A First in Turkey: The Cybersecurity Law Published

Turkey is facing a groundbreaking development in the field of cyber security: The Cyber Security Law (**Law**) has been published.

Until now, we did not have a comprehensive framework legislation specifically regulating the field of cybersecurity, unlike “The Personal Data Protection Law” or “The Law on the Regulation of Electronic Commerce”. However, **this new Law, published today in the Official Gazette**, aims to fill a significant gap as an overarching regulation in cybersecurity.

This Law, which affects all individuals and entities providing services in the digital sphere, adds a new compliance item to many topics ranging from personal data to electronic commerce, consumer rights to competition: **cyber compliance.**

While the Law is based on fundamental concepts such as “institutionalization”, “continuity” and “sustainability”, it prioritizes **the principle of accountability.** Therefore, everyone subject to the Law must now be able to “prove” and “document” their compliance. This, in fact, requires an internal compliance study and its integration.

Cyberspace: How Broad Is the Scope?

The Law applies to all public institutions and organizations, professional chambers, and natural and legal persons operating in cyberspace. Cyberspace is defined as the "environment consisting of IT systems connected to the internet or electronic networks and the networks connecting these systems." **This definition makes it clear that everyone operating in the digital world will fall under the Law's scope.**

Highlights of the Law

The new regulation addresses critical topics relevant to everyone involved with technology, including:

- Provisions to protect organizations against cyberattacks,
- Establishment of **the Cybersecurity Board** and its duties and powers,
- Enhancing the cyber resilience and maturity levels of public institutions and critical infrastructure organizations,
- Centralized monitoring, detection, and mitigation of cybersecurity incidents,
- Implementation of auditing processes and deterrent sanctions,

- Regulation of standardization, certification, and authorization processes,
- Severe penalties for cybercrimes and incidents.

What will be the responsibilities of companies?

The main responsibilities and duties regarding cybersecurity of those who are covered by the Law and who provide services, collect, process data and carry out similar activities by using IT systems are as follows:

- Provide **all data, information, documents, hardware, software and other contributions requested** by the Presidency within the scope of its duties and activities **in a priority and timely manner.** This is quite critical because its violations may result in imprisonment and administrative fines.
- To take the measures stipulated by the legislation for the purposes of national security, public order or the proper execution of public service for cyber security, **to notify the Presidency without delay of any vulnerability or cyber incidents detected in the area where they provide services.**
- Procure cybersecurity products, systems, and services to be used in public institutions and organizations and critical infrastructures from cybersecurity experts, producers, and companies authorized and certified by the Presidency.
- To obtain the Presidency's approval within the framework of the existing regulations before starting operations by cybersecurity companies subject to certification, authorization and accreditation.

Cybersecurity Presidency and Its Role

The newly established **Cybersecurity Presidency** will take a proactive role against cyber threats. The Presidency will take crucial responsibilities such as increasing the resilience of critical infrastructure, detecting, preventing, and mitigating cyberattacks. Carrying out the certification, authorization, and accreditation processes for cybersecurity experts and companies will be one of the main duties of the Presidency. In addition, it will determine the criteria for software, hardware, products and services that will be used in the information systems of public institutions and organizations and critical infrastructures and that have an impact on cyber security, and the procedures and principles regarding the reports to the Presidency.

Sanctions and Penalties

- **Failure or obstructing to provide information and documents:** Those who fail to provide or obstruct the receipt of a requested information, document, software, data, and hardware by authorities other than public institutions: 1 to 3 years imprisonment and 500 to 1,500 days judicial fine.

- **Failure to comply with cyber security measures:** Those who do not take the measures required by the legislation or do not report cyber incidents: from ₺1 million to ₺10 million administrative fine.
- **Those who neglect to procure cyber security services from authorized experts in public institutions and critical infrastructures:** from ₺1 million to ₺10 million administrative fine.
- **Not being open to audit:** Those who do not provide the necessary infrastructure for auditing: from ₺100 thousand to ₺1 million administrative fines. Failure to comply with this obligation in commercial companies: An administrative fine equal to 5% of the company's gross sales revenue.
- **Unauthorized activity:** Those who carry out activities without obtaining the required approvals, authorizations, or permits: 2 to 4 years imprisonment and 1,000 to 2,000 days judicial fine.
- **Violating confidentiality obligations:** 4 to 8 years imprisonment.
- **Sharing personal or critical institutional data in cyberspace without authorization:** Those who share or resell data as a result of a data leak or without authorization: 3 to 5 years imprisonment.
- **Causing distress, fear and panic among the public even though there is no data leak:** Those who cause or untrue content regarding cybersecurity-related data leaks in order to create distress, fear and panic among the public or to target institutions or individuals, despite being aware that there is no data leak in cyberspace: 2 to 5 years imprisonment.
- **Cyber-attacks and misuse of acquired data:** In attacks targeting the country's cyber power 8 to 12 years imprisonment for anyone who commits a cyberattack; 10 to 15 years imprisonment for anyone who shares, disseminates or sells the data obtained.
- **Those who abuse their duties and powers arising from the law or causing data breach in critical infrastructure:** Those who abuse their duties and powers to cause data breach by acting against the requirements of the task: 1 to 3 years imprisonment.
- **Failure of cybersecurity service providers to meet their obligations:** from ₺10 million to ₺100 million administrative fine.

Compliance and Transition Timelines:

- The sale abroad of cybersecurity products, systems, software, hardware, and services will be conducted in line with the procedures and principles to be determined by the Presidency. In this context, the Presidential approval will be obtained for the sale of products subject to authorization abroad.

- Merger, division share transfer or sale transactions of cyber security companies will be notified to the Presidency. In this context, transactions that provide real or legal persons, individually or jointly, with direct or indirect control rights or decision-making authority over the company will be subject to the approval of the Presidency. This matter requires

special attention, as any actions taken without Presidential approval will be legally invalid.

- Although the law will enter into force on its date of publication, companies operating in the field of cyber security are obliged to complete their certification processes within one year from the entry into force of the relevant regulations.

- Secondary regulations are expected to be finalized within one year.

This “cyber compliance” area, which has entered our legislation for the first time, directly aligns with our expertise under the leadership of our esteemed Professor Bedii Kaya.

Rapid compliance with the regulations and initiating the process without delay is of critical importance.

Please feel free to reach out to Gökçe with any questions you may have.