LBF Partners

SIGNIFICANT MILESTONE IN CYBERSECURITY

Law No. 7545 on Cybersecurity Has Come into Force

www.lbfpartners.com

LBF Partners

SIGNIFICANT MILESTONE IN CYBERSECURITY
Law No. 7545 on Cybersecurity Has Come into Force

A. Introduction

The Cybersecurity Law No. 7545 ("Law"), enacted to counter cyber threats and mitigate the potential impacts of cyber incidents, was published in the Official Gazette dated 19 March 2025 and numbered 32846, thereby entering into force.

B. Significant Regulations Introduced by the Law

The purpose of the Law can be summarized as establishing the fundamental principles for identifying internal and external threats to ensure Türkiye's cybersecurity, mitigating the impact of cyber incidents, and setting out general principles to protect both the public and private sectors against cyberattacks.

The scope of the Law includes public legal entities, private legal entities, and natural persons, while intelligence activities are excluded as an exception.

1. Presidency of Cybersecurity

Grounded in the principle that cybersecurity is an integral part of national security, the Law assigns various duties to the Presidency of Cybersecurity ("**Presidency**") to ensure cybersecurity. The key duties among these are as follows:

- To carry out activities aimed at protecting critical infrastructures which host information systems where a loss of confidentiality, integrity, or availability of the data they process may result in loss of life, large-scale economic damage, security vulnerabilities, or disruption of public order—and information systems against cyberattacks, as well as preventing such attacks and mitigating their impacts.
- To identify critical infrastructures along with the institutions they belong to and their locations.
- To establish or have established, operate or have operated the necessary infrastructures to ensure the cybersecurity of public institutions and critical infrastructures.
- To provide or ensure the provision of hosting services to public institutions and organizations through secure systems and infrastructures.
- To establish, have established, supervise Cyber Incident Response Teams (**CIRT**), and enhance their response capabilities through exercises and drills.
- To establish standards in the field of cybersecurity and carry out testing and certification processes.

The Presidency is also authorized to carry out the following tasks and procedures while performing the duties assigned to it under the Law:

- To take or have taken preventive measures against cyberattacks in order to ensure the protection of institutions covered by the Law.

- To provide on-site or remote incident response support to entities subject to cyberattacks, to trace attack footprints, gather evidence, and in cases of suspected criminal activity, share such evidence with the relevant authorities and ensure local and international coordination.
- To obtain, assess, and use information, documents, and data related to its activities for a maximum period of two years, and subsequently destroy them.
- To collect, store, analyze log records from information systems, and prepare reports to be shared with the relevant authorities.

The Law further stipulates that the procedures and principles regarding the exercise of the Presidency's powers shall be determined by a regulation to be issued.

2. Duties and Responsibilities

The Law sets out the cybersecurity-related duties and responsibilities of those who provide services, collect or process data, or engage in similar activities through the use of information systems. The key responsibilities among these are as follows:

- To promptly and primarily provide the Presidency with any data, information, documents, hardware, software, and any other contributions requested within the scope of the Presidency's duties and activities.
- To report to the Presidency any cyber incidents identified within the scope of their services, as well as vulnerabilities—referring to weaknesses and security gaps in cyber assets that may be exploited by any cyber threat.
- To procure cybersecurity products, systems, and services to be used in critical infrastructures from cybersecurity experts, manufacturers, or companies authorized and certified by the Presidency.
- To obtain the approval of the Presidency, in accordance with the applicable regulations, prior to commencing operations by cybersecurity companies that are subject to certification, authorization, and accreditation.
- To implement the matters set forth in the policies, strategies, and action plans developed by the Presidency, as well as other regulatory instruments published to enhance cyber maturity, and to take the necessary measures accordingly.

3. Audit

The Law also authorizes the Presidency, as well as independent auditors and independent audit firms authorized and certified by the Presidency, to audit the activities and operations of institutions, organizations, and other relevant natural and legal persons within the scope of the Law in relation to its provisions.

4. Cybersecurity Council

The Law also establishes the Cybersecurity Council ("Council"). Chaired by the President of the Republic, the Council may invite individuals outside its members to attend meetings, depending on the nature of the agenda, in order to gather information and opinions.

The duties of the Council are as follows:

- To make decisions regarding policies and other regulatory instruments related to cybersecurity.

- To make decisions regarding the nationwide implementation of the technology roadmap.
- To identify priority areas to be supported through incentives in the field of cybersecurity.
- To identify critical infrastructure sectors.
- To make decisions regarding disputes that may arise between the Presidency and public institutions.

5. Sanctions

In order to enhance the effectiveness and ensure the deterrent effect of the Law, detailed provisions have been established regarding criminal sanctions and judicial fines for those who violate the obligations set forth under the Law.

- Except for public institutions and organizations, those who fail to provide the information, documents, software, data, or hardware requested by the authorities and audit officers authorized under the Law, or who obstruct the acquisition of such materials, shall be punished with imprisonment from one to three years and a judicial fine ranging from five hundred to one thousand five hundred days.
- Those who operate without obtaining the necessary approvals, authorizations, or permits required under the Law shall be punished with imprisonment from two to four years and a judicial fine ranging from one thousand to two thousand days
- Those who fail to fulfill their confidentiality obligations shall be sentenced to imprisonment from four to eight years.
- Those who, due to data leaks in cyberspace, make accessible, share, or offer for sale—whether for free or for a fee—personal data or institutional data falling under critical public services that had previously been exposed, without the consent of the individuals or institutions concerned, shall be sentenced to imprisonment from three to five years.
- Those who, despite knowing that no data breach has occurred in cyberspace, create or disseminate false content claiming a cybersecurity-related data breach with the intent to incite public concern, fear, or panic, or to target institutions or individuals, shall be sentenced to imprisonment from two to five years.
- Those who carry out cyberattacks targeting the elements that constitute the national cyber power of the Republic of Türkiye, or who store any data obtained as a result of such attacks in cyberspace, shall be sentenced to imprisonment from eight to twelve years, unless the act constitutes another offense requiring a more severe penalty. Those who disseminate, transfer, or offer for sale in cyberspace any data obtained as a result of such attacks shall be sentenced to imprisonment from ten to fifteen years.
- Those who abuse their duties and powers arising from the Law, or who, by acting contrary to the requirements of their duties in the context of protecting critical infrastructures against cyberattacks, cause a data breach to occur, shall be sentenced to imprisonment from one to three years.

- Those who provide services, collect, or process data through information systems and fail to fulfill their obligation to report security vulnerabilities and cyber incidents to the Presidency, or who fail to procure cybersecurity products, systems, and services to be used in public institutions and critical infrastructures from authorized or certified cybersecurity experts and companies, shall be subject to an administrative fine ranging from one million to ten million Turkish lira.

- Failure to seek the opinion or approval of the Presidency in the sale of cybersecurity products or services abroad, or in the merger, transfer, or sale of a company producing any product or service related to cybersecurity, as well as failure to respond to the Presidency's requests for information, shall be subject to an administrative fine ranging from ten million to one hundred million Turkish lira.

- Those who fail to fulfill their obligation to cooperate with auditors shall be subject to an administrative fine ranging from one hundred thousand to one million Turkish lira. In cases where such obligations are not fulfilled by commercial companies, an administrative fine of no less than one hundred thousand Turkish lira and up to 5% of the gross sales revenue stated in their independently audited annual financial statements shall be imposed.

6. Cybersecurity Products and Companies

The Law stipulates that the export of cybersecurity products, systems, software, hardware, and services shall be carried out in accordance with the procedures and principles to be determined by the Presidency. In addition, changes in the shareholding structure of cybersecurity companies are also subject to the approval of the Presidency.

C. Conclusion

The Law establishes a general framework aimed at strengthening national cybersecurity and lays the foundation for regulations that concern both the public and private sectors. Natural and legal persons falling within the scope of the Law will be required to carry out compliance efforts, particularly by closely following the secondary legislation to be introduced within the coming year.

For more information and support, please feel free to contact us at info@lbpartners.com.

LBF Partners Law Firm