Chambers AND PARTNERS

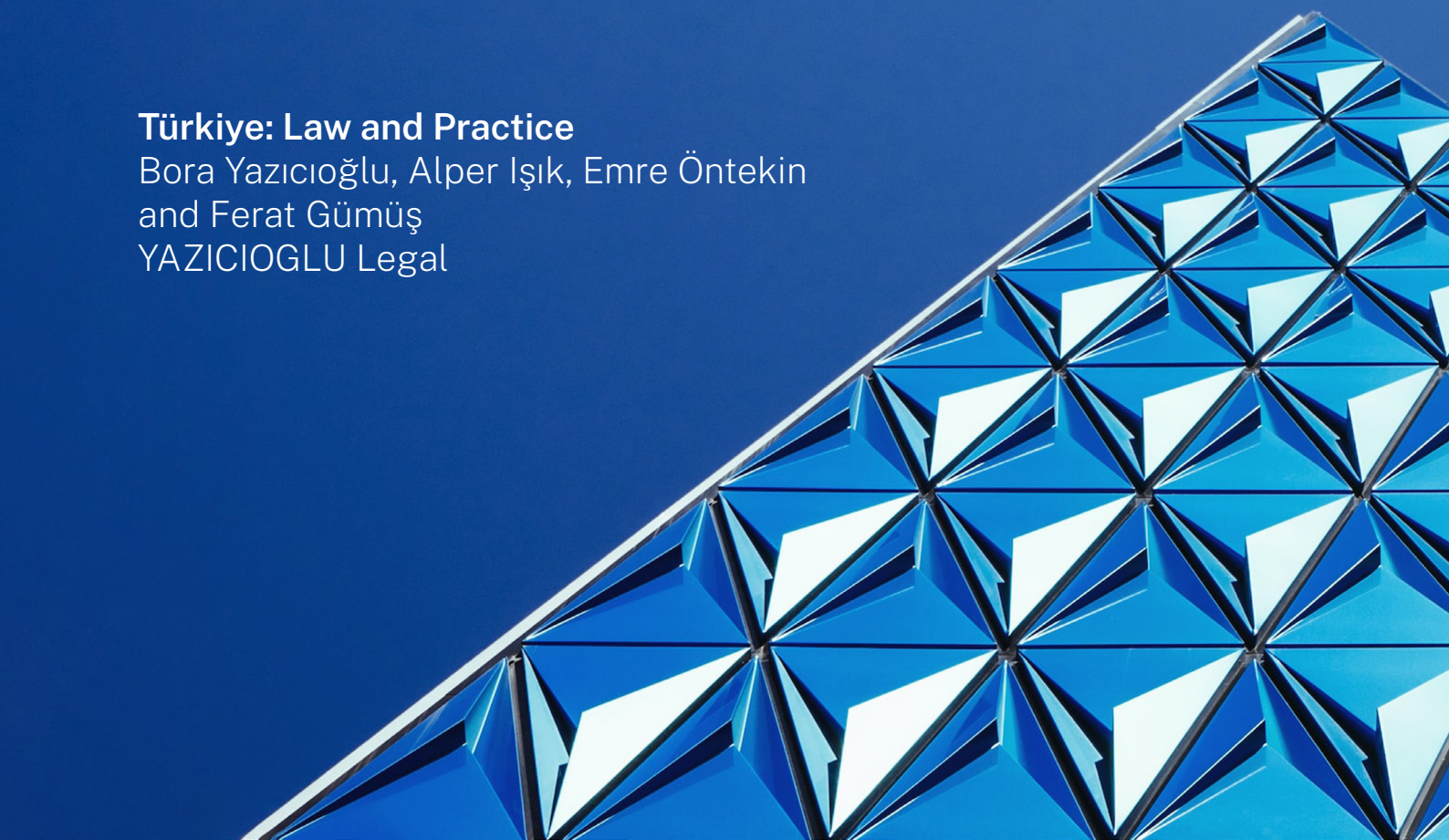
CHAMBERS GLOBAL PRACTICE GUIDES

Cybersecurity 2026

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

Türkiye: Law and Practice

Bora Yazıcıoğlu, Alper Işık, Emre Öntekin and Ferat Gümüş
YAZICIOGLU Legal



TÜRKIYE

Law and Practice

Contributed by:
Bora Yazıcıoğlu, Alper Işık, Emre Öntekin and Ferat Gümüş
YAZICIOGLU Legal

Contents

YAZICIOGLU Legal is an Istanbul-based boutique technology law firm, focusing on legal matters related to technology, media and 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 17 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 in investigations and data breaches before the Turkish Data Protection Authority. It also provides assistance to local and international clients, including Acer, Reddit and Workday, on ensuring compliance with data protection legislation, particularly in cross-border data transfers. The firm is a Bronze Corporate Member of the International Association of Privacy Professionals (IAPP).

Authors

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

Alper Işık is a counsel at Yazıcıoğlu Legal, and an associate professor of public law and faculty member in the Department of Public Law at Istanbul Medeniyet University Faculty of Law. He specialises in personal data protection law, e-commerce law, cybersecurity law and public law.

Emre Öntekin is a senior associate at Yazıcıoğlu Legal. He focuses on various areas of law, including data protection law, e-commerce law, consumer law, commercial law, administrative law, criminal law and dispute resolution.

Ferat Gümüş is an associate at YAZICIOGLU Legal. He focuses on various areas of law, including data protection, cybersecurity, e-commerce, contracts law and consumer protection law.

YAZICIOGLU Legal

NidaKule – Goztepe,
Merdivenköy Mahallesi Bora Sokak No:1
Kat:7 34732 Kadıköy
İstanbul
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 over 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 globally and awarded a full score in all areas of strength.

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

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

- cyber-resilience;
- proactive cyber-defence and deterrence;
- a 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 Programme (2024–2028)

The 12th Development Programme sets out the following general policy goals for information technologies, as well as sector-specific policies:

- strategic, regulatory and technological efforts to ensure national cybersecurity and strengthen institutional structures;
- updating national strategies in the context of new-generation cyber threats and technological developments;
- enacting regulations in line with the EU's "NIS 2 Directive" and the best international practices;
- administrative structuring for high-level co-ordination of national cybersecurity activities;
- strengthening threat intelligence through AI and big data analytics;
- strengthening the national cybersecurity infrastructure;
- enacting procedures and principles on the establishment of an information security system in critical infrastructures;
- introducing cybersecurity standards;
- improving the domestic cybersecurity ecosystem;
- supporting the global competitiveness of domestic solutions;
- developing test infrastructures for cybersecurity;
- increasing the use of domestic cybersecurity products;
- expanding cybersecurity awareness, workforce training and new business models, and building programmes to that end; and
- improving the content, quality and environment for training personnel.

The Medium-Term Programme (2025–2027)

The Medium-Term Programme provides the following policy objectives:

- fully utilising digital technologies to strengthen cybersecurity through policies, to enhance the efficiency of public administration, and to develop public services;
- enacting dedicated legislation on cybersecurity and secondary regulations in line with the relevant EU legislation;
- implementing public–university–private sector co-operation programmes to train qualified personnel in strategic fields, including cybersecurity; and
- enhancing resilience in payment and electronic institutions' cybersecurity.

The Presidency Programme for 2026

The Presidency Programme for 2026 sets out more specific plans based upon the six objectives set out in the NCS 2024, including:

- legislative works in line with the EU legal framework;
- enhancement of technical infrastructure to counter cybercrime;
- development of domestic cybersecurity solutions;
- defining roles and qualifications for cybersecurity professionals;

- reporting on strategies to expand the qualified cybersecurity workforce; and
- expanding cybersecurity higher education.

Recently Enacted Regulations

Establishment of the Cybersecurity Directorate and the Cybersecurity Act

Aiming at providing a standalone institution for cybersecurity, on 8 January 2025, Presidential Decree No 177 on the Cybersecurity Directorate established the Cybersecurity Directorate ("Directorate"). The powers and duties of the Directorate were later determined by the Cybersecurity Act. For detailed information, see **1.2 Cybersecurity Laws** and **1.3 Cybersecurity Regulators**.

Other regulations

The Communiqué on Information Systems Management took effect on 30 June 2025 and covers the security of information systems used in the capital markets sector. For detailed information, see **3. Operational Resilience in the Financial Sector**.

1.2 Cybersecurity Laws

On 19 March 2025, the Cybersecurity Act was published in the official gazette and entered into force. According to the Cybersecurity Act's provisory articles, 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 does not explicitly address cybersecurity. However, as cybersecurity also covers data protection, it can be considered that cybersecurity is partly and indirectly covered by Article 20 (3) of the Constitution, which provides for the right to protection of personal data. Additionally, Article 22 recognises freedom of communication as an individual right. Furthermore, because the Cybersecurity Act defines cybersecurity as an integral part of national security, many constitutional rights can be restricted on this basis.

The Cybersecurity Act

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

Certain actions are criminalised, such as:

- failure to provide information, documents and data to the audit personnel;
- causing a data breach due to a failure to fulfil the duties regarding the protection of critical infrastructure against cyber-attacks;
- 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.

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

The purpose section includes a provision regarding the identification and elimination of existing and potential threats, both internal and external, directed in cyberspace against all elements constituting the national power of Türkiye. However, the Cybersecurity Act's territorial scope is not explicitly specified, so must be determined by general rules of criminal law or international public/private law, depending on the context.

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 ("Internet Law")

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

internet. Although the Internet Law imposes cybersecurity-related duties on the Turkish Information and Communication Technologies Authority (ICTA), that body will no longer be able to carry out these duties when the Directorate's organisation is completed according to the Cybersecurity Act.

The Law on Electronic Communication No 5809 ("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.

ICTA is the authorised regulatory body in the e-communications sector, but its authority in cybersecurity measures has now been transferred to the Directorate.

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

This decision is one of the landmarks of Türkiye's cybersecurity legislation, defining national cybersecurity and setting cybersecurity-related duties and powers for the MTI. The Cybersecurity Act transfers the MTI's cybersecurity-related duties and powers to the Directorate; however, it does not explicitly annul this decision.

Presidential Decree No 177 on the Cybersecurity Directorate

On 8 January 2025, 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; please see **1.3 Cybersecurity Regulators** for further discussion of the duties of the Directorate.

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

The purpose of this communiqué is 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 ("Institutional CERT Guideline") and the Guideline for Establishment and Management of Sectoral CERTs ("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 and their relationship with each other and the TR-CERT. They also include the principles for communication with internal/external stakeholders and establishing institutional and sectoral CERTs.

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

The Presidency Decree sets security measures for critical data, the compromise of which could threaten national security or public order. It mandates securely storing critical data (eg, population, health and communication records, genetic and biometric data) within Türkiye.

The Presidency Decree applies to public institutions and organisations and businesses providing critical infrastructure services (eg, electronic communications, banking and finance, and transportation); see **2.1 Scope of Critical Infrastructure Cybersecurity Regulation** for further details.

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

The DP Law covers personal data processing activities in Türkiye. From a cybersecurity perspective, it also regulates the security of personal data and 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.

These obligations, along with incident notification obligations, overlap with the Cybersecurity Act. However, the interplay between the DP Law and the Cyberse-

curity Act remains unclear as both have broad scopes and lack a prevailing clause.

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

The Turkish Criminal Code (TCrC) No 5237

The TCrC prescribes imprisonment of between six months and eight years for cybersecurity offences, including:

- unlawful access;
- blocking or bricking the cyber-system, or destroying, modifying or making inaccessible the data within;
- misuse of debit or credit cards;
- trafficking devices or software used to bypass security for criminal purposes;
- committing theft or fraud via cyber-systems;
- unlawful recording, transfer, publication or acquisition of personal data; and
- failure to destroy personal data after the legal retention periods.

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

KamuNet (loosely translated as PublicNet) is a closed-circuit, isolated virtual network infrastructure for public institutions and organisations in their service, transaction and data traffic transfers. Hence, it is more secure against physical and cyber-attacks. All public institutions and organisations must utilise the KamuNet network.

The Communiqué on KamuNet sets the requirements for public entities integrated into KamuNet, such as having a TS ISO/IEC 27001 certificate. In addition, it authorises the MTI to determine which public entities are to be integrated and to assess their suitability.

1.3 Cybersecurity Regulators

The Cybersecurity Directorate

The Directorate has been designated as a general authority on cybersecurity matters. Its main duties and powers 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 cybersecurity;
- carrying out testing and certification procedures for cybersecurity;
- conducting cybersecurity audits and imposing sanctions; and
- determining the technical criteria for cybersecurity products and services to be used in public institutions and critical infrastructures.

Amendments made to Presidential Decree No 177 on the Cybersecurity Directorate on 25 December 2025 provided some additional powers and duties on standardising, governing and operating the national digital infrastructure and AI ecosystem.

The Directorate is also authorised to conduct audits and on-site inspections for activities of all persons and institutions subject to the Cybersecurity Act. For reasons of national security, public order or the prevention of crime or cyber-attacks, and pursuant to a judicial decision or, in cases of urgency, a written order from a public prosecutor, it may also search and seize in residences, workplaces and other non-public indoor spaces.

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.

On 24 October 2025, the head of the Directorate was appointed. On 25 December 2025, the following additional units were formally established under the Directorate:

- General Directorate of Public AI;
- General Directorate of Digital State;
- General Directorate of Administrative Services;
- Strategy Development Department; and
- Office of the Private Secretary.

However, the Directorate has not yet become fully operational or published any regulation.

Moreover, it has been reported that the Directorate was involved in joint cyber operations against a network attempting to gain unauthorised access to data belonging to public institutions.

The Ministry of Transport and Infrastructure

The Council of Ministers Decision on Cybersecurity authorises the MTI to govern national cybersecurity strategy and implementation, with strategic oversight provided by the TR-CERT. The Cybersecurity Act delegates MTI's cybersecurity-related responsibilities to the Directorate.

The Cybersecurity Board

The Cybersecurity Board is presided over by the President of the Republic of Türkiye and 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 disputes between the Directorate and public institutions.

The Information Technologies and Communication Authority

ICTA is an independent administrative institution that regulates telecommunications, closely monitors cybersecurity incidents, and audits and warns private companies concerning cybersecurity threats and vulnerabilities.

The Cybersecurity Act restricts ICTA's general cybersecurity-related powers and limits its duties to the data systems within its own competency. However, ICTA will continue carrying out its duties until the Directorate's organisation becomes fully operational.

The Digital Transformation Office (DTO)

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

In 2013, the TR-CERT was established under ICTA to identify emerging threats, take measures to eliminate the effects of attacks and incidents on national cyberspace and share them with the relevant actors. The TR-CERT oversees the management of response to cybersecurity incidents from the beginning until the resolution. It co-ordinates with CERTs, which are required to report cyber incidents to the TR-CERT. The 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

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. Furthermore, ICTA is authorised to order a public or private organisation to establish and maintain a CERT, regardless of its sector. 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 (DPA)
The DPA is the primary supervisory and regulatory authority for data protection matters. It is authorised to regulate data protection activities, to take measures to protect the rights of data subjects, and to receive data breach notices.

The National Intelligence Agency (NIA)
The NIA is entitled to collect and analyse data by using any method, tool and system regarding foreign intelligence, national defence, counterterrorism, international crimes and cybersecurity, and to deliver the produced intelligence to the relevant institutions.

The Turkish National Police Department of Cybercrime Prevention
This department provides support in investigating crimes committed using information technology, and gathers forensic data to fight cybercrime. This department is also the 24/7 Contact Point of the Budapest Convention on Cybercrime.

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 (AFAD)
AFAD is responsible for crisis co-ordination and management, to protect critical infrastructures in the event of disasters.

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

2. Critical Infrastructure Cybersecurity Regulation

2.1 Scope of Critical Infrastructure Cybersecurity Regulation
General
There is no framework legislation on critical infrastructure cybersecurity.

The Cybersecurity Act delegates the duty to determine critical infrastructures and the organisations and locations to which they belong to the Directorate and the Cybersecurity Board. 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 of authorised institutions and sector-specific by-laws.

The DTO's Information and Communication Security Guide ("ICS Guide")
The ICS Guide published by the DTO defines "critical infrastructures" 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 entities and businesses providing critical infrastructure services. It sets out general security measures and those specific to the energy and e-communication sectors. It defines, among other things, the asset groups, their criticality level, measures, the application process, and their respective compliance plans.

Guidance of the MTI

The MTI is tasked with identifying critical infrastructures along with the institutions they belong to and their locations (although 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 those 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 forces;
- roads and bridges;
- dams; and
- services provided via critical systems where salary and judicial transactions are performed and their records are kept.

The MTI has also published the "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 of providing the procedures and principles for operators to apply in order to ensure network and information security. It applies to operators that are subject to 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, which aims to define the minimum level of security of industrial control systems used in the energy sector and establish the procedures and principles governing their cyber-resilience, proficiency and maturity.

The By-Law covers industrial control systems owned by legal entities with the following licences:

- electricity transmission;
- electricity distribution;
- electricity generation facility;
- natural gas transmission licence for pipeline transmission;
- natural gas distribution;
- natural gas storage;
- crude oil transmission; and
- refinery.

Banking and Finance

The By-Law on Information Systems of Banks and Electronic Banking Services ("By-Law ISBEBS") aims to manage information systems used by banks, establishing the minimum standards for electronic banking services and the management of risks related thereto.

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 have not yet been determined as the Directorate has not yet become fully operational.

For information on certification requirements of critical infrastructures, see **5.1 Key Cybersecurity Certification Legislation**.

The Presidency Decree provides the following security measures for critical infrastructure security of public entities:

- 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 entities and businesses providing critical infrastructure services:

- network and system security measures;
- application and data security measures;
- portable device and media security measures;
- IoT devices security measures;
- personnel security measures; and
- physical environment security measures.

The ICS Guide also provides:

- a roadmap for compliance;
- responsible personnel for each process of compliance;
- guidance on categorising asset groups and determining critical assets;
- measures required for supply chain security;
- measures required for threat and vulnerability management; and
- measures required for disaster recovery and business continuity.

The ICS Guide also prescribes security measures for the e-communications and energy sectors. There are also other sector-specific regulations governing critical infrastructure cybersecurity, which are detailed below.

E-Communications Sector

Security measures to be taken by actors in the e-communications sector in accordance with the ICS Guide include the following:

- service security and continuity;
- signalling traffic security;
- establishing trusted communication;
- 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 operators to prepare a report on NIS annually – until the end of March – and to retain it for five years, to be submitted to ICTA upon request and/or during inspections. The report includes information such as details on information security breach incidents that have occurred.

Per the By-Law, operators cannot allow unlicensed software and software violating Information Security Management Systems Policy rules. They must protect information and software against harmful codes, and identify security measures for external networks downloads. Operators must also define and document rules related to the software's transfer from the development environment to the production environment.

Energy Sector

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

- device configurations;
- network, physical and user access management;
- authentication;
- ensuring system continuity;
- prevention of data manipulation;
- 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 that must be implemented by obligated organisations will be identified with sectoral criticality degrees determined by the EMRA.

Banking and Finance Sector

Banks and other financial institutions under the authority of the BRSA must take the measures out-

lined in the By-Law ISBEBS. Moreover, personal data specific to banking relationships is also considered customer secrets under the Banking Law. For specific requirements, see **3.1 Scope of 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 mandates that civil aviation enterprises implement:

- effective oversight of information systems;
- regular risk and threat assessments for operational assets;
- comprehensive policies, procedures and process documents;
- mechanisms to detect, prevent and respond to breaches;
- testing, auditing, monitoring and reporting cybersecurity controls and structures; and
- a continuity management process and plan.

2.3 Incident Response and Notification Obligations

There are several incident response and notification obligations for businesses providing critical infrastructures. Depending on the sector, persons/institutions can be subject to more than one notification obligation. Since there are no specific provisions determining the interplay between the relevant regulations, notifications must be made to each authority separately.

Notification to CERTs

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

If an organisation is required to establish a CERT, in principle, its CERT must report any cyber incident (which the Communiqué on CERTs defines as a "breach or attempted breach of confidentiality, integrity, or accessibility of industrial control or information systems or data processed thereby") 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 obliged to report (although voluntary reporting is allowed).

Notification to the Directorate

Under the Cybersecurity Act, institutions and persons using information systems are required to notify the Directorate of any vulnerability or cyber incidents that they detect in their service area. Non-compliance is subject to an administrative fine of between TRY1,254,900 and TRY12,549,000.

The Cybersecurity Act defines a "cyber incident" as "the violation of the confidentiality, integrity, or availability of information systems or data", whereas "vulnerability" is defined as "weaknesses and security gaps in cyberspace assets that may be exploited by any cyber threat".

Since the Directorate has not yet become operational, there is no available channel for notification to the Directorate; the details that must be reported to the Directorate have also not yet been determined.

Although prompt notification is required, the Cybersecurity Act does not specify timelines for the notification.

Personal Data Breach Notification

Controllers must report to the DPA within 72 hours and notify the relevant data subjects within the shortest time possible in case of data breach. The notification must be made using the "Data Breach Notification Form" published by the DPA. This form must be submitted to the DPA via email or through the web portal available on the DPA's website.

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 security breaches affecting more than 5% of its subscribers and the circumstances interrupting the continuity of the business. The notification must include at least the time, nature, impact and duration of the breach, and the measures taken.

In the banking sector, 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.

In the civil aviation sector, the Cybersecurity Directive for Civil Aviation Enterprises requires civil aviation enterprises to immediately report cyber incidents escalating into a crisis or affecting critical information systems or personal data to the GDCA.

2.4 State Responsibilities and Obligations

According to the Cybersecurity Act, one of the duties of the Directorate is to obtain, generate and share cyber threat intelligence. The Directorate is also responsible for promoting co-operation between the public sector, the private sector and universities through working groups. The government and the private sector also co-operate to develop cybersecurity standards and procedures through initiatives such as the Türkiye Cybersecurity Cluster.

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** regarding the obligations provided for public institutions under the ICS Guide.

3. Operational Resilience in the Financial Sector

3.1 Scope of Financial Sector Operational Resilience Regulation

No general legislation governs the Turkish financial sector's operational resilience. Rather, relevant regulations of the BRSA, TRCB and CMB govern 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 the By-Law ISBEBS, which applies to banks established in Türkiye and to branches of foreign banks in Türkiye.
- The information systems of payment 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 ("Communiqué on Payment Services"). The Communiqué covers an exhaustive list of payment and electronic money institutions that are established in Türkiye and authorised by the TRCB in accordance with the Law on Payment and Securities Settlement Systems, Payment Services, and Electronic Money Institutions. Therefore, although it does not apply to payment and electronic money institutions located abroad, it applies to international transactions made through Turkish payment and electronic money institutions.
- The CMB has a Communiqué on Information Systems Management ("CMB Communiqué"), which took effect on 30 June 2025 by superseding a similar Communiqué. This Communiqué concerns stock exchanges, market operators and other organised marketplaces, publicly held corporations, and capital market institutions (eg, investment firms and crypto-asset service providers), among others. Since these institutions are required to be established in Türkiye, the Communiqué is not directly applicable to foreign institutions. However, it may be applied to international transactions of the institutions in scope.
- Crypto-asset service providers' obligations under the CMB Communique are specified in "Criteria for Information Systems and Technology Infrastructures of Crypto Asset Service Providers", which was published by the Scientific and Technological Research Council of Türkiye (STRCT) on 8 May 2025.

3.2 ICT Service Provider Contractual Requirements

There is no legal definition for ICT or cloud service providers. However, several sectoral regulations indicate different service providers for ICT services.

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.

Requirements Under the By-Law ISBEBS, the Communiqué on Payment Services, and the CMB Communiqué ("Financial NIS")

The Financial NIS regulates the outsourcing of ICT services by the financial sector institutions. It aims to guarantee that financial sector institutions retain their control over outsourced information systems and 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**.

Outsourcing requirements include:

- assessing service provider access risks;
- determining exit strategies; and
- in case of procuring cloud services for primary and secondary systems, ensuring that the systems used for these cloud services are located in Türkiye.

The Financial NIS requires outsourcing contracts to 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;
- provisions granting the respective financial institution the right to request necessary documents and information regarding the outsourced services;
- provisions ensuring that the outsourcing provider is also subject to inspection/audit of the respective regulator;
- terms for changes and termination;
- data destruction obligations for the outsourcing provider in case of termination; and
- provisions regarding the management of risks related to unexpected termination.

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.

Classification of ICT Services

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

While the By-Law ISBEBS and the Communiqué on Payment Services regulate "critical information systems" without defining the term, 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 for remote identity verification as critical information systems in terms of the By-Law ISBEBS.

The CMB Communiqué also does not define "critical information systems", but it does define "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 specific requirements, such as real-time monitoring of unauthorised access.

3.3 Key Operational Resilience Obligations

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

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

must also impose internal control mechanisms for the same (eg, approval of senior staff).

Cyber Incident Management and Reporting Obligations

Cyber incident response measures include keeping a detailed record, preventing similar incidents, establishing internal incident management mechanisms, and identifying the root causes.

Certain details of cyber incidents must be reported to internal senior staff and the relevant institutions. In addition, regarding critical infrastructure, financial institutions must also follow the notification obligations mentioned in **2.3 Incident Response and Notification Obligations**.

Although the respective regulations require prompt notification, there is no general time frame for reporting obligations, except for personal data breaches, as detailed under **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

Enforcement of operational resilience obligations is shared by the BRSA, TRCB and CMB.

Banking Regulation and Supervision Agency

The BRSA is authorised to carry out examination of all books, records and documents, and to conduct on-site audits and ex officio inspections concerning the support service organisations. The By-Law ISBEBS also authorises BRSA to inspect banks' ICT providers, mandating the submission of requested information and documents and the maintenance of records in a readable format.

Moreover, the BRSA is authorised to impose administrative fines in case of non-compliance, ranging between TRY1,919,682 and TRY19,197,873 for 2026. According to its 2024 Annual Report, BRSA has fined 51 companies for non-compliance with the regulations on information security.

Turkish Republic Central Bank

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.

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, the TRCB may revoke the operating licence.

Depending on the case, the TRCB may impose an administrative fine of between TRY825,996 and TRY2,065,087 for non-compliance with the regulations on payment services and electronic money institutions.

Capital Markets Board

The CMB has the authority to audit capital market activities of entities subject to the Capital Markets Law and other relevant real or legal persons. Auditors may request relevant documents and information. Failure to provide these and obscuring the audit are criminalised under the Capital Markets Law.

Depending on the case, the CMB may impose an administrative fine of between TRY445,189 and TRY5,565,500 on persons who fail to comply with the Capital Markets Law and its secondary legislation. Of the decisions of the CMB that were published in 2025, 16 included administrative fines for non-compliance with the CMB Communiqué; most of these decisions concerned penetration testing and information security continuity requirements.

3.5 International Data Transfers

Data 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.

Banking Law and its Secondary Legislation

Under the Banking Law, customer secrets cannot be disclosed or transferred abroad without customer instruction, with the following two exceptions:

- transfers to authorities authorised by Turkish laws; and
- sharing information and documents related to the preparation of consolidated financial statements, risk management and internal audit practices with a foreign parent company, provided that its capital share is at least 10% and a non-disclosure agreement is signed

The By-Law on the Sharing of Secret Information applies to bank and customer secrets collectively, and also provides exceptions to secrecy prohibitions. Permitted transfers include:

- per a Board resolution, sharing with third parties bank secrets that only contain banks-classified information; and
- disclosures to the foreign judicial and alternative dispute resolution authorities or to the parties representing the bank in such disputes, when necessary for the proof of the claim or defence.

The Communiqué on Payment Services

Institutions may share data with foreign third parties for cross-border payment transactions, subject to domestic storage, necessity and proportionality. For outsourced products or services, the Communiqué on Payment Services requires the use of local products, or the manufacturers thereof to have R&D centres and response centres in Türkiye.

General DP Law Regime on International Personal Data Transfers

International personal data transfers are governed by the DP Law, amended on 12 March 2024 (effective from 1 September 2024) to align with the General Data Protection Regulation.

International personal data transfers are permitted under the following conditions.

- The existence of a valid legal basis under the DP Law and an adequacy decision for the recipient country, international organisation or the sectors therein (note that the DPA has not yet issued any adequacy decision).
- In the absence of an adequacy decision – the existence of a valid legal basis under the DP Law, enforceable 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 or appropriate safeguards – 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, debates on interpreting these provisions persist.

The DP Law provides a reservation for provisions under other laws. Consequently, where such a specific provision is applicable, it will override the transfer regime under the DP Law.

The provisions explicitly mentioned in the Banking Sector Best Practices Guide on the Protection of Personal Data 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 for the minimum information to be included in an international e-transfer, will also apply in a preceding manner.

3.6 Threat-Led Penetration Testing

According to the Cybersecurity Act, one of the duties of the Directorate is to conduct vulnerability and penetration tests in order to prevent cyber-attacks against critical infrastructures and information systems. In addition, the Financial NIS imposes penetration testing obligations for their respective financial sector institutions, as detailed below.

For detailed information on the scope of the Financial NIS, see **3.1 Scope of Financial Sector Operational Resilience Regulation**.

The By-Law ISBEBS

Banks must have annual penetration tests performed by independent teams that are not involved in the information systems operations. Banks' Institutional CERTs must also 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 mandates that payment and electronic money institutions must:

- conduct annual penetration tests for scenarios covering possible internal and external threats (pursuant to the procedure provided under Annex 5 therein);
- have the penetration tests conducted by accredited, independent third parties (natural or legal entities) with no involvement in information security operations; and
- submit annual reports to the TRCB, detailing breaches, test results, critical vulnerabilities identified and remediation measures.

The CMB Communiqué

The information systems of the related institutions and organisations must have annual penetration tests pursuant to the procedure provided under the Annex 1 of the CMB Communiqué. The reports related to the penetration tests must be submitted to the CMB each year by January 31st.

Penetration tests must be conducted by independent third parties (natural or legal entities) who are not involved in information security operations and are certified nationally or internationally.

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 Programme for 2026 includes a plan to enact legislation in line with the EU's Cyber Resilience Act (CRA). Cyber resilience regulation is anticipated, since cyber resilience is listed as a core objective of the NCS 2024. In this regard, the Cybersecurity Act objective of "establishing principles to mitigate the possible impacts of cyber incidents" indicates cyber resilience.

According to the Cybersecurity Act, "activities aimed at detecting attacks and cyber incidents, activating response and alert mechanisms, and restoring the situation to its state prior to the cyber incident" are considered as part of cybersecurity, which seems to imply cyber resilience.

4.2 Key Obligations Under Legislation

The Cybersecurity Act delegates a specific duty to the 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 must ensure resilience during and after cyber incidents by:

- co-ordinating with their sectoral CERTs to prevent or mitigate damage;

- reporting cyber incidents to their institutions, notifying the TR-CERT and their sectoral CERTs without delay;
- primarily trying to eliminate a cyber incident internally, and requesting assistance from the TR-CERT and their sectoral CERT, as applicable;
- reporting suspected criminal activity to the competent authorities and the TR-CERT without delay;
- having 24/7-accessible contact information and notifying their sectoral CERTs and the TR-CERT thereof;
- recording vulnerabilities;
- monitoring the types, quantities and costs of cyber incidents; and
- submitting to the management of the institution for corrective/preventative actions.

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

- co-ordinating with the TR-CERT to prevent or mitigate incidents;
- immediately notifying the TR-CERT of cyber incidents affecting their CERTs;
- having 24/7-accessible contact information and notifying their CERTs and the TR-CERT thereof;
- supporting their CERTs in cyber incidents; and
- reporting suspected crimes to the competent authorities and the TR-CERT without delay.

5. Security Certification for ICT Products, Services and Processes

5.1 Key Cybersecurity Certification Legislation

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

The Cybersecurity Act provides for 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 that will be certified by the Directorate. Procurement from uncertified experts or companies will be subject to an administrative fine of between TRY1,254,900 and TRY12,549,000.

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.

ICS Guide Compliance Audit Service Providing Personnel and Firm Certification

Persons or firms auditing the public institutions and businesses providing critical infrastructure services are certified by a programme conducted by the DTO, Turkish Standards Institute and STRCT.

The Financial Sector

The BRSA requires all banks to meet Control Objectives for Information and Related Technologies (COBIT) standards. COBIT process management is also used in the finance and production sectors.

The By-Law on Banking Cards and Credit Cards requires 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 the 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 must provide an appropriate level of security for the personal data they process, and ensure their processors provide a level of security for personal data that is at least equivalent to their own. To enforce this, 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) ("Measures Guideline") in 2018, which lists and details the technical and administrative measures to be taken by data controllers, such as:

- 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; and
- using brute force algorithm (BFA).

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

Administrative fines for failure to take the necessary technical and organisational measures (interpreted very broadly, including unlawful data transfer abroad and violation of fundamental principles) range between TRY256,357 and TRY17,092,242 for 2026.

See also **2.3 Incident Response and Notification Obligations** regarding the data breach notification duty.

6.2 Cybersecurity and AI

Currently, Türkiye has no specific AI legislation. However, on 5 October 2024, the Turkish Parliament established a parliamentary research commission to establish a legal infrastructure in this field and to determine measures to prevent the risks of AI. The commission's work remains undisclosed.

In addition, a proposal for an AI Act was submitted to parliament on 25 June 2024, focusing on risk management and auditing. Although its approval is unlikely, it is the first legislative initiative in this field. Another proposal aimed at regulating AI was submitted to parliament on 7 November 2025. It included cybersecurity requirements for AI system service providers.

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, including:

- authentication and authorisation;
- end-to-end encryption;
- self-deleting messages;
- configuration access controls; and
- secure history storage.

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 minor protection.

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

- complying with international standards, having certificates, and ensuring privacy by default; and
- in data communication, preferring secure methods for transmitting inputs.

In addition, 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.

Finally, the DPA has recently published the "Guidance on Generative AI and Personal Data Protection", which includes recommendations related to matters such as:

- using privacy by design and privacy by default approaches;
- conducting impact assessments;
- integrating privacy enhancing technologies;
- diverse red teaming;
- prioritising trusted data sources; and
- regular validation checks.

Regulations Determining the Authorities to Regulate AI

On 25 December 2025, two presidential decrees were published, authorising two authorities to regulate AI. Accordingly, the General Directorate of National Technology and AI under the Ministry of Industry and Technology is authorised to regulate AI technologies in general, while the Cybersecurity Directorate is now authorised to regulate AI in the public sector.

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 the Health Information Systems General Directorate (HISGD) under the Ministry of Health, which was established to regulate information systems and communication technologies used in the healthcare sector.

The MoH InfoSec Directive establishes the Information Security Management Commission and sub-commissions responsible for information security and cyber incident management across all central and provincial Ministry of Health organisations. 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. It includes some requirements related to information security, such as reporting information security breaches to the Ministry of Health through an online web portal.

For details of the certification obligation, see **5.1 Key Cybersecurity Certification Legislation**.

The By-Law on Personal Health Data

Supplementing the DP Law provisions on special categories of personal data, the By-Law on Personal Health Data provides for the specific procedure to be followed by healthcare providers while processing health data. It covers accessing, securing, rectifying, destroying and transferring health data. It requires taking the information security measures under the MoH InfoSec Directive and using KamuNet to transfer health data where feasible.

The Guide on Protection of Personal Data in Pharmacovigilance Activities

In the context of pharmaceutical R&D, the Turkish Medicines and Medical Devices Agency's Guide on Protection of Personal Data in Pharmacovigilance Activities mandates specific technical and organisational measures, such as:

- personnel training;
- setting up a firewall;
- using an internet gateway;
- using antivirus and antispam software;
- removing vulnerable and unused software;
- limiting access;
- monitoring penetrations and unexpected movements in information networks;
- keeping regular log records;
- establishing an official reporting procedure;
- reporting security issues to the data controller as quickly as possible;
- ensuring security of environments containing personal data; and
- taking additional measures when 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