PANORAMIC

CYBERSECURITY

Türkiye

LEXOLOGY

Cybersecurity

Generated on: July 14, 2025

Contents

Cybersecurity

Recent developments and future changes

Contributors

Türkiye

YAZICIOGLU Legal

Bora Yazıcıoğlu	bora@yazicioglulegal.com
Kübra İslamoğlu Bayer	kubra@yazicioglulegal.com
Aslı Rabia Savaş	asli@yazicioglulegal.com
Beren Aşkın	beren@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 astandalone cybersecurity legal framework until very recently. 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.
- 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 the Cybersecurity Board. Additionally, the Cybersecurity Law introduces new categories of cybercrimes 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.
- 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.
- Presidential Decree No. 177, issued on 8 January 2025, established the Cybersecurity Directorate as a financially autonomous public legal entity under the Presidency, granting it general regulatory authority over cybersecurity matters. However, this directorate is yet to become fully operational.
- 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 institutions, organisations and businesses providing critical infrastructure services.
- The Communiqué on the Procedures and Principles for Connecting to and Auditing the KamuNet Network mandates public institutions and organisations to connect to KamuNet, a secure, closed-circuit virtual network with enhanced protection against cyber-attacks. All public institutions and organisations are obliged to employ the KamuNet network.
- The National Cybersecurity Strategy for 2024-2028, The 12th Development Program 2024-2028, Medium Term Program 2025-2027 and The Presidency Program 2025 are the latest policy documents outlining Türkiye's strategic goals and initiatives to enhance cybersecurity resilience.

Law stated - 15 Mayıs 2025

Most affected economic sectors

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

Special importance is dedicated to critical infrastructure sectors and systems. These are infrastructures that incorporate information technologies, and 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 operating in critical infrastructure sectors, these regulations also contribute to advancing cybersecurity within these sectors.

Currently, the critical infrastructure sectors include e-communications, finance, energy, transport, water management and critical public services (such as civil registration, land registration, taxation, commerce, social security and health). However, this list may be updated since the Cybersecurity Law grants the Cybersecurity Directorate and Cybersecurity

Board the power to determine critical infrastructures and the organisations and locations to which they belong.

Law stated - 15 Mayıs 2025

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, e-invoice services) and for public institutions and organisations. Notably, many organisations adopt this standard voluntarily to strengthen their cybersecurity practices.

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

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

- the Control Objectives for Information and Related Technologies standards in the banking and finance sectors;
- the 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 - 15 Mayıs 2025

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), that includes 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 (eg, regular vulnerability assessments, penetration testing, regular data backups and regular personnel training). The BoD may be held responsible for breaching its duty of care in the case of violations thereof.

Similar obligations may be found in sectoral 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 be subject to 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 Management of Information Systems that was replaced by the Communiqué on the Procedures and Principles of Information Systems Management on 30 June 2025. 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 and creditors or risk dismissal if they breach their duty of care.

The BoD members may face imprisonment or a judicial fine for unauthorised sharing or disclosing of trade secrets, banking secrets or consumer secrets. BoD members may face imprisonment for personal data-related offences, if committed pursuant to managerial instructions, BoD decisions or established company practices.

Law stated - 15 Mayıs 2025

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 the 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'.

The existing legislation does not define cybercrime. However, cybercrime refers to crime targeting the 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 - 15 Mayıs 2025

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. The protective measures may be found under 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 to be used in critical infrastructures must be procured from experts and companies certified by the Cybersecurity Directorate. Non-compliance with this obligation is subject to an administrative fine between 1 million and 10 million Turkish liras. The minimum technical criteria for the cybersecurity products and services to be used 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 institutions, organisations, 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 - 15 Mayıs 2025

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 - 15 Mayıs 2025

Cyberthreats to critical infrastructure

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

A comprehensive regulatory framework for critical infrastructure cybersecurity is yet to be fully established, pending secondary legislation under the Cybersecurity Law. However, various policy documents and sector-specific by-laws are currently in place.

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 stands as a key regulation, setting 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 - 15 Mayıs 2025

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 TCrC prescribes criminal penalties for violating the confidentiality of communications, interception of and recording conversations between individuals, 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 prosecutor's order to obtain evidence of committed or ongoing crimes. However, it applies only to certain offences excluding cybercrimes.

Law stated - 15 Mayıs 2025

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, giving to others or keeping forbidden devices and software that are used to break a computer program's password or a code as such in order to commit a crime described in the bullet points above;
- committing theft or fraud via cyber-systems;
- unlawful recording, 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 that commit these offences to secure an undue advantage.

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.

Law stated - 15 Mayıs 2025

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, and secure communication protocols).

Cloud service providers must also meet specific security criteria (eg, protection against DDoS attacks, 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).

Law stated - 15 Mayıs 2025

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 (including banks, payment institutions, electronic money institutions, financial leasing, factoring and finance companies) and e-communications, the organisations must be established in Türkiye. Similarly, certain social network providers are required to appoint a representative in Türkiye. There are specific localisation requirements for both local and foreign organisations that extend to these industries.

Law stated - 15 Mayıs 2025

BEST PRACTICE

Recommended additional protections

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

The Cybersecurity Directorate is yet to publish any guidelines.

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

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 including a collaboration 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 Ministry of Transport and Infrastructure to assess the cybersecurity measures and activities undertaken by public institutions and organisations, as well as private sector representatives.

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

Law stated - 15 Mayıs 2025

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 yet to be determined, there are currently no incentives in place.

Law stated - 15 Mayıs 2025

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.

The Institutional CERTs Guideline and the Sectoral CERTs Guideline also provide guidance in cybersecurity as a code of practice for their relevant organisations. Organisations may implement these guidelines according to their specific capabilities.

Law stated - 15 Mayıs 2025

Responding to breaches

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

Aside from the mandatory reporting requirements under relevant legislation, 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 - 15 Mayıs 2025

Voluntary information sharing

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

There are no regulations for voluntary information sharing.

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

Law stated - 15 Mayıs 2025

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.

It was created with the involvement of public institutions, private companies, and academic organisations, with support from the Secretariat of Defence Industries. These entities work together through joint efforts to identify needs, develop innovative solutions and establish cybersecurity standards.

In practice, regulatory authorities may engage stakeholders in preparing sectoral regulations by discussing and 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 - 15 Mayıs 2025

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 small and medium-sized enterprises – and its adoption is widespread. However, in practice, insurance policies often exclude organisations operating in industries where potential cyber risks are considered high (eg, finance, health except pharmacy, e-commerce, IT, maritime and aviation industries).

Law stated - 15 Mayıs 2025

ENFORCEMENT

Regulatory authorities

Which regulatory authorities are primarily responsible for enforcing cybersecurity rules?

Recently, the Cybersecurity Directorate was established as the general regulatory authority for cybersecurity matters. However, the powers of current regulators will prevail until units within the Directorate are established and become 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, the Presidency of Defence Industries, and the 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
- the Nuclear Regulatory Authority.

Law stated - 15 Mayıs 2025

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 pursuant to 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.

ICTA is authorised to audit and investigate on 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.

R-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 Data Protection Authority's (DPA) conducts investigations ex officio or upon complaint. Data controllers are obliged to 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, including documents, data and records 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 - 15 Mayıs 2025

Most common enforcement issues

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

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 - 15 Mayıs 2025

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 detected in their service areas.

If a cybersecurity breach constitutes a personal data breach, data controllers must report to the DPA promptly and no later than 72 hours after becoming aware of the situation. Data subjects affected must also be notified even if there is no risk to the rights and freedoms thereof.

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

- Institutional CERTs of critical infrastructure organisations must notify TR-CERT and the relevant sectoral CERTs without delay.

- Operators of e-communications must immediately notify ICTA if a cybersecurity breach affects more than 5 per cent of their subscribers or interrupts the business continuity. Additionally, operators must notify their customers or users of specific threats to their network and service security promptly.
- Banks must report cyber incidents to the BRSA.
- In the healthcare sector, the Ministry of Health has a central breach notification portal.

Law stated - 15 Mayıs 2025

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 provides an administrative fine between 1 million and 10 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.

There are also sectoral regulations in place.

Non-compliance by e-communications operators may result in 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 11,448 to 11,459,756 Turkish liras. ICTA may only issue a warning upon its discretion.

For a personal data breach, the DPA may impose an administrative fine between 204,285 and 13,620,402 Turkish liras (as at 2025) on grounds of failure to fulfil the obligations of data security. The DPA may also order the data controller to rectify any violations or prohibit its data processing activities under certain circumstances.

For public institution controllers, the DPA does not impose administrative fines. Instead, disciplinary action must be taken against the relevant personnel with due procedure and the DPA must be notified of the consequence thereof.

BRSA, CMB, TRCB and EMRA can also impose administrative fines on the institutions of their respective sectors for non-compliance.

Law stated - 15 Mayıs 2025

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 million and 10 million Turkish liras.

Law stated - 15 Mayıs 2025

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 the event of material damage, general tort law and contracts law may be applied to, as appropriate. Parties may also claim compensation for non-pecuniary damage for infringement of their personal rights. Legal persons may claim non-pecuniary damage for loss of reputation.

If a cybersecurity breach concerns personal data, data subjects may seek redress from controllers. They may also apply to the general rules under the tort law on the basis of violation of personal rights.

Law stated - 15 Mayıs 2025

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 that are taken 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. In the case of processing of personal data, controllers and processors must ensure an appropriate level of security. Lastly, sectoral regulations may impose information system-security obligations.

Law stated - 15 Mayıs 2025

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 keep log records of cyber events. Records must be stored at least for one year unless provided otherwise in specific regulations.

E-communications operators must keep records of access to their critical and personal data-related systems and store them for at least two years. They must also prepare and keep for five years an annual report including information on information security breaches.

Payment and securities settlement system operators must keep audit trails of their information systems and any evidence of breach for 10 years – even if the 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 - 15 Mayıs 2025

Regulatory reporting requirements

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

Persons and institutions operating in cyberspace are required to report to the Cybersecurity Directorate any vulnerabilities and cyber incidents they detect in the field in which they provide services. In case of a personal data breach, the controller must notify the Data Protection Authority's (DPA) and affected data subjects. In critical infrastructure sectors, institutional CERTs must reported 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 - 15 Mayıs 2025

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 - 15 Mayıs 2025

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 - 15 Mayıs 2025

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, from private entities to public institutions and other state bodies, one of the principal challenge to developing cybersecurity regulations is balancing and covering these varying 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.

For 2025, the most important development is the Cybersecurity Law, which was published on the Official Gazette and became effective on 19 March 2025. It provides a general legal framework for entities operating in cyberspace and the powers and duties of Cybersecurity Directorate. It centralises cybersecurity-related powers and duties that are 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 that exist, operate and provide services in cyberspace. It defines the concepts of cybersecurity, cyberspace and cyber-attack. The law 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 a one-year period 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.

Law stated - 15 Mayıs 2025