PANORAMIC

CYBERSECURITY

Türkiye

LEXOLOGY

Cybersecurity

Contributing Editors

Colman McCarthy, Jon Wilson, Josh Hansen, Lindsey Knapton and Brandon Large

Shook Hardy & Bacon LLP

Generated on: September 15, 2026

Contents

Cybersecurity

Recent developments and future changes

Contributors

Türkiye

YAZICIOGLU Legal

Bora Yazicioglu	bora@yazicioglulegal.com
Emre Öntekin	emre@yazicioglulegal.com
Yağmur Yaren Özdabakoğlu	yaren@yazicioglulegal.com
Ece Ogur	eceogur@yazicioglulegal.com
Ferat Gümüş	ferat@yazicioglulegal.com

LEGAL FRAMEWORK

Key legislation

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

Türkiye did not have a standalone cybersecurity legal framework until 2025. The Cybersecurity Law, which came into force on 19 March 2025, laid the foundation for a comprehensive legal regime. Until the secondary regulations, which are to be adopted within one year, become effective, existing regulations will remain in force, provided that they are compatible with the Cybersecurity Law.

At present, cybersecurity is governed by a fragmented set of legal instruments and policy documents, as outlined below:

- The Constitution of the Turkish Republic (Constitution) indirectly addresses cybersecurity through article 20(3), which guarantees the right to the protection of personal data and article 22, which establishes the right to freedom of communication. Furthermore, because the Cybersecurity Law defines cybersecurity as an integral part of national security, many constitutional rights can be restricted on this basis.
- The Cybersecurity Law No. 7545 (Cybersecurity Law) regulates duties and powers of the Cybersecurity Directorate, together with obligations of institutions and persons who operate in cyberspace. It also establishes and determines the duties of Cybersecurity Board. Additionally, the Cybersecurity Law introduces new categories of cybercrimes (eg, creating and disseminating false content regarding data breaches in cyberspace) and provides specific obligations for companies that develop cybersecurity products and services.
- The Law on Electronic Communications No. 5809 (E-Communications Law) and its secondary legislation provide the primary legal framework for network security, the confidentiality of communication, and personal data protection related thereto.
- The Law on Regulation of Publications via the Internet and Combating Crimes Committed by Means of Such Publications No. 5651 (Internet Law) applies to content, hosting, access providers and other related institutions and organisations for ensuring the safe use of the Internet. While the Internet Law currently mandates cybersecurity duties for the Turkish Information and Communication Technologies Authority (ICTA), these responsibilities will transfer to the Directorate once its organisation under the Cybersecurity Law is finalised.
- The Turkish Data Protection Law No. 6698 (DP Law) and its secondary legislation govern personal data processing in Türkiye. The DP Law requires data controllers and processors to implement technical and organisational measures for personal data across both automated and non-automated systems. These obligations, along with incident notification obligations, overlap with the Cybersecurity Law. However, the interplay between the DP Law and the Cybersecurity Law remains unclear as both have broad scopes and lack a prevailing clause.
- Presidential Decree No. 177, issued on 8 January 2025, established the Cybersecurity Directorate, granting it general regulatory authority over cybersecurity matters.

- The Council of Ministers Decision on Carrying Out, Managing, and Co-ordinating National Cybersecurity Activities, dated 11 June 2012, is a landmark decision granting the Ministry of Transport and Infrastructure (MTI) the responsibility to manage national cybersecurity. This includes the development of policies, strategies, and action plans to ensure cybersecurity nationwide. The MTI will continue these cybersecurity-related duties until the Cybersecurity Directorate becomes operational.
- The Communiqué on Procedures and Principles of the Establishment, Duties and Activities of Cyber Incidents Response Centres (CERTs) (Communiqué on CERTs) sets the procedures and principles of CERTs' establishment, duties and work to ensure their effective and efficient functioning.
- The Guideline for Establishment and Management of Institutional CERTs (Institutional CERTs Guideline) and the Guideline for Establishment and Management of Sectoral CERTs (Sectoral CERTs Guideline), published by the National Cyber Incidents Response Centre (TR-CERT), provide guidance on establishing and managing institutional CERTs and sectoral CERTs in relevant organisations. They cover CERTs' relationship with TR-CERT, capacity planning, personnel qualifications (education and experience), mandatory training and required actions before, during and after a cybersecurity incident.
- Decree 2019/12 on Information and Communication Security Measures issued by the Presidency of Türkiye (Presidency Decree) establishes measures to address security risks and maintain critical data confidentiality, integrity, and accessibility. It ensures the safe storage of critical data (eg, population, health and communication records, genetic and biometric data) in Türkiye. The Presidency Decree applies to public entities and businesses providing critical infrastructure services.
- The Communiqué on the Procedures and Principles for Connecting to and Auditing the KamuNet Network mandates public entities to connect to KamuNet, a secure, closed-circuit virtual network with enhanced protection against cyber-attacks. All public entities are obliged to employ the KamuNet network.
- The Turkish Criminal Code No. 5237 (TCrC) prescribes imprisonment between six months and eight years for cybersecurity offences (eg, blocking the cyber-system, committing theft via cyber-systems).
- The National Cybersecurity Strategy for 2024-2028, The 12th Development Program 2024-2028, Medium Term Program 2025-2027 and The Presidency Program 2026 are the latest policy documents outlining Türkiye's strategic goals and initiatives to enhance cybersecurity resilience.

Law stated - 2 March 2026

Most affected economic sectors

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

Critical infrastructure sectors and systems that rely on information technologies are of special importance. Any disruption to the confidentiality, integrity, or availability of their data could lead to loss of life, large-scale economic damage, national security risks, and public

disorder. While the main objective is to secure organisations in these sectors, the regulations also enhance cybersecurity within them.

Currently, the critical infrastructure sectors include e-communications, banking, finance, energy, transport, water management and critical public services (such as civil registration, land registration, taxation, commerce, social security and health). This list may be updated, as the Cybersecurity Law empowers the Cybersecurity Directorate and Cybersecurity Board to determine critical infrastructures and associated organisations and locations.

Law stated - 2 March 2026

International standards

Has your jurisdiction adopted any international standards related to cybersecurity?

The Turkish Standards Institute has translated and recognised ISO/IEC 27001 as TS EN ISO/IEC 27001. Compliance is mandatory in some sectors (eg, e-communications, energy, healthcare and e-invoice services) and for public entities. Notably, many organisations adopt this standard voluntarily to strengthen their cybersecurity practices.

The Centre for Internet Security Critical Security Controls is another global standard increasingly implemented among public institutions and large-scale private sector companies in Türkiye.

There are also mandatory sector-specific standards and certifications, such as:

- Control Objectives for Information and Related Technologies standards for banking and finance sectors;
- Payment Card Industry Data Security Standards for organisations entering into merchant agreements with banks;
- Certified Information Systems Auditor certification for auditors of public companies; and
- TS ISO/IEC 15504 Software Process Improvement and Capability Determination certificate for health information systems' service providers.

Law stated - 2 March 2026

Personnel and director obligations

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

The Turkish Commercial Code imposes a broad duty of care on the Board of Directors (BoD), including overseeing and approving cybersecurity policies and strategies for the company's information assets and systems.

For personal data, DP Law does not directly impose any liability on the BoD; however, it requires the data controller to implement appropriate technical and organisational measures. The BoD may be held responsible for breaching its duty of care in the case of violations thereof. Similar obligations existing sector-specific regulations, such as:

- The BoD oversees the implementation of information systems under Banking Law No. 5411.
- The BoD is accountable for managing the information systems of the organisations in the payment services sector, under the Communiqué on Data Sharing Services in the Payment Services Area of Payment and Electronic Money Institutions' Information Systems and Payment Service Providers.
- Under the Capital Markets Law No. 6362, both companies and their BoD members are liable for regulatory violations and may face administrative fines.
- The By-Law on Network and Information Security (By-Law on NIS) requires e-communications businesses to implement an information security policy approved by the BoD and establish disciplinary procedures for violations.

The BoD manages cybersecurity training that is mandatory in certain sectors. For instance, the BoD of banks and capital market institutions are responsible for training their personnel according to the By-Law on Information Systems of Banks and Electronic Banking Services (By-Law on ISBEBS) and the Capital Market Board's Communiqué on the Procedures and Principles of Information Systems Management (CMB Communiqué). Similarly, the Institutional and sectoral CERTs Guidelines set capacity and qualification standards, including mandatory training programmes.

The BoD members may face financial liability for damages to the company, shareholders, or creditors, or risk dismissal for breaching their duty of care. They may also face imprisonment or a judicial fine for unauthorised sharing or disclosing of trade secrets, banking or consumer secrets, or personal data-related offences committed under managerial instructions, BoD decisions or established company practices.

Law stated - 2 March 2026

Key definitions

How does your jurisdiction define 'cybersecurity' and 'cybercrime'?

The Cybersecurity Law defines cybersecurity as

> all activities that involve protecting the information technologies which constitute cyberspace from attacks, ensuring the confidentiality, integrity and availability of the data processed in these systems, detecting attacks and cyber incidents, activating response and alert mechanisms against those, and restoring the systems back to pre-cyber incident conditions

While the existing legislation does not define cybercrime, it refers to crime targeting security, data or users of an information system, committed via information technologies as defined in the National Cybersecurity Strategy Action Plan 2020-2023. The Court of Cassation

defines it as 'a crime committed via information systems against data and/or systems connected to data processing'. Accordingly, information system security and cybersecurity enforcement may be considered aligned.

However, there is no clear distinction between data privacy and cybersecurity, both terms often being interconnected.

Law stated - 2 March 2026

Mandatory minimum protective measures

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

The Cybersecurity Law does not explicitly address the measures but rather requires those that fall under the scope of this law to adopt the measures that are specified in the relevant laws. Protective measures are detailed in various legal instruments and categorised by data type and sector.

Critical infrastructures and critical infrastructure sectors

The Cybersecurity Law mandates that cybersecurity products, systems, and services in critical infrastructures must be procured from experts and companies certified by the Cybersecurity Directorate. Non-compliance with this obligation results in an administrative fine of between 1.25 million Turkish liras and 12.55 million Turkish liras. The minimum technical criteria for the cybersecurity products and services in public institutions and critical infrastructures are pending to be determined by the Cybersecurity Directorate.

Additionally, sector-specific regulations require critical infrastructure sector organisations to ensure the security of their information systems.

For critical infrastructure in public institutions, the Information and Communications Security Guideline (ICS Guideline) published by the Digital Transformation Office of the Presidency of Republic of Türkiye, which was abolished with a Presidency Decree on 28 March 2025 and whose cybersecurity-related duties and assets have been transferred to the Cybersecurity Directorate, outlines minimum-security requirements for:

- network and system;
- application and data;
- portable device and media;
- internet of things devices;
- personnel; and
- physical environment.

The ICS Guideline provides specific security measures (eg, for personal data, instant messaging, cloud computing, cryptographic applications, new developments and procurement).

The Institutional CERTs Guideline, addressing to public institutions and private entities operating critical infrastructure, does not provide detailed security specifications. Rather, it highlights awareness-raising and security tests for incident-readiness. These include penetration and distributed denial-of-service tests, firewall assessments and wireless network evaluations.

Critical data

The Presidency Decree provides measures for public entities and businesses providing critical infrastructure services to protect critical data essential to national security and public order (eg, population, health and communication records, genetic and biometric data).

Personal data

Under DP Law, data controllers must implement appropriate technical and organisational measures for personal data processing. The Data Protection Authority's (DPA) Personal Data Security Guideline (Measures Guideline) offers practical measures and best practices, including cybersecurity-related measures (eg, using firewalls and gateway, password-protecting and creating an access control matrix to prevent common attacks such as brute force). For sensitive personal data, the DPA mandates specific measures.

Law stated - 2 March 2026

Cyberthreats to intellectual property

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

The Law on Intellectual and Artistic Works No. 5846 criminalises the following actions with penalties ranging from six months to two years of imprisonment:

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

The By-Law on Common Database for Intellectual Property Rights establishes a common database to ensure monitoring and protection of intellectual property rights and regulates its security.

Law stated - 2 March 2026

Cyberthreats to critical infrastructure

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

Pending secondary legislation under the Cybersecurity Law, critical infrastructure cybersecurity is currently governed by various policy documents and sector-specific by-laws.

The Presidency Decree and ICS Guideline outline general security measures for critical infrastructures.

In the e-communications sector, ICS Guideline provides specific security measures, and the By-Law on NIS sets procedures and principles for ensuring network and information security.

For the energy sector, the By-Law on Cybersecurity Competency Model complements ICS Guideline by setting minimum security standards for industrial control systems and procedures and principles for their cyber-resilience, proficiency, and maturity.

For the banking and finance sector, financial institutions regulated by the Banking Regulation and Supervision Agency must comply with the security measures under the By-Law on ISBEBS.

In the healthcare sector, the Information Security Directive and Guideline regulates information security. These regulations also mandate cybersecurity measures. Additionally, the By-Law on Personal Health Data outlines health data processing procedures, while the-Pharmacovigilance Guideline specifies technical measures for securing health data in R&D activities of medicine.

For civil aviation sector, the Cybersecurity Directive for Civil Aviation Enterprises serves as the primary legislation, setting security measures to combat cyberthreats.

Law stated - 2 March 2026

Restrictions on cyberthreat information sharing

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

Türkiye's legal framework regulates the interception and recording of communications while providing for exceptions in specific circumstances.

Aside from the constitutional right to freedom of communication, the criminalises breaching communication confidentiality, interception of and recording conversations, violating privacy by recording images or sounds, and unlawfully recording personal data.

However, the Code of Criminal Procedure permits communication surveillance (eg, interception of and recording communications, analysis of signal data and tracking mobile phone locations) if a decision is obtained from a judge or, in urgent cases, with a public prosecutors order to obtain evidence of committed or ongoing crimes. However, it applies only to certain offences excluding cybercrimes.

Law stated - 2 March 2026

Criminal activities

What are the principal cyberactivities (such as hacking) that are criminalised by the law of your jurisdiction?

The TCrC includes the following cybercrimes that apply to both legal and natural persons:

- unlawful access to a cyber-system;
- blocking or bricking the cyber-system or destroying, modifying or making inaccessible the data therein;
- misuse of debit or credit cards;
- manufacturing, importing, dispatching, transporting, storing, accepting, selling, offering for sale, purchasing, transferring or possessing forbidden devices or software designed to breach computer program passwords or similar codes for purpose of committing offences described above;
- committing theft or fraud via cyber-systems;
- unlawful recording, transfer, publication or acquisition of personal data; and
- failure to destroy personal data after the retention period set forth in the applicable laws.

The TCrC imposes sanctions that require enforcing security measures for legal entities committing these offences for undue advantage.

The implementation of the Cybersecurity Law has intensified judicial and executive focus on cybercrime. A recent operation by the Ministry of the Interior highlights this enforcement shift, resulting in 324 detentions and 181 arrests.

Additionally, certain actions are now criminalised under the Cybersecurity Law, such as:

- failure to provide information, documents and data to the Cybersecurity Directorate's audit personnel;
- distributing, sharing or selling certain 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.

Last, as part of the first cyber operation involving the Cybersecurity Directorate, suspects who targeted personal data and attempted to gain unauthorised access to public institution systems were arrested under the Cybersecurity Law, following investigations coordinated by the National Intelligence Organisation (MIT).

Law stated - 2 March 2026

Cloud computing

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

Türkiye does not have a regulation specifically addressing information security challenges in cloud computing. However, certain regulations for public institutions and critical infrastructure services directly address these issues.

Under the Presidency Decree, public institutions must store their data in cloud services with localisation requirements and adhere to ICS Guideline. This guideline outlines security measures for cloud computing (eg, localisation for critical data, access controls).

Cloud service providers must also meet specific security criteria (eg, securing data storage policies and providing disaster recovery options). Service contracts must include mutual confidentiality clauses, criticality-based security measures and periodic security audits.

For personal data, the DPA introduced a number of measures in its Measures Guideline (eg, encryption of personal data in cloud systems and destruction of encryption keys when services are terminated).

Additionally, Türkiye is party to international agreements relevant to cloud computing security, including the Council of Europe Convention on Cybercrime (Budapest Convention) and Convention 108+. These conventions establish international standards for protecting the confidentiality, integrity and availability of information systems and personal data, including in cloud environments and facilitate international cooperation in addressing cyber incidents and protecting data processed across borders.

Law stated - 2 March 2026

Foreign organisations

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

The Cybersecurity Law does not have a specific provision for territorial scope. The provisions related to cybersecurity are regulated in a fragmented manner with some being applicable for specific sectors. For instance, in highly regulated sectors such as banking, finance and e-communications, the organisations must be established in Türkiye. Similarly, certain social network providers are required to appoint a local representative. There are specific localisation requirements for both local and foreign organisations in these industries.

Law stated - 2 March 2026

BEST PRACTICE

Recommended additional protections

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

The Cybersecurity Directorate has yet to publish any guidelines.

Institutional Computer Emergency Response Team are responsible for proposing and adopting technical and organisational measures within their organisations for the establishment, operation or development of their information systems to prevent or mitigate cyber incidents.

Organisational Cybersecurity Measures published by the TR-CERT serve as a guide in which the TR-CERT outlines several general measures for organisations and recommends

collaborating with a cybersecurity specialist to develop a cybersecurity policy tailored to the specific needs of each organisation.

The Assessment Document on Cybersecurity Measures for Institutions is a guiding and informative instrument prepared by the MTI to assess the cybersecurity measures and activities undertaken by public entities, as well as private sector representatives.

The Measures Guideline outlines technical and organisational measures for personal data and there are case-specific measures in DPA's decisions.

Law stated - 2 March 2026

Government incentives

How does the government incentivise organisations to improve their cybersecurity?

The Cybersecurity Law tasks the Cybersecurity Board with identifying priority fields to be incentivised. However, since these are not determined yet, there are currently no incentives in place.

Law stated - 2 March 2026

Industry standards and codes of practice

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

Apart from sector-specific certifications, according to the Cybersecurity Law, cybersecurity products, systems and services for public institutions and critical infrastructure are required to be sourced from cybersecurity experts and companies certified by the Cybersecurity Directorate.

Law stated - 2 March 2026

Responding to breaches

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

Aside from the mandatory statutory reporting, the Guideline on Organisational Cybersecurity Measures suggests establishing an emergency response plan for fast and effective response (eg, in the case of a cyber-attack or data breach). Additionally, TR-CERT provides recommendations for corrective actions and preventive measures, based on an analysis of commonly identified deficiencies and inaccuracies through cyber incident responses.

Law stated - 2 March 2026

Voluntary information sharing

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

In practice, TR-CERT designated an email address and online form for individuals to report for cyber incidents. Sectoral regulations may also include similar mechanisms (eg, the Ministry of Health's Information Management Systems Unit for citizens to report cybersecurity breaches).

Law stated - 2 March 2026

Public-private cooperation

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

The government and private sector cooperate to develop cybersecurity standards and procedures through initiatives such as the Türkiye Cybersecurity Cluster, established in 2017.

Supported by the Secretariat of Defence Industries, it was established through public, private, and academic collaboration to identify needs, develop innovative solutions and establish cybersecurity standards.

In practice, regulatory authorities may engage stakeholders in preparing sectoral regulations by getting feedback on draft regulations.

In addition, Cybersecurity Directorate is responsible for promoting greater cooperation between the public sector, private sector, and universities through working groups.

Law stated - 2 March 2026

Insurance

Is insurance for cybersecurity breaches available in your jurisdiction and is such insurance obtainable for most organisations? How common is it?

Several insurers in Türkiye provide commercial cybersecurity insurance for organisations – particularly SMEs – and its adoption is widespread. However, in practice, insurance policies often exclude organisations in high-risk sectors (eg, finance, health except pharmacy and e-commerce).

Law stated - 2 March 2026

ENFORCEMENT

Regulatory authorities

Which regulatory authorities are primarily responsible for enforcing cybersecurity rules?

The Cybersecurity Directorate was recently established as the general regulatory authority for cybersecurity matters. However, the powers of current regulators will prevail until the Directorate becomes fully operational. These regulators are:

- Ministry of Transport and Infrastructure;
- Information and Communication Technologies Authority (ICTA);
- National Cyber Incidents Response Centre;
- Sectoral and Institutional Cyber Incidents Response Teams;
- Personal Data Protection Authority;
- National Intelligence Agency (NIA);
- Turkish National Police Department of Cybercrime Prevention (PDCP);
- Ministry of National Defence, Presidency of Defence Industries, and Turkish Armed Forces Cyber Defence Command; and
- Ministry of Interior Disaster and Emergency Management Presidency.

Some sectoral institutions also have regulative authority for cybersecurity matters in their respective sectors, including:

- Banking Regulation and Supervision Agency;
- Capital Markets Board;
- Turkish Republic Central Bank (TRCB);
- Energy Market Regulatory Authority; and
- Nuclear Regulatory Authority.

Law stated - 2 March 2026

Extent of authorities' powers

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

The Cybersecurity Directorate is authorised to conduct audits and on-site inspections for activities of all persons and institutions falling under the scope of the Cybersecurity Law. For reasons of national security, public order or the prevention of crime or cyber-attacks and pursuing a judicial decision or, in cases of urgency, a written order from a public prosecutor, it may also search and seizure in residences, workplaces and other non-public indoor spaces. The Cybersecurity Directorate may impose administrative fines based on these audits.

On 24 October 2025, the head of the Directorate was appointed. Additionally, on 25 December 2025, additional units were established under the Directorate and it became authorised to regulate AI in public sector. However, the Directorate has not become fully operational and published any regulations yet.

ICTA is authorised to audit and investigate natural or legal persons in e-communications sector and impose sanctions, including administrative fines. The cybersecurity-related duties

of ICTA have been reassigned to the Cybersecurity Directorate, yet the former will retain these duties until the latter becomes fully operational.

TR-CERT oversees response management to cybersecurity incidents from the beginning until the resolution and acts in cooperation with institutional and sectoral Computer Emergency Response Team (CERTs) on detection, prevention and damage minimisation in cyber incidents.

For personal data-related matters, the DPA conducts investigations ex officio or upon complaint. Data controllers must provide the information and documents requested by the DPA (except state secrets) and the means for on-site examination when necessary.

The NIA is responsible for collecting information on cybersecurity from public or private institutions and persons.

The PDCP is authorised to gather forensic data to fight cybercrime.

The Banking Regulation and Supervision Agency (BRSA), Capital Market Board's (CMB), TRCB and Energy Market Regulatory Authority (EMRA) are also authorised to monitor compliance, conduct investigations on and prosecute infringements of persons and institutions operating in their respective sectors.

Law stated - 2 March 2026

Most common enforcement issues

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

Regulatory authorities rarely publish decisions regarding cybersecurity regulations. For instance, in 2025, CMB issued 16 decisions regarding non-compliance with cybersecurity regulations, mostly concerning penetration testing and information security continuity.

However, in general, regulatory authorities do not sufficiently inform the public about the enforcement process of cybersecurity regulations. Therefore, it is difficult to identify the most common enforcement issues.

Law stated - 2 March 2026

Regulatory and data subject notification

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

The Cybersecurity Law obliges the institutions and persons using information systems to immediately notify the Cybersecurity Directorate of vulnerabilities and cyber incidents they detect.

If an incident constitutes a personal data breach, data controllers must notify the DPA within 72 hours after becoming aware of the situation. Data subjects affected must also be notified.

In general, if an organisation is required to establish an Institutional CERT (eg, critical infrastructure organisations), its CERT must report any cybersecurity incident without delay to the TR-CERT and the relevant sectoral CERTs. There are also sectoral cyber incident notification obligations:

- Operators of e-communications must immediately notify ICTA and their customers or users if a cybersecurity breach affects more than 5 per cent of their subscribers or interrupts the business continuity.
- Banks must report cyber incidents to the BRSA.

In the healthcare sector, the Ministry of Health has a central breach notification portal.

In civil aviation sector, civil aviation enterprises must immediately report cyber incidents escalating into a crisis, or affecting critical information systems or personal data to the General Directorate of Civil Aviation.

Law stated - 2 March 2026

Penalties for non-compliance with cybersecurity regulations

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

The Cybersecurity Law imposes administrative fines between 1.25 million Turkish liras and 12.55 million Turkish liras for non-compliance with the obligation to adopt cybersecurity measures provided by the relevant laws to protect national security, public order or the effective operation of public services. It also provides penalties for other relevant acts such as failure to cooperate with the Cybersecurity Directorate during audits. Additionally, if companies commit the audit violation, an administrative fine of up to 5% of gross sales revenue may be imposed, with the lower limit not being less than the minimum amount. Additionally, if a cybersecurity breach constitutes a crime (such as hacking into a system or corrupting data), imprisonment may also be imposed in accordance with the TCrC.

Sectoral regulations provide additional sanctions. For e-communication operators, ICTA may issue a warning or impose an administrative fine of up to 1 per cent of their net sales from the previous calendar year, increasing to 3 per cent for violations involving personal data protection obligations, while non-operators face fines ranging from approximately 14,366 to 14.38 million Turkish liras.

For a personal data breach, the DPA may impose an administrative fine between 256,357 and 17.09 million Turkish liras (as at 2026) for failure to fulfil data security obligations and may order the data controller to rectify any violations or prohibit its data processing activities under certain circumstances.

For public institution controllers, administrative fines are not imposed; instead, disciplinary action must be taken against responsible personnel and the DPA must be notified of the consequences.

BRSA, CMB, TRCB and EMRA can also impose administrative fines within their respective sectors for non-compliance.

Law stated - 2 March 2026

Penalties for failure to report threats and breaches

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

The Cybersecurity Law penalises failure to report vulnerabilities and cyber incidents to the Cybersecurity Directorate without delay, imposing an administrative fine between 1.25 million Turkish liras and 12.55 million Turkish liras.

Law stated - 2 March 2026

Private enforcement

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

There is no specific regulation on private redress for unlawful cyberactivity. In cases of material damage, general tort and contract law may apply as appropriate. Parties may also claim compensation for non-pecuniary damage arising from infringement of personal rights and legal persons may seek such compensation for reputational harm.

If a cybersecurity breach concerns personal data, data subjects may seek redress from controllers and rely on general the tort law based on the violation of personal rights.

Law stated - 2 March 2026

THREAT DETECTION AND REPORTING

Internal policies and procedures

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

The Cybersecurity Law requires persons and institutions operating in cyberspace to comply with regulatory actions adopted by the Cybersecurity Directorate to enhance cybersecurity maturity. Additionally, public institutions and critical infrastructure service providers must comply with Presidency Decree and the Information and Communications Security Guideline. When processing personal data, controllers and processors must ensure an appropriate level of security. Sectoral regulations may impose information system-security obligations.

Law stated - 2 March 2026

Record-keeping requirements

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

Institutional Computer Emergency Response Teams (CERTs) of public institutions and critical infrastructure service providers must retain cyber events log records for at least one year unless provided otherwise in specific regulations.

E-communications operators must retain access records to critical and personal data systems for at least two years and maintain, for five years, annual report including information on information security breaches.

Payment and securities settlement system operators must keep information system audit trails and breach evidence for 10 years – including where system is outsourced.

Financial leasing, factoring and financing companies must store audit trails for at least three years, and payment and electronic money institutions must keep evidence of security breaches for at least 10 years.

Health information management system service providers must keep their log records for two to five years.

Law stated - 2 March 2026

Regulatory reporting requirements

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

Persons and institutions operating in cyberspace must report to the Cybersecurity Directorate any vulnerabilities and cyber incidents they detect. In case of a personal data breach, the controller must notify the DPA and affected data subjects. In critical infrastructure sectors, institutional CERTs must report cyber incidents to TR-CERT and the relevant sectoral CERTs. There are reporting requirements for specific sectors following a cyber incident. Yet there are no rules for attempted attacks or vulnerabilities.

Law stated - 2 March 2026

Time frames

What is the timeline for reporting to the authorities?

The relevant rules require prompt notification. There is no general time frame for reporting obligations except for personal data breaches, which must be notified to the DPA without delay and within 72 hours at the latest from the time when the data controller learns about the breach.

Law stated - 2 March 2026

Other reporting requirements

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

A cyber-attack affecting a public company must be disclosed to the public as per the Communiqué on Material Events Disclosure.

Law stated - 2 March 2026

UPDATE AND TRENDS

Recent developments and future changes

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

Cybersecurity has been a crucial part of Türkiye's strategic policies for the past decade, closely tied to national security. Türkiye has defined its cybersecurity strategy and objectives through various regulatory bodies' policy frameworks.

Since cybersecurity concerns various stakeholders, including private entities, public institutions and other state bodies, a key challenge in developing cybersecurity regulations is balancing these diverse interests. In this regard, companies can play a crucial role in shaping a favourable regulatory environment by working closely with public institutions, academia, non-governmental organisations and other stakeholders to strengthen national cybersecurity efforts.

The Cybersecurity Law provides a general legal framework for entities operating in cyberspace and defines the powers and duties of Cybersecurity Directorate, centralises cybersecurity-related authorities currently shared between the Ministry of Transport and Infrastructure and Information and Communication Technologies Authority.

The Cybersecurity Law covers public institutions, professional organisations, natural and legal persons and non-legal entities operating or providing services in cyberspace. It defines the concepts of cybersecurity, cyberspace and cyber-attack and establishes a Cybersecurity Board, whose duties include:

- developing policies, strategies, action plans and regulatory actions related to cybersecurity, and setting exemptions from certain decisions, if any;
- identifying priority areas for cybersecurity incentives and deciding on human resources development; and
- determining critical infrastructure sectors.

The Cybersecurity Law provides one year from 19 March 2025 for the secondary regulations to be enacted. These regulations are expected to provide more details on the scope and application of the Cybersecurity Law. The impact thereof will depend on these regulations and the Cybersecurity Directorate's approach.

Last, Criteria for Information Systems and Technology Infrastructures of Crypto Asset Service Providers was published by the Scientific and Technological Research Council of Türkiye on 8 May 2025, specifying crypto asset service providers' obligations under the CMB Communiqué.

Law stated - 2 March 2026