Turkey | March 2025

Turkish cyber security law has entered into force.

The long-awaited Turkish Cyber Security Law ("**Law**") was published in the Official Gazette on 19 March 2025. This Law establishes fundamental principles and objectives for ensuring nationwide cybersecurity and defines the roles and responsibilities of public institutions regarding cybersecurity in Türkiye.

The Law primarily applies to companies operating in critical infrastructure sectors ("**Critical Infrastructure Sectors**"), as well as legal entities, individuals, and organizations operating in cyberspace with or without legal personality ("**Relevant Institutions**"). Additionally, it covers public institutions ("**Public Institutions**") that use software, hardware, products, and services ("**Cyber Security Products**") affecting their cybersecurity infrastructure. It also applies to independent auditors conducting cybersecurity audits ("**Auditors**").

The Law designates the Cyber Security Presidency ("**Presidency**") as the primary authority responsible for cybersecurity across Türkiye and assigns it key duties. The Presidency is also authorized to identify Critical Infrastructure Sectors.

Key Provisions of the Law are as follows:

1. Measures for Ensuring Cybersecurity

Cyber Security Products

The Presidency will conduct certification, authorization and documentation processes for Relevant Institutions offering Cyber Security Products-related services and will establish minimum security criteria for Cyber Security Products. Relevant Institutions offering Cyber Security Products-related services wish to sell such products abroad, they must obtain authorization from the Presidency before operating.

Cyber Attacks

The Presidency is responsible for assessing cyberattacks occurring within Türkiye's cyberspace, implementing mitigation measures, and providing intelligence on cyber incidents. Relevant Institutions must comply with Presidency directives regarding the installation of software and hardware necessary for defense against cyberattacks. The Presidency is authorized to collect,

store, and analyze system-generated data and log records to investigate cyber incidents and may share findings with legal authorities or other relevant parties when necessary.

Cyber Security Audits

The Presidency, alongside authorized independent Auditors, will be able to conduct cybersecurity audits before Relevant Institutions and Public Institutions due to the transactions falling under the scope of the Law. The audits will be carried out by the Presidency or authorized Auditors. The Presidency and Auditors are authorized to conduct searches in residences, workplaces, and non-public areas within the scope of these audits. A judge's decision is required for such searches. In urgent cases where delays are inconvenient, searches may be conducted based on written permission from a public prosecutor.

2. Obligations Stipulated in the Law

The Law outlines several key obligations for Relevant Institutions and the Presidency, including:

- Individuals engaging in activities without the required approvals, permits or authorizations pursuant to the Law are subject to imprisonment and judicial fines.
- Individuals who fail to provide requested information, documents, software, data, or hardware related to cybersecurity audits, or obstruct their collection, will be subject to imprisonment, judicial fines and administrative fines.
- Relevant Institutions that fail to report cybersecurity vulnerabilities or cyber incidents to the Presidency in a timely manner and organizations from the Critical Infrastructure Sector that procure Cyber Security Products from suppliers not authorized by the Presidency will face administrative fines.

3. Obligations regarding Cyber Security Products and Relevant Institutions

Compliance with the rules set by the Presidency is required for the sale of Cybersecurity Products abroad. In this regard, for Cybersecurity Products subject to sales authorization, prior approval must be obtained from the Presidency before the sale transaction.

Additionally, companies producing Cybersecurity Products must notify the Presidency in cases of mergers, demergers, share transfers, or sales transactions. For certain transactions, obtaining approval from the Presidency is mandatory.

4. Transition and Compliance Deadlines

The law entered into force upon its publication in the Official Gazette, and the Relevant Institutions are expected to comply with their cybersecurity obligations. However, if cybersecurity activities require authorization or certification by the Presidency, these procedures must be completed in accordance with the Presidency's instructions within one year from the date of publication of the secondary legislation. It is stipulated that commercial companies failing to complete the authorization and certification procedures within this period shall be prohibited from engaging in cybersecurity-related activities.

Please contact us if you require further information regarding this new cybersecurity legislation.