ELİG
GÜRKAYNAK
Attorneys at Law

A New Era for Cybersecurity in Turkiye: Key Takeaways from Cybersecurity Law

Authors: Dr. Gönenç Gürkaynak, Ceren Yıldız Özgökçen, Yasemin Doğan and Ece Oğur

Turkiye has taken an important step toward reinforcing its national cybersecurity architecture with the enactment of **Cybersecurity Law No. 7545 ("Cybersecurity Law")**, which entered into force upon its publication in the Official Gazette numbered 32846 and dated March 19, 2025.

Cybersecurity Law establishes a legal, institutional, and technical foundation for addressing cyber risks, securing critical infrastructure, and aligning national cybersecurity practices with emerging global standards.

I. Scope and Application

The scope of Cybersecurity Law is extensive, it applies to public institutions and organizations, professional organizations in the nature of public institutions, real and legal persons and entities without legal personality that exist, operate and provide services in cyberspace.

Cybersecurity Law is particularly focused on the protection of critical infrastructure, which is broadly defined to include sectors such as energy, finance, communications, transportation, water utilities and health. Entities operating in these sectors are subject to stringent cybersecurity obligations, including mandatory risk assessments, reporting duties and incident response preparedness.

II. Institutional Structure and Strategic Governance

A cornerstone of the new legal framework is the institutional reorganization of Türkiye's cybersecurity governance. Cybersecurity Law regulates two primary bodies: Cybersecurity Council ("**Council**") and Cybersecurity Presidency ("**Presidency**").

Chaired by the President of the Republic, the Council is the highest policy-making authority on national cyber security. The Council is responsible for developing the national cybersecurity strategy, setting priorities and ensuring inter-agency coordination.

The newly established Presidency, which complements the Council, became effective on January 8, 2025, with Presidential Decree No. 177. It is authorized to develop technical standards, certify cybersecurity products and services, oversee sectoral compliance, support capacity building and coordinate incident response mechanisms among critical infrastructure operators and digital service providers.

III. Regulatory Obligations for the Private Sector

Private sector entities, especially those identified as part of the national critical infrastructure, are required to comply with a number of substantial obligations established under Cybersecurity Law. These obligations include:

- Timely submission of all kinds of data, information, documents, hardware, software and all other contributions requested by the Presidency within the scope of its duties and activities;
- Immediate reporting of any vulnerability or cyber incidents and taking the measures required by the legislation for cybersecurity;
- Use of authorized and certified cybersecurity products, systems, and services for public institutions and entities, and critical infrastructures;
- Obtaining the approval of the Presidency for cybersecurity companies subject to licensing, authorization, or certification before initiating their activities; and
- Implementation of policies, strategies, action plans developed by the Presidency.

In addition, the Cybersecurity Law strengthens the strong cooperation and obliges the Presidency to work in collaboration with all relevant actors in the fulfillment of its activities.

IV. Compliance Considerations for Entities

In light of the new legal framework, entities operating in Turkiye should assess their current cybersecurity posture. This includes (i) reviewing and upgrading internal cybersecurity policies and technical controls, (ii) initiating engagements with legal and technical advisors to prepare for potential audits or regulatory requests, and (iii) confirming whether existing products and services meet the Directorate's certification requirements.

Especially for multinational entities operating in Turkiye, certification and localization requirements may require adjustments to procurement strategies, vendor selection processes and cross-border data governance frameworks.

V. Enforcement Mechanisms and Sanctions

Cybersecurity Law contains strong enforcement mechanisms for non-compliance, including both administrative and criminal sanctions. Failure to provide requested information, obstruction of surveillance or conducting unauthorized cybersecurity operations can result in prison sentences, as well as significant judicial fines.

Persons who unauthorizedly make available, share or sell personal or institutional data previously compromised by a cyber incident can face three to five years in prison. This includes critical information related to public services. In addition, those who knowingly fabricate or disseminate false information about a cyber incident, despite knowing that no such breach has occurred, with the aim of creating public fear, panic or discrediting institutions or persons, may be sentenced to imprisonment from two to five years.

VI. Conclusion

Cybersecurity Law marks a significant step forward in Turkiye's regulatory approach to cybersecurity. It not only centralizes Turkiye's cybersecurity governance under a national authority but also introduces detailed obligations for private sector actors that form an integral part of the Turkiye's digital ecosystem.

For entities operating in or with Turkiye, complying with this new Cybersecurity Law is an opportunity to build robust, secure and reliable digital infrastructures aligned with Turkiye's long-term vision of digital sovereignty and national security, not just a matter of avoiding sanctions.

Article Contact: Dr. Gönenç Gürkaynak E-mail: gonenc.gurkaynak@elig.com

(First published by Mondaq on June 2, 2025)