determining the procedures and principles to be followed by those operating in the field of cybersecurity;
- establishing and operating the necessary infrastructure for the cybersecurity of public institutions and critical services, providing secure hosting services, and defining the procedures and principles thereof;
- determining the standards for the cybersecurity field;
- carrying out testing and certification procedures for the cybersecurity field;
- conducting cybersecurity audits and imposing sanctions; and
- determining the technical criteria for the cybersecurity products and services to be used in public institutions and critical infrastructures.

However, the Directorate's duties will continue to be performed by the existing relevant public institutions and organisations until the relevant units within the Directorate are established and become operational.

The Ministry of Transport and Infrastructure (the MTI)

The Council of Ministers Decision on Cybersecurity authorises the MTI for the implementation, administration and co-ordination of national cybersecurity actions and preparation and co-ordination of policy, strategy and action plans regarding the governance of national cybersecurity.

MTI oversees and conducts cybersecurity activities at the strategic level through the TR-CERT.

The Cybersecurity Act delegates MTI's cybersecurity-related responsibilities to the Directory.

The Cybersecurity Board

The Cybersecurity Board, presided by the President of the Republic of Türkiye, is tasked with:

- adopting resolutions regarding cybersecurity policies, strategies, action plans, and other regulatory measures;
- adopting resolutions for the implementation of the cybersecurity technology roadmap prepared by the Directorate;
- identifying priority areas for incentives in cybersecurity;

- adopting resolutions for the development of human resources in the cybersecurity field;
- determining critical infrastructure sectors; and
- resolving the disputes between the Directorate and public institutions.

The Information and Communication Technologies Authority (the ICTA)

ICTA is an independent administrative institution and has administrative and financial autonomy.

In addition to its regulatory role in telecommunications, ICTA closely monitors cybersecurity incidents through publicly available and private forums and mediums. ICTA also audits and warns private companies concerning specific cybersecurity threats and technical vulnerabilities.

The Cybersecurity Act annuls the provisions granting the ICTA general cybersecurity-related powers and limits its duties to the data systems within its own competency. However, ICTA will continue carrying out its duties for the time being. According to the Cybersecurity Act, when the Directorate's organisation becomes fully operational, ICTA will transfer to the Directorate all its assets that are exclusively used for national cybersecurity activities.

The Digital Transformation Office (the DTO)

The DTO has played an active role in cybersecurity, big data, artificial intelligence, and digital transformation since its establishment in 2018.

The DTO was abolished with a Presidency Decree on 28 March 2025 and its cybersecurity-related duties and assets have been transferred to the Directorate.

National Cyber Incidents Response Centre (the TR-CERT)

In 2013, the TR-CERT was established under ICTA to identify emerging threats, take measures to reduce and eliminate the effects of possible attacks and incidents on national cyberspace and share them with the relevant actors.

TR-CERT oversees the management of response to cybersecurity incidents from the beginning until the resolution. It co-ordinates with CERTs who are required to report cybersecurity events to the TR-CERT.

TR-CERT also carries out awareness-raising and guidance activities to increase the awareness of public institutions and organisations against cyber-attacks.

Cyber Incidents Response Teams (CERTs)

Sectoral CERTs

Sectoral CERTs are established under:

- the regulatory and supervisory bodies; or
- the relevant ministries of critical sectors, which are:
  - (a) the Ministry of Interior;
  - (b) the Ministry of Justice;
  - (c) the Ministry of Treasury and Finance;
  - (d) the Ministry of Environment, Urbanisation and Climate Change;
  - (e) the Ministry of Labour and Social Security;
  - (f) the Ministry of Agriculture and Forestry; and
  - (g) the Ministry of Health.

Sectoral CERTs are responsible for co-ordination, regulation and supervision of cybersecurity in their respective critical sectors. They act in

co-ordination with the TR-CERT and institutional CERTs operating in the sectors concerned.

Institutional CERTs

Institutional CERTs are established within public and private organisations.

All organisations operating in the critical infrastructure sectors must establish an institutional CERT thereunder and ICTA has the authority to order a public or private organisation to establish and maintain a CERT, even if that organisation does not operate in critical infrastructure sectors.

Institutional CERTs also act in co-ordination with the TR-CERT and sectoral CERTs operating in the relevant sector, as applicable.

The Personal Data Protection Authority (the DPA)

The primary supervisory and regulatory authority for data protection matters is the DPA. It is an independent administrative institution that has administrative and financial autonomy.

The DPA is authorised to regulate data protection activities and to take measures to protect the rights of data subjects. The DPA is competent to receive data breach notices according to the DP Law.

The National Intelligence Agency

The National Intelligence Agency is entitled to collect, record, and analyse information, documents, news, and data by using any technical intelligence and human intelligence method, tool and system regarding foreign intelligence, national defence, counterterrorism, international crimes and cybersecurity, and to deliver the produced intelligence to the necessary institutions.

The Turkish National Police Department of Cybercrime Prevention

Established in 2011, this department provides support in investigating crimes committed using information technology. It gathers forensic data to fight cybercrime effectively and efficiently.

The Ministry of National Defence, the Presidency of Defence Industries, and the Turkish Armed Forces Cyber Defence Command

These entities ensure cybersecurity from the perspective of military and national defence.

The Ministry of Interior Disaster and Emergency Management Presidency

The Ministry of Interior Disaster and Emergency Management Presidency is responsible for crisis co-ordination and management to protect critical infrastructures in the event of a disaster.

Others

Apart from the above, sector-specific administrative institutions such as the Banking Regulation and Supervision of Agency (the BRSA), the Capital Markets Board (the CMB), the Turkish Republic Central Bank (the TRCB), the Energy Market Regulatory Authority (the EMRA), the General Directorate of Civil Aviation (the GDCA), and the Nuclear Regulatory Authority are entitled to regulate cybersecurity-related issues in their respective sectors.

2. Critical Infrastructure Cybersecurity

2.1 Scope of Critical Infrastructure Cybersecurity Regulation

General

There is no framework legislation on critical infrastructure cybersecurity like the EU's NIS2

or the USA's Cyber Incident Reporting for Critical Infrastructure Act. However, enacting regulations in line with the EU's *"NIS2 Directive"* is a policy goal identified by the 12th Development Program.

The Cybersecurity Act delegates to the Directorate and the Cybersecurity Board the duty to determine critical infrastructures and the organisations and locations to which they belong. Currently, there is no precise scope for critical infrastructure cybersecurity regulation, and the relevant sectoral legislation must be consulted. The applicable legal texts are policy documents published by authorised institutions and sector-specific by-laws.

The DTO's Information and Communication Security Guide (the "ICS Guide")

The ICS Guide published by DTO defines *"critical infrastructure"* as *"infrastructures that incorporate information technologies which may cause loss of life, economic harm of large-scale, national security gaps and public disorder when the confidentiality, integrity and availability of data/information therein are disrupted"*.

The ICS Guide applies to public institutions, organisations and businesses providing critical infrastructure services. It sets out general security measures and those specific to the energy and e-communication sectors. The ICS Guide defines, among other things, the asset groups (eg, network and systems, apps, devices, physical places, and personnel), their criticality level, measures, the application process, and their respective compliance plan.

Guidance of the MTI

The MTI is tasked with identifying critical infrastructures along with the institutions they belong to and their locations. (However, this duty will be transferred to the Directorate when it is operational.) There are six critical infrastructure sectors:

- e-communications;
- energy;
- finance;
- transport;
- water management; and
- critical public services.

The Sectoral CERT Guideline published by the MTI defines critical public services as services provided by critical systems with which citizens frequently interact, and mentions the following:

- civil registration;
- land registration;
- taxation;
- commerce;
- social security;
- health (emergency services, medical services, blood and organ donation and public health);
- food;
- security (police, *gendarmerie,* – a police force that is part of the armed forces in Türkiye that is affiliated to the Ministry of Interior and carries out duties related to safety, public order and security assigned to it by certain laws and regulations – and coast guard);
- roads and bridges;
- dams; and
- services provided via critical systems where salary and judicial transactions are performed and their records are kept.

The MTI also published: *"Document for Minimum Security Measures for Critical Information System Infrastructure"* and *"Minimum Information Security Criteria for Public Institutions to Comply"*.

E-Communications

The By-Law on NIS in the E-Communications Sector is the main regulation for the e-communications sector, with the purpose to provide the procedures and principles of operators to ensure network and information security. It applies to the operators within the scope of the E-Communications Law.

Energy

The main regulation on cybersecurity in the energy sector is the By-Law on Cybersecurity Competency Model in the Energy Sector. It aims to improve cybersecurity and define the minimum acceptable level of security of industrial control systems used in the energy sector, and establish the procedures and principles related to the cyber-resilience, proficiency, and maturity thereof.

The By-Law covers industrial control systems owned by legal entities with the following licences: electricity transmission licence, electricity distribution licence, electricity generation facility licence, natural gas transmission licence for pipeline transmission, natural gas distribution licence, natural gas storage licence (LNG, underground), crude oil transmission licence, and refinery licence.

Banking and Finance

By-Law on Information Systems of Banks and Electronic Banking Services aims to manage information systems used by banks in the performance of their operations and set forth the minimum procedures and principles to be applied in the offer of electronic banking services and management of risks related thereto. It covers the entities falling within the scope of the Banking Law (eg, deposit and participation banks, branches of foreign institutions within Türkiye, etc).

2.2 Critical Infrastructure Cybersecurity Requirements

General

According to the Cybersecurity Act, one of the duties of the Directorate is to determine technical criteria for cybersecurity products and services to be used in public institutions and critical infrastructures. However, these criteria are not determined yet as the Directorate has not become fully operational.

The Presidency Decree provides the following security measures for critical infrastructure security of public institutions and organisations:

- conducting security clearances for personnel of critical importance; and
- requiring communication service providers to establish internet exchange points in Türkiye.

For comprehensive measures, the Presidency Decree refers to the ICS Guide, which provides the following for critical infrastructure security in public institutions and organisations and businesses providing critical infrastructure services:

- network and system security measures (eg, protection against malware, penetration tests, and cybersecurity management);
- application and data security measures (eg, secure software development, error handling and log management, and database and record management);
- portable device and media security measures (eg, securing smartphones and tablets, portable computers and portable media);
- IoT devices security measures (eg, internal data storage, authentication and authorisation, and API and connectivity security);
- personnel security measures (eg, training and awareness programmes, and suppliers' relationship security); and

- physical environment security measures (eg, protection of server room/data centre, and protection against electromagnetic information leakage (TEMPEST)).

The ICS Guide also sets out sector-specific security measures for e-communications and energy sectors. Additionally, there are other sector-specific regulations setting the requirements for critical infrastructure cybersecurity. Refer to the details of the sector-specific regulations below.

E-Communications Sector

Security measures to be taken by the actors in the e-communications sector in accordance with the ICS Guide are as follows:

- service security and continuity;
- infrastructure services security;
- fraud detection and prevention;
- signalling traffic security;
- establishing trusted communication;
- hardening activities;
- monitoring equipment failures;
- ensuring equipment security;
- threat intelligence management;
- communication with authorities;
- prevention of caller ID manipulation; and
- ensuring that domestic communication traffic remains within the country.

The By-Law on NIS in the E-Communications Sector requires that a report on NIS must be prepared by the operator every year – until the end of March – and kept for five years to be sent to ICTA upon request and/or submitted during the inspections made by ICTA. The report includes information such as:

- risk assessment and processing methods, and details of transactions made according to these methods;
- business continuity plans; and
- details on information security breach incidents that have occurred.

Per the By-Law, operators cannot allow unlicensed software and software going against Information Security Management Systems Policy rules and must take measures to protect information and software against harmful codes and identify security measures for downloading files or software via external networks.

Operators are also obligated to define and document rules related to the transfer of software from the development environment to the production environment.

Energy Sector

The actors in the energy sector must take the following security measures per the ICS Guide:

- device configurations;
- network access control;
- authentication;
- access management;
- physical access security;
- ensuring system continuity;
- prevention of data manipulation;
- user access management;
- SSL/TLS protected communication;
- security of GPS communication and synchronisation;
- ensuring equipment security;
- threat intelligence management;
- communication with authorities; and
- using safe methods for data transmission.

The competency model under the By-Law on Cybersecurity Competency Model in the Energy

Sector sets out three basic competency levels. The applicable competency level will be identified with sectoral criticality degrees determined by the EMRA. The obligated organisations must implement the competency model after EMRA determines the respective criticality degrees and notifies them.

Banking and Finance Sector

Banks and other financial institutions under the authority of the BRSA must take the measures outlined in the By-Law on Information Systems of Banks and Electronic Banking Services.

Moreover, personal data specific to banking relationships are also considered customer secrets under the Banking Law. For specific requirements and restrictions thereto, see **3. Financial Sector Operational Resilience Regulation**.

Health Sector

See **6.3 Cybersecurity in the Healthcare Sector**.

Civil Aviation Sector

The Cybersecurity Directive for Civil Aviation Enterprises (the *"Directive"*) outlines the following measures to be taken by civil aviation enterprises against cyber threats:

- effective oversight of use of information systems;
- regular cybersecurity risk and threat assessments for operational assets;
- implementation of policies, procedures, and process documents;
- mechanisms to detect, prevent, and respond to potential cybersecurity breaches;
- testing, auditing, and monitoring cybersecurity controls and structures, and reporting the results; and
- developing a continuity management process and continuity plan for IT systems to ensure critical cybersecurity processes remain operational.

2.3 Incident Response and Notification Obligations

General Notification Duties

One of the main obligations provided under the Presidency Decree for public institutions is adopting the necessary measures regarding cyber threat notifications.

"cybersecurity event" is defined in the *Communiqué* on CERTs as *"breach or attempted breach of confidentiality, integrity, or accessibility of industrial control or information systems or data processed thereby"*. If an organisation is required to establish a CERT, in principle, its CERT must report any cybersecurity event to the TR-CERT and the relevant sectoral CERT (if applicable). See **1.3 Cybersecurity Regulators** for more details.

Conversely, an organisation that is not required to establish a CERT, is not under obligation to report (although, voluntary reporting is allowed).

In addition, when the Directorate becomes operational, institutions and persons using information systems will be required to notify the Directorate of any vulnerability or cyber incidents that they detect in their service area. Also, those who fail to fulfil their duties and responsibilities by not reporting cyber incidents and vulnerabilities to the Directorate will be subject to an administrative fine between TRY1 million and TRY10 million.

Personal Data Breach Notification to the DPA

Controllers must report to the DPA within 72 hours and notify the relevant data subjects within the shortest time possible if third parties unlawfully acquire personal data (regardless of

the likelihood or lack thereof to result in a risk to the rights and freedoms of natural persons).

Sectoral Notification Duties

- In the e-communications sector, the By-Law on NIS in the E-Communication Sector requires the operator to notify ICTA regarding network and information security breaches that affect more than 5% of its subscribers and the circumstances that interrupt the continuity of the business. The notification must include, as a minimum, the time, nature, impact and duration of the breach, as well as the measures taken.
- In the banking sector, the By-Law on Information Systems of Banks and Electronic Banking Services (the *"By-Law ISBEBS"*) requires banks to report cyber-events to the BRSA.
- A cyber-attack affecting a public company must be disclosed to the public as per the *Communiqué* on Material Events Disclosure.
- In the healthcare sector, as per the Directive on the Information Security Policies of the Ministry of Health, all information security breach incidents related to the Ministry of Health must be submitted to the central breach notification system thereof.

2.4 State Responsibilities and Obligations

For the allocation of duties and the details thereof, see **1.3 Cybersecurity Regulators**. See also **2.1 Scope of Critical Infrastructure Cybersecurity Regulation** and **2.2 Critical Infrastructure Cybersecurity Requirements** for obligations provided for public institutions under the ICS Guide.

3. Financial Sector Operational Resilience Regulation

3.1 Scope of Financial Sector Operational Resilience Regulation

There is no general legislation covering the Turkish financial sector's operational resilience. Rather, relevant regulations of the BRSA, TRCB and CMB set the rules on the management of information systems for banks, payment and electronic money institutions, and capital market institutions respectively.

- The information systems of banks are regulated by By-Law ISBEBS. It applies to deposit banks, participation banks, development and investment banks established in Türkiye and the Turkish branches of such foreign banks.
- The information systems of payment institutions and electronic money institutions are regulated by the *Communiqué* on Data-Sharing Services in the Payment Services Area of Payment and Electronic Money Institutions' Information Systems and Payment Service Providers (the *"Communiqué on Payment Services"*). The *Communiqué* covers payment institutions and electronic money institutions, which consist of an exhaustive list of institutions that are authorised by the TRCB in accordance with the Law on Payment and Securities Settlement Systems, Payment Services, and Electronic Money Institutions.
- The CMB has a *Communiqué* on Information Systems Management (The *"CMB Communiqué"*). This *Communiqué* concerns stock exchanges and market operators and other organised marketplaces, publicly held corporations, and capital market institutions (eg, investment firms, collective investment schemes, portfolio management companies, and cryptocurrency service providers), among others. This *Communiqué* was superseded

by another *Communiqué* (The *"New CMB-Communiqué"*) that will take effect on 30 June 2025. The new *Communiqué* will cover crypto-asset service providers as well.

3.2 ICT Service Provider Contractual Requirements

There is no legal definition for ICT service providers or cloud service providers. However, several sectoral regulations indicate different service providers for ICT services. Since they are regulated sectorally, there is no general classification of critical ICT services either.

The By-Law ISBEBS, the Communiqué on Payment Services, and the CMB Communiqué (collectively, the *"Financial NIS"*)

The Financial NIS regulates the outsourcing of ICT services by the institutions it covers. Thus, it includes provisions concerning the financial sector institutions' outsourced information systems services.

The Financial NIS aims to guarantee that financial sector institutions retain their control over even the outsourced information systems and for them to remain accountable to the relevant parties (eg, their customers). For the scope of Financial NIS, see **3.1 Scope of Financial Sector Operation Resilience Regulation**.

The By-Law ISBEBS defines *"outsourcing"* as support services that banks acquire from external sources, which may potentially affect the confidentiality, integrity, and availability of banking data, continuity of banking services, and services involving access to or sharing of banking data.

Banks must also follow the conditions set under the By-Law on Support Services for Banks, which covers the banks' outsourcing of any type of support services.

Outsourcing contracts must include certain clauses, including:

- the scope of the contract and the responsibilities of the parties;
- the liability of the external outsourcing provider with regard to information security;
- the liability of the sub-contractors of the outsourcing provider, which must be equivalent to thereof; and
- terms for changes and termination.

Classification of ICT Services

The Financial NIS does not define any ICT services as *"critical"*.

The By-Law ISBEBS and the *Communiqué* on Payment Services mention additional requirements for *"critical information systems"* without providing any definition. However, the By-Law on Remote Identity Verification Methods to be Used by Banks and the Establishment of Contractual Relationships in Electronic Environment classifies the systems used in the context of remote identity verification as critical information systems in terms of the By-Law ISBEBS.

The New CMB *Communiqué* (taking effect on 30 June 2025) does not define *"critical information systems"* either. However, it defines *"criticality"* as *"the quality of the information asset that indicates its importance or necessity in achieving the business objectives of the institution, organisation or company"*. It also sets additional requirements for critical information systems, such as establishing mechanisms to instantly monitor unauthorised access attempts.

3.3 Key Operational Resilience Obligations

As outlined above, there is no overarching digital operation resilience regulation, and the applicable legal requirements are fragmented across several legislative pieces.

The Financial NIS imposes several obligations on the institutions of their respective areas to increase the resilience of financial sector institutions' information systems. Financial NIS aims to establish the standards for strengthening these systems. It provides measures to be taken for information security as well as the management of cyber incidents.

Localisation Obligations

The following entities must keep their primary and secondary information systems in Türkiye:

- banks;
- payment institutions and electronic money institutions;
- insurance and private pension companies (except for services such as email, teleconference or videoconference);
- certain public companies, as well as certain capital markets institutions; and
- financial lease, factoring and finance companies.

For outsourced products or services, the *Communiqué* on Payment Services requires use of local products, or the manufacturers thereof to have R&D centres and response centres in Türkiye.

Risk Management Obligations

Financial sector institutions are required to prepare a plan and policy for the detection, analysis, and management of risks related to information systems. They also impose internal control mechanisms for the same (eg, approval of senior staff).

Cyber Incident Management and Reporting Obligations

The measures to be taken in the event of a cyber incident include keeping a detailed record thereof, preventing the recurrence of a similar incident, establishing internal mechanisms for cyber incident management, and identifying the root causes of cyber incidents.

Certain details of cyber incidents must be reported to the internal senior staff as well as the relevant institutions (eg, the BRSA, TRCB and Institutional CERTs). Additionally, since the financial sector is one of the critical infrastructure sectors, financial sector institutions must also follow the notification obligations mentioned in **2.3 Incident Response and Notification Obligations**.

Other Obligations

For other crucial obligations see **3.2 ICT Service Provider Contractual Requirements**, **3.5 International Data Transfers** and **3.6 Threat-Led Penetration Testing**.

3.4 Operational Resilience Enforcement

The enforcement of the operational resilience obligations outlined above is shared by the BRSA, TRCB, and CMB.

The Banking Regulation and Supervision of Agency (the BRSA)

The BRSA is authorised to carry out examination of all books, records, and documents, and conduct on-site audits and ex officio inspections concerning the support service organisations.

The By-Law ISBEBS also authorises BSRA to carry out inspections concerning the ICT providers of banks and requires them to provide the

necessary information and documents requested and to keep and operate all kinds of records in a readable format.

Moreover, BSRA is authorised to impose administrative fines in case of non-compliance with its regulations in accordance with the Banking Law.

The Turkish Republic Central Bank (the TRCB)

The TRCB is authorised to audit banks, payment institutions, electronic money institutions, and their branches, representatives or outsourced service providers of the Post and Telegraph Organisation A.Ş.

The TRCB may request the payment institution and electronic money institution to take the necessary measures in relation to the issues identified. In case of failure to take these measures in a reasonable time, TRCB may revoke the operating licence.

Depending on the case, TRCB may impose a wide range of administrative fines for non-compliance with the regulations on payment services and electronic money institutions.

The Capital Markets Board (the CMB)

The CMB has the authority to audit the activities concerning capital markets of all institutions and organisations under the scope of the Capital Markets Law and other relevant real or legal persons. The auditing personnel may request relevant documents and information. The failure to provide these and obscuring the audit are criminalised under the Capital Markets Law.

Depending on the case, CMB may impose a wide range of administrative fines on persons who fail to comply with the Capital Markets Law and its secondary legislation.

3.5 International Data Transfers

Banking Law and Its Secondary Legislation

Refer to the localisation obligation under **3.3 Key Operational Resilience Obligations**.

Additionally, customer secrets under the Banking Law cannot be disclosed or transferred to foreign (or domestic) third parties without receiving the customer's request or explicit instruction. There are two exceptions.

- Customer secrets can be transferred to authorities that are authorised by Turkish laws.
- Information and documents may be shared to the parent company located abroad, provided that its capital share equals to or exceeds ten percent, and a non-disclosure agreement is signed with the parent company. Even then, only the following information may be shared – preparation of consolidated financial statements, risk management, and internal audit practices.

The By-Law on the Sharing of Secret Information, which applies to bank secrets and customer secrets collectively, also provides exceptions to the prohibition to share secret information. Accordingly, the following transfers are allowed.

- Per a BoD decision to be adopted by the bank, sharing with third parties bank secrets that only contain classified information belonging to the bank.
- The disclosures made to the foreign judicial and alternative dispute resolution authorities or to the parties representing the bank in such disputes, where the disclosure is necessary for the proof of the claim or defence.

The Communiqué on Payment Services

In cases where one of the parties of the payment transaction is located abroad, the institution may share the required data with the relevant third parties abroad. However, the following conditions must be satisfied:

- data must be stored domestically;
- data must be limited to the extent necessary for the performance; and
- the principle of proportionality must be respected.

General DP Law Regime on International Personal Data Transfers

If data transferred is personal data, the DP Law also applies.

Provisions on international personal data transfers under the DP Law have been significantly amended on 12 March 2024, effective from 1 September 2024. The purpose of the amendment was to align the DP Law with the General Data Protection Regulation.

The new regime allows personal data to be transferred abroad or to international organisations under the following conditions.

- Existence of one of the applicable legal bases under the DP Law and an adequacy decision for the country, international organisation or the sectors therein to which the data will be transferred (note that, as of the date of this publication, the DPA has not issued any adequacy decision yet).
- In the absence of an adequacy decision – the existence of one of the applicable legal bases under the DP Law and enforceable data subject rights and effective legal remedies for data subjects and provision of one of the following appropriate safeguards:
  - (a) a legally binding and enforceable instrument between public authorities or bodies;
  - (b) binding corporate rules;
  - (c) standard contractual clauses; or
  - (d) a written letter of commitment, together with the approval of the transfer by the Board.
- In the absence of an adequacy decision and where appropriate safeguards cannot be provided – the existence of derogations for specific situations outlined in the DP Law, where the transfer is *"occasional"*.

Although the DPA published the By-Law on Procedures for the Transfer of Personal Data Abroad and a guideline, there are many ongoing discussions on interpreting the provisions therein.

Besides the amendments, there is an unaltered provision under the DP Law, which provides a reservation for provisions under other laws applying to personal data transfers abroad. In the Banking Sector Best Practices Guide on the Protection of Personal Data, the DPA states that where such a specific provision is applicable, it will override the transfer regime under the DP Law.

The provisions explicitly mentioned in the Banking Guide are those on *"consumer secrets"* under the Banking Law and related secondary regulations. Although not explicitly mentioned, Article 24 under the By-Law on Measures for Preventing Money Laundering and Financing of Terrorism, which provides the minimum information to be included in an international e-transfer, will also apply in a preceding manner.

International Treaties

International treaties to which Türkiye is a party may allow or require banks to transfer data

abroad under some conditions (eg, the Agreement Between the Government of the Republic of Türkiye and the Government of the United States of America to Improve International Tax Compliance requires Turkish financial institutions to report US citizens and residents' data for tax compliance purposes). In these cases, the treaties will have precedence over the local laws according to Article 90(3) of the Constitution. If the transferred data is personal data, the reservation under the DP Law may also be applicable.

3.6 Threat-Led Penetration Testing

The Financial NIS imposes penetration testing obligations for their respective financial sector institutions as detailed below.

The By-Law ISBEBS

Banks must have penetration tests performed at least once a year by independent teams that are not involved in the design, development, implementation or execution of the services provided through information systems.

The Institutional CERTs of banks are also required to conduct routine penetration tests on IT assets, routinely monitor trace records and check for correlations that may lead to meaningful results.

The Communiqué on Payment Services

The *Communiqué* provides the following penetration testing requirements for payment and electronic money institutions.

- They must have regular penetration tests performed at least once a year for scenarios covering possible internal and external threats. The procedure to be followed for penetration testing is provided under the Annex 5 therein.
- They must submit a report to TRCB at least annually, detailing security breaches, penetration test results, and critical vulnerabilities identified, measures taken to eliminate them and the results thereof.

The CMB Communiqué

The information systems of the related institutions and organisations must have penetration tests performed at least once a year. The procedure to be followed for penetration testing is provided under the Annex 1 therein.

4. Cyber-Resilience

4.1 Cyber-Resilience Legislation

There is no general legislative instrument on cyber resilience in Türkiye.

Currently, the main regulations on managing cyber incidents are the *Communiqué* on the Procedures and Principles Regarding the Establishment, Duties and Activities of CERTs and MTI's guidelines on establishing institutional and sectoral CERTs. For further information on CERTs, see **1.3 Cybersecurity Regulators**.

However, the Presidency Program for 2025 includes a plan to enact legislative regulations in line with the EU's Cyber Resilience Act (CRA). It is possible to expect a cyber resilience regulation in the following years, since cyber resilience is listed as one of the six main objectives of the NCS 2024. In this regard, *"establishing principles to mitigate the possible impacts of cyber incidents"* objective of the Cybersecurity Act indicates at cyber resilience.

According to the Cybersecurity Act, cybersecurity *"encompasses a set of activities aimed at protecting from attacks the information systems that constitute cyberspace, ensuring the confidentiality, integrity, and availability of data processed*

therein, detecting attacks and cyber incidents, activating response and alert mechanisms, and restoring the situation to its state prior to the cyber incident". The last part of this definition seems to include cyber resilience thereunder.

4.2 Key Obligations Under Legislation

The Cybersecurity Act delegates a specific duty to the Cybersecurity Directorate for *"increasing the cyber resilience of critical infrastructures and information systems through vulnerability and penetration tests and risk analysis, cyber-threat intelligence, and malware inspection operations"*.

Currently, the Institutional CERTs are subject to the following resilience-related obligations during and after a cyber incident:

- carrying out their activities to prevent cyber incidents or mitigate damages in co-ordination with their sectoral CERTs, if any.
- notifying the TR-CERT of the situation without delay;
- reporting cyber incidents to their institutions, notifying the TR-CERT and their sectoral CERTs without delay;
- primarily trying to eliminate a cyber incident with their own means and capabilities, and requesting assistance from the TR-CERT and their sectoral CERT, as applicable;
- reporting to the competent authorities and the TR-CERT without delay, if there is doubt that a crime has been committed during the intervention of a cyber incident;
- having 24/7-accessible contact information and notifying their sectoral CERTs and the TR-CERT thereof;
- identifying and keeping record of the vulnerability that led to the incident immediately;
- measuring and monitoring the types, quantities and costs of cyber incidents; and
- submitting to the management of the institution for corrective/preventive actions that can be taken in relation to the incident.

The Sectoral CERTs, on the other hand, have the following obligations:

- carrying out activities for preventing cyber incidents or mitigating their damages in co-ordination with the TR-CERT;
- notifying the TR-CERT of cyber incidents experienced by their CERTs without delay;
- having 24/7-accessible contact information and notifying their CERTs and the TR-CERT thereof;
- supporting their CERTs in cyber incidents; and
- reporting to the competent authorities and the TR-CERT without delay, if there is doubt that a crime has been committed during the intervention of a cyber incident.

5. Security Certification for ICT Products, Services and Processes

5.1 Key Cybersecurity Certification Legislation

Currently, there is no general legal framework for certification requirements of ICT products and services. However, there are sector-specific legislation with certification requirements.

The Cybersecurity Act provides certain certification requirements. According to the Cybersecurity Act, cybersecurity products, systems and services to be used in public institutions and organisations and critical infrastructures have to be procured from cybersecurity experts and companies who will be certified by the Cybersecurity Directorate. Procurement from uncertified experts or companies will be subject to an

administrative fine between TRY1 million and TRY10 million.

TS ISO/IEC 27001 Certificate

In the e-communications and energy sector, and for e-invoice service providers, obtaining a TS ISO/IEC 27001 certificate is a de jure standard. However, many other organisations also choose to voluntarily comply with this standard as a good practice to improve cybersecurity.

The Financial Sector

- The BRSA requires all banks to meet Control Objectives for Information and Related Technologies (COBIT) standards. COBIT process management is used not only in banks but also in the finance and production sectors.
- The By-Law on Banking Cards and Credit Cards require organisations entering into merchant agreements with banks to comply with the Payment Card Industry Data Security Standards (PCI DSS) standards.
- According to the CMB's *Communiqué* on Independence Audit of Information Systems, auditors who audit publicly held companies must have a Certified Information System Auditor (CISA) certificate.

The Healthcare Sector

The By-Law on Health Information Management Systems requires health information systems' service providers to have following certificates:

- TS ISO/IEC 27001;
- TS ISO/IEC 15504 Software Process Improvement and Capability Determination (SPICE) certificate at a minimum of the second level, which is obtained from institutions and organisations with TS ISO/IEC 17065 accreditation and include SPICE lead auditor; or
- CMMI certificate at a minimum of the third level, which is obtained from institutions or companies with CMMI lead auditor.

6. Cybersecurity in Other Regulations

6.1 Cybersecurity and Data Protection

Data controllers are obliged to provide an appropriate level of security for the personal data they process. Hence, data controllers must ensure that their processors provide a level of security for personal data that is, at minimum, equivalent to their own. Data controllers are also held liable for the security measures taken by data processors. They may conduct or commission the necessary audits on their processors' systems containing personal data, review the results, and inspect the data processor on-site.

The DPA issued the Guideline on Personal Data Protection (Technical and Organisational Measures) (the *"Measures Guideline"*) in 2018, which lists and details the technical and administrative measures to be taken by data controllers. The guideline suggests the following cybersecurity-related measures:

- using a firewall and internet gateway;
- patch management;
- software updates;
- limiting access to systems containing personal data;
- using strong passwords for such systems;
- creating an access control matrix;
- using brute force algorithm (BFA);
- using antivirus, antispam and similar products that regularly scan the information system network and detect potential threats; and

- using SSL or more secure methods for data collection from different websites and/or mobile application channels.

There are stricter requirements for the processing of special categories of data per the DPA Decision No 2018/10. The DPA may also specify case-specific measures in its published decisions.

Administrative fines for failure to take necessary technical and organisational measures (interpreted very broadly, including unlawful data transfer abroad and violation of fundamental principles) range between TRY204,285 and TRY13,620,402 for 2025.

Also refer to the data breach notification duty explained under **2.3 Incident Response and Notification Obligations**, where failing to comply with this obligation results in a data breach.

6.2 Cybersecurity and AI

Currently, there is no legislation in Türkiye regulating AI or providing obligations regarding AI.

However, on 5 October 2024, the Turkish Parliament published a decision on the establishment of a parliamentary research commission to determine the steps to be taken toward the achievements of AI, to establish a legal infrastructure in this field and to determine measures to prevent the risks of the use of AI. Members of this commission were elected recently. However, there is no public information on the progress of the commission's work.

In addition, a proposal for an AI Act was submitted to parliament on 25 June 2024. The proposal included provisions on risk management in production and use of AI and auditing AI operators. Although its approval is unlikely, it marks a significant milestone as the first legislative initiative in this field.

The DTO's National Artificial Intelligence Strategy for 2021–2025

The strategy is a framework document outlining strategic priorities, goals and measures. The strategic priorities are as follows:

- training AI experts and increasing employment in the field of AI;
- supporting research, entrepreneurship and innovation;
- broadening access opportunities to quality data and technical infrastructure;
- taking regulatory actions to expedite socio-economic compliance;
- strengthening co-operation at the international level; and
- expediting structural and workforce transformation.

The Action Plan of National Artificial Intelligence Strategy for 2024–2025 includes the following:

- improving the data governance regulations in the AI ecosystem;
- enacting a national regulation on the development and use of AI systems and the market supply of systems containing AI, which follows international norms;
- preparing a Legal Evaluation Guide for AI Applications; and
- developing an AI Values and Principles Impact Analysis Framework.

There are recommended security measures concerning AI under the following documents:

The DTO's Report on Chatbot Applications and the Case of ChatGPT

The report provides information on security risks and methods to reduce them. These methods include:

- authentication and authorisation;
- end-to-end encryption;
- self-deleting messages;
- configuration of user control and access rights; and
- proper storage of chat history.

Recommendations by the DPA

The DPA's informational document on chatbots highlights:

- the importance of transparency in AI chatbot applications;
- the potential risks, such as over-sharing of personal data by the data subjects and cyber incidents; and
- the need for special protection for minors.

The following measures are suggested to be taken while developing a chatbot application:

- complying with internationally recognised standards, having certificates, and ensuring privacy by default at every stage in the development process thereof; and
- in data communication, preferring secure methods for transmitting inputs such as text, voice, speech and images to the hosting environments.

Finally, the DPA's *"Recommendations on Data Protection in the Context of Artificial Intelligence"* consists of data protection-related recommendations for developers, producers, service providers, and decision-makers vis-à-vis AI systems.

6.3 Cybersecurity in the Healthcare Sector

The Directive on the Information Security Policies of the Ministry of Health (*"MoH InfoSec Directive"*) and the Guideline for Information Security Policies (*"MoH InfoSec Guideline"*)

The MoH InfoSec Directive and MoH InfoSec Guideline were published by Health Information Systems General Directorate (HISGD) under the Ministry of Health, which was established to regulate information systems and communication technologies that are used in the healthcare sector.

MoH InfoSec Directive establishes the Information Security Management Commission and sub-commissions that are responsible for information security and cyber incident management across all central and provincial organisations of the Ministry of Health.

It also establishes the sectoral CERT for the healthcare sector and requires the appointment of an information security officer. Moreover, the MoH InfoSec Directive tasks HISGD with the management of information security breaches and auditing information security.

For details of the certification obligation for service providers of health information systems, see **5.1 Key Cybersecurity Certification Legislation**.

The By-Law on Personal Health Data

In addition to the provisions under the DP Law pertaining to special categories of personal data, the By-Law on Personal Health Data provides the specific procedure to be followed by healthcare providers while processing health data.

It covers accessing, securing, rectifying, destroying, and transferring health data. It emphasises

the data security measures required by the DP Law and requires taking the information security measures under the MoH InfoSec Directive. In addition, using KamuNet to transfer health data – where technical infrastructure allows – is required.

The Guide on Protection of Personal Data in Pharmacovigilance Activities

Health data is also protected in the context of the R&D process of medicines. In this regard, the Turkish Medicines and Medical Devices Agency published the Guide on Protection of Personal Data in Pharmacovigilance Activities. It specifies the technical and organisational measures for the security of the data processed in pharmacovigilance activities, such as:

- personnel training for the first intervention regarding cybersecurity;
- setting up a firewall;
- using an internet gateway;
- using antivirus and antispam software;
- removing software with vulnerabilities and unused software;
- patch management and software updates;
- limiting access to systems containing personal data;
- checking which software and services are running on information networks;
- determining whether there is penetration or unexpected movements in information networks;
- keeping a regular record of all users' activity (such as log records);
- establishing an official reporting procedure for security issues;
- reporting security issues to the data controller as quickly as possible;
- collecting and storing evidence in case of cyber incidents;
- preferring to use internationally recognised encryption programs;
- ensuring security of environments containing personal data; and
- taking measures such as 2FA and encrypting with cryptographic methods in case of storing in a cloud.

CHAMBERS GLOBAL PRACTICE GUIDES

Chambers Global Practice Guides bring you up-to-date, expert legal commentary on the main practice areas from around the globe. Focusing on the practical legal issues affecting businesses, the guides enable readers to compare legislation and procedure and read trend forecasts from legal experts from across key jurisdictions.

To find out more information about how we select contributors, email Rob.Thomson@chambers.com