Legal 500
Country Comparative Guides
Hot Topic | TMT

Türkiye's Cybersecurity Law: Cyber Governance, Resilience and Accountability

Contributor

AFG LEGAL

Ali Feyyaz Gül

Founding Partner | ali@afg-legal.com

For a full list of jurisdictional Q&As & hot topic articles visit **legal500.com/guides/**

Türkiye's Cybersecurity Law Cyber Governance, Resilience and Accountability

I. Introduction

On 19th March 2025, Law No. 7545 on Cybersecurity (the "**Cybersecurity Law**") was published in the Official Gazette and entered into force on the same date. It is Türkiye's first dedicated law addressing cybersecurity on a horizontal basis and introduces a more structured legal framework for the management of cyber risk.

The Cybersecurity Law also confirms a broader shift in how cybersecurity is expected to be managed. Cybersecurity can no longer be treated only as a technical matter for IT teams or as a secondary component of personal data protection compliance. It now forms part of legal governance, operational resilience, regulatory compliance and, in some cases, transaction planning.

This development did not emerge in isolation. Cybersecurity has been a recurring priority in Türkiye's strategic policy documents for more than a decade. The National Cybersecurity Strategy for 2024–2028 identifies cyber resilience, proactive cyber defence, secure use of technology, domestic cybersecurity capacity and international reputation among Türkiye's main cybersecurity objectives. The 12th Development Programme for 2024–2028 expressly refers to regulations to be enacted in line with the EU's Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union ("**NIS2 Directive**") and international best practices. The Medium-Term Programme for 2025–2027 similarly refers to dedicated cybersecurity legislation and secondary regulations aligned with relevant EU legislation, while the 2026 Presidential Annual Programme refers to legislative work in line with the EU legal framework. Türkiye's international positioning has also improved in this area: the International Telecommunication Union's Global Cybersecurity Index 2024 ranked Türkiye as a Tier-1 "role-modelling" country.

Seen against this background, the Cybersecurity Law follows a direction that is conceptually close to the NIS2 Directive in several respects. It seeks to strengthen cyber resilience, establish institutional coordination, introduce incident notification duties and focus on critical infrastructure. However, the comparison should not be overstated. Türkiye has not simply transposed the NIS2 Directive. The Cybersecurity Law reflects domestic priorities, including national security, institutional control and the regulation of the cybersecurity market. Still, the NIS2 Directive is likely to be an important reference point when secondary legislation, technical standards and practical guidance are developed.

For international businesses, the regime may also have implications beyond ordinary local compliance where they have a Turkish presence or where their Turkish operations interact with regulated or critical infrastructure environments. This is because the Cybersecurity Law introduces Türkiye-specific obligations on notification, cooperation with the Cybersecurity Directorate, certification of certain cybersecurity products and services, and approval or notification requirements for certain transactions in the cybersecurity sector. Global cybersecurity policies based on the GDPR and NIS2 Directive may provide a useful starting point but should be tested against these local requirements.

 © 2026 Legalease Ltd

II. From Information Security to Cyber Resilience

The Cybersecurity Law reflects a regulatory shift from traditional information security towards cyber resilience.

Information security has traditionally been framed around the confidentiality, integrity and availability of information. These principles remain essential. The Cybersecurity Law, however, adopts a broader approach. Its purpose is not limited to system protection; it also covers the identification and elimination of existing and potential internal and external cyber threats, the mitigation of the possible effects of cyber incidents, the adoption of regulations to protect public and private actors against cyber-attacks, and the development of strategies and policies to strengthen Türkiye's cybersecurity.

This broader statutory purpose has practical consequences. If the Cybersecurity Law is concerned not only with prevention, but also with mitigation, response and resilience, organisations must be able to manage cyber incidents as legal and operational events, not merely as technical disruptions. A ransomware attack may disrupt operations, expose personal data, trigger contractual defaults, create regulatory notification duties, raise evidence preservation issues, affect insurance coverage and involve criminal law considerations. A vulnerability in a third-party system may affect the continuity of a regulated service. Failure to maintain adequate logs may make it difficult to establish what happened, when it happened and whether the organisation acted with due care.

This is where the Cybersecurity Law's accountability principle becomes particularly important. The Cybersecurity Law should not be understood only as a set of rules aimed at preventing attacks. It is also concerned with preparation, response, recovery and the ability to demonstrate compliance. Regulators, courts, contractual counterparties and affected persons may increasingly ask whether an organisation had a defensible governance framework, whether responsibilities were properly allocated, and whether the organisation can document the steps taken before, during and after an incident.

III. The Cybersecurity Directorate

A central feature of the new regime is the Cybersecurity Directorate ("**Directorate**"). The Directorate has been established as the main public authority responsible for cybersecurity policy, coordination, standards, certification, audits, incident-related processes and the strengthening of national cyber resilience.

The Directorate's powers are extensive. They include determining standards, carrying out or commissioning audits, requesting information and documents, setting criteria for cybersecurity products and services used in public institutions and critical infrastructures, conducting certification processes and supporting cooperation between the public sector, private sector and academia.

This institutional structure changes how businesses should approach regulatory engagement. Under the previous framework, cybersecurity obligations were dispersed across sectoral rules and different authorities. The Cybersecurity Law creates a more centralised cybersecurity authority, while leaving room for existing sectoral regulators to continue exercising their own powers. In practice, businesses may therefore face a layered regulatory environment rather than a complete replacement of existing rules.

 © 2026 Legalease Ltd

At the time of writing, a bill submitted to the Grand National Assembly of Türkiye on 3 July 2026 proposes further consolidation of digital and cybersecurity-related powers under the Directorate. If enacted, the bill would transfer certain powers historically exercised by the Information and Communication Technologies Authority, including powers relating to domain names, internet infrastructure and technical systems supporting the detection and analysis of communications, to the Directorate. The significance of the proposal is not only administrative. It indicates that functions previously treated as part of telecommunications and internet regulation may increasingly be reframed as elements of national cybersecurity governance.

IV. Scope and Regulatory Prioritisation

The Cybersecurity Law is drafted broadly. It applies to public institutions and organisations, professional organisations with public institution status, natural and legal persons, and entities without legal personality that exist, operate or provide services in cyberspace. Certain intelligence, defence and security-related activities carried out under specific laws are expressly excluded from its scope.

This broad wording is one of the Cybersecurity Law's most significant features. In principle, it may reach a wide range of actors operating in cyberspace. That said, compliance expectations are unlikely to be identical for every organisation. The practical scope and intensity of compliance will largely depend on secondary legislation, technical standards and guidance to be issued by the Directorate. These instruments are expected to be particularly important in determining how obligations will apply across different sectors, risk levels and categories of actors.

Secondary legislation has not yet been published. However, statements by the Directorate indicate that a risk-based and proportionate compliance approach is expected to be adopted. In practice, factors such as the field of activity, institutional capacity and criticality of the relevant services may become relevant in determining the applicable compliance level. Forthcoming regulations, communiqués and guidance are expected to clarify key implementation issues, including the classification of obliged entities, audit mechanisms, certification and authorisation processes, and the incident notification procedure. In this respect, the secondary legislation may draw on concepts familiar from NIS2 Directive, such as differentiated categories of entities and proportionate obligations based on risk and criticality, although the Turkish framework may ultimately adopt its own terminology and thresholds.

The Cybersecurity Board ("**Board**") has already taken an important step in this direction. At its meeting on 5th May 2026, the Board determined the critical infrastructure sectors, expanding the pre-existing list to include digital infrastructures, digital services, electronic communications, energy, finance, food and agriculture, manufacturing, public services, media and crisis communications, postal and cargo services, healthcare, defence industry, water management, transportation and space. Further detail is still expected from the Directorate regarding the specific infrastructures, entities and technical criteria within these sectors.

The result is an emerging risk-based compliance landscape rather than a one-size-fits-all regime. While the general scope of the Cybersecurity Law is wide and all actors operating in cyberspace should be prepared to adopt reasonable cybersecurity measures, the practical level of scrutiny and compliance burden is expected to depend on the categories, criteria and thresholds to be introduced by secondary

 © 2026 Legalease Ltd

legislation. Pending those details, organisations operating critical or regulated services, organisations providing cybersecurity products or services for public institutions or critical infrastructures, and companies active in the cybersecurity market are likely to require closer attention.

Businesses should therefore begin with a scope and exposure analysis. Relevant questions include whether the organisation operates in a sector already subject to cybersecurity or information security rules, whether it provides cybersecurity products or services to public institutions or critical infrastructures, whether it provides other technology services into a regulated environment subject to sector-specific information security or outsourcing rules, and whether a cyber incident could affect service continuity, contractual obligations or regulated activities.

V. Core Obligations for Businesses

The Cybersecurity Law introduces several obligations that are particularly relevant from a business perspective.

First, organisations within scope must cooperate with the Directorate. This includes providing requested data, information, documents, software, hardware and other relevant materials within the scope of the Directorate's duties. Failure to provide information, documents, data or technical materials requested by authorised bodies may lead to serious consequences, including criminal liability in certain cases.

Second, relevant actors must take the cybersecurity measures required under applicable legislation. The content of this obligation will not be determined by the Cybersecurity Law alone.

Nevertheless, several sectors are already subject to detailed information security, operational resilience, outsourcing, data localisation, penetration testing, incident management or reporting requirements under sector-specific rules. For example, banks and other financial institutions are subject to information systems and electronic banking rules issued by the Banking Regulation and Supervision Agency; payment and electronic money institutions are subject to Central Bank rules; capital markets institutions are subject to the Capital Markets Board's Communiqué on Information Systems Management; electronic communications operators, energy market participants, healthcare actors and civil aviation enterprises are also subject to their own cybersecurity or information security requirements.

In addition, where personal data is processed, the Turkish Personal Data Protection Law imposes a general obligation on data controllers to take necessary technical and organisational measures to ensure an appropriate level of security and to prevent unlawful processing of, and unlawful access to, personal data.

The forthcoming secondary legislation, technical standards and guidance under the Cybersecurity Law will need to be read together with these existing sectoral regimes and data protection requirements.

Third, organisations must notify the Directorate of vulnerabilities or cyber incidents detected in their service area. The Cybersecurity Law refers to notification without delay, but the timing, form and procedure of such notifications will need to be clarified through secondary legislation and regulatory practice. Businesses should not wait for an incident to design this process. Internal escalation rules, legal assessment steps and evidence preservation protocols should be prepared in advance.

 © 2026 Legalease Ltd

Fourth, cybersecurity products, systems and services used in public institutions and critical infrastructures must be procured from experts, manufacturers or companies authorised and certified by the Directorate.

Fifth, cybersecurity companies subject to certification, authorisation and documentation requirements must obtain approval before commencing their activities. This reflects the sensitive nature of cybersecurity services. Providers may gain access to confidential systems, vulnerabilities, logs, data and business-critical infrastructure.

Finally, the Cybersecurity Law introduces specific rules for companies producing cybersecurity products, systems, software, hardware or services. Certain transactions, including mergers, demergers, share transfers and sales, must be notified to the Directorate. Where a transaction grants direct or indirect control or decision-making power, approval may be required. Transactions carried out without the required approval may not become legally valid.

VI. NIS2 Directive as a Practical Reference Point

Although the Cybersecurity Law has its own structure and policy choices, NIS2 Directive is likely to influence Turkish practice.

NIS2 Directive is relevant because it addresses many of the regulatory questions that Türkiye will need to resolve through secondary legislation. These include how entities should be classified, how different risk levels should be distinguished, what proportionate security measures should look like, how incident notification should be structured, how supply chain security should be regulated, how audit powers should be exercised and how management accountability should be framed.

One of the most important lessons from NIS2 Directive is proportionality. NIS2 Directive does not treat all entities in the same way. It distinguishes between essential and important entities, introduces different supervisory approaches and links obligations to risk. Turkish secondary legislation may develop a similar approach, particularly because the Cybersecurity Law itself has a broad general scope.

Management accountability is another important point. NIS2 Directive expressly brings cybersecurity risk management closer to the responsibility of management bodies. The Turkish Cybersecurity Law does not reproduce NIS2 Directive wording, but its emphasis on accountability, cooperation, continuity, sustainability and the responsibility of all stakeholders points in a similar direction. In practice, cybersecurity governance will increasingly need to be visible at senior management level.

However, businesses should avoid assuming that NIS2 Directive-based compliance will automatically satisfy Turkish requirements. NIS2 Directive may help with methodology, but Turkish law will determine the actual notification, cooperation, certification and approval obligations.

VII. Incident Response, Data Protection and Suppliers

One of the most important practical consequences of the new regime is the need to coordinate incident response across multiple legal frameworks.

 © 2026 Legalease Ltd

A cyber incident may trigger notification obligations under the Cybersecurity Law. If personal data is affected, notification obligations under the Turkish Personal Data Protection Law may also arise. In regulated sectors, separate notification obligations may apply to sectoral authorities. For example, electronic communications operators, banks, capital markets institutions, healthcare actors and civil aviation enterprises may each be subject to separate incident reporting obligations under their own sectoral frameworks.

Depending on the facts, contractual notice obligations, public disclosure considerations, criminal complaint issues and insurance notification requirements may also need to be considered.

Incident response is therefore a legal governance issue, not only a technical exercise. Businesses should have an internal playbook identifying who assesses the incident, who preserves evidence, who determines whether personal data is affected, who manages communication with authorities and who approves notifications.

The new regime also increases the importance of supplier governance. Cybersecurity risk often enters organisations through third parties, including outsourced technology providers, software vendors, maintenance contractors, managed security providers, consultants and other operational partners. Supplier contracts should therefore be reviewed to determine whether they adequately address security standards, audit rights, incident notification timelines, cooperation obligations, evidence preservation, subcontractor controls, access management, business continuity, data location, regulatory cooperation and liability allocation.

A contract cannot eliminate regulatory responsibility. However, properly drafted supplier obligations can help an organisation demonstrate that it took reasonable steps to manage third-party risk and maintain operational resilience.

VIII. Transactions and Foreign Investment

One of the more distinctive features of the Cybersecurity Law is its treatment of cybersecurity products and service providers.

The Cybersecurity Law does not treat the cybersecurity market as an ordinary technology market. This is understandable. Cybersecurity providers may have privileged access to customer systems. Their products may operate deep within technical infrastructure. Their personnel may identify vulnerabilities, examine sensitive logs, access confidential data or support incident response. Trust in these providers is therefore a regulatory concern.

The transaction-related obligations introduced by the Cybersecurity Law create a new diligence item for buyers and investors. They will need to consider whether the target's activities fall within the relevant categories, whether notification or approval is required, whether past transactions were properly handled and whether regulatory approvals may affect timing or closing conditions.

This is particularly relevant for foreign investors and strategic buyers. In transactions involving Turkish cybersecurity companies, or businesses providing cybersecurity products or services into Türkiye, regulatory notification and approval requirements should be assessed at an early stage. These issues may

 © 2026 Legalease Ltd

affect transaction structuring, conditions precedent, closing timelines and post-closing integration.

IX. What Businesses Should Do Now

The most sensible approach is staged and risk-based.

Businesses should begin with a scope and exposure assessment. This should identify whether the organisation falls within the general scope of the Cybersecurity Law, whether it operates in or supports a regulated or critical environment, whether it provides or procures cybersecurity products or services, and whether certification, authorisation or transaction approval requirements may apply.

The next step is to map applicable cybersecurity measures. This exercise should not be limited to the Cybersecurity Law. Businesses should assess existing sector-specific information security, outsourcing, operational continuity, incident management and reporting requirements, as well as data protection security obligations under the Turkish Personal Data Protection Law. Once secondary legislation and technical standards are issued by the Directorate, these should be integrated into the same gap analysis.

Businesses should also prepare for regulatory cooperation. Since the Cybersecurity Law allows the Directorate and authorised bodies to request information, documents, data, software, hardware and other technical materials, organisations should determine in advance who will receive, assess and respond to such requests, and how legal privilege, confidentiality, personal data and trade secrets will be handled.

Incident notification obligations should be mapped separately. This should cover the Cybersecurity Law, data protection rules, sectoral obligations, contractual notification duties and internal reporting lines. The aim should be to create a practical notification matrix that can be used during a crisis, not merely a theoretical compliance document.

Cybersecurity governance documents should also be reviewed. Policies should allocate roles and responsibilities clearly. Incident response plans should be tested. Legal, compliance, IT, information security, communications and management teams should know how they are expected to work together before an incident occurs.

Supplier and procurement processes require particular attention. Businesses should review whether cybersecurity products, systems or services used in public institutions or critical infrastructures must be procured from authorised or certified providers. More generally, supplier contracts should be reviewed where vendors have access to important systems, regulated data, sensitive information or operational infrastructure.

Companies active in the cybersecurity market should separately assess whether their activities may trigger certification, authorisation, approval or notification requirements. Transaction planning should also take these rules into account, particularly where mergers, demergers, share transfers, sales or other arrangements may result in a change of control or decision-making power.

Finally, cyber risk should be reported to senior management in a clear and usable format. A concise board-level report is often more valuable than a lengthy technical document. Decision-makers should be able to understand material risks, resource needs, regulatory exposure and remediation priorities.

 © 2026 Legalease Ltd

X. Outlook

The Cybersecurity Law is more than a technical regulation. It is part of a broader legal and institutional shift in which cybersecurity is treated as a matter of governance, resilience and public interest.

The full impact of the Cybersecurity Law will depend on secondary legislation, technical standards and the practice of the Directorate. NIS2 Directive is likely to provide a useful reference point, especially on proportionality, entity classification, incident reporting, supply chain security and management accountability. Turkish practice, however, will also reflect domestic priorities, including national security, public order, critical infrastructure protection and the development of local cybersecurity capacity.

The bill submitted to Parliament in July 2026 also suggests that institutional reform in the digital sphere may continue. Businesses should therefore monitor not only secondary legislation under the Cybersecurity Law, but also broader reforms that may reshape the boundaries between cybersecurity, internet governance and electronic communications regulation.

International businesses should treat Turkish cybersecurity compliance as part of their wider regional and global cyber governance framework, rather than as an isolated local-law issue.

Companies that approach the Cybersecurity Law as a one-off compliance exercise are likely to fall short. The better approach is to build governance structures that can adapt as legal, technical and regulatory expectations evolve. In that sense, the Cybersecurity Law should be seen not only as a new compliance obligation, but also as an opportunity to connect legal oversight, technical resilience and business continuity within the same governance framework.

Contributors

Ali Feyyaz Gül
Founding Partner
ali@afg-legal.com

 © 2026 Legalease Ltd