January 2025

The Grand National Assembly of Türkiye published the Proposal of Cybersecurity Law ("Proposal")

The Grand National Assembly of Türkiye started the new year by introducing the Proposal of Cybersecurity Law ("**Proposal**"). This proposal aims to strengthen the country's cybersecurity framework by countering cyber threats, mitigating incident impacts, and protecting institutions, individuals, and organizations against cyberattacks. The Proposal also establishes the Cybersecurity Council ("**Council**") to set policies, regulations, strategies, identify critical infrastructure sectors, and determine exemptions. Pursuant to the Proposal, the members of the Board will be the President, the Vice President, and the ministers of Türkiye. The Cybersecurity Directorate ("**Directorate**") will operate under the guidance of the Council in its activities.

Our key takeaways from the Proposal are detailed below:

Purpose and Scope: The scope of the Proposal includes private persons/entities. Its purpose is to ensure the protection of public institutions, organizations, professional bodies having public institution status, real persons, legal entities, and unincorporated organizations from cyberattacks, strengthen Türkiye's cybersecurity, and regulate principles regarding the establishment of the Council.

Definitions: The Proposal aims to introduce new definitions such as cybersecurity, cyberattack, and cyberspace. In line with the Information and Communication Security Guidance the Proposal defines critical infrastructures as "*Infrastructure that hosts information systems where the confidentiality, integrity, or availability of information/data is compromised, potentially leading to loss of life, large-scale economic damage, security vulnerabilities, or disruption of public order*".

Principles: The Proposal stipulates that priority will be given to domestic and national products in ensuring cybersecurity, the protection of critical infrastructure and information systems is a fundamental objective, and private persons/entities are also responsible for taking the necessary measures.

Establishing Cybersecurity Council: The Proposal aims to establish the Council and to determine the duties of it mainly (i) identifying critical infrastructure zones, and (ii) making decisions on policies, strategies, action plans, and other regulatory processes related to cybersecurity, and determining which institutions and organizations may be exempt from these decisions, either in whole or in part.

Duties and Powers of Cybersecurity Directorate: The Proposal aims to regulate the duties and powers of the Directorate. Please find the highlighted provisions in the table below:

Duties of Directorate (Article 5)	Powers of the Directorate (Article 6)
Identify owners and locations of critical infrastructures.	Request information and access archives, electronic data centers, and communication infrastructures.
Maintain inventories of public institutions, organizations, and critical infrastructures regarding their assets, conduct risk analyses, and ensure security measures are implemented based on criticality of the assets owned by them.	Classify the actors and, when necessary, establish provisions that apply only to certain parts of their activities.
Establish Cyber Incident Response teams.	Authorize and revoke the authorization of independent cybersecurity audit firms.
Regulate cybersecurity procedures and principles.	Set minimum security standards for cybersecurity products, manage certification processes, and ensure compliance with standards.
Develop and review cybersecurity standards.	
Test and certify cybersecurity-related software, hardware, systems, and services; manage certification, authorization, and documentation processes for experts and companies.	
Conduct cybersecurity audits and impose sanctions.	

Audit Power: The Proposal grants the Directorate significant audit powers specifically including:

- **Search and Seizures:** The Directorate can search residences, workplaces, and non-public closed areas with a judge's order or, in urgent cases, with a written order from the president of the Directorate. Non-judicial orders must be submitted to the judge within 24 hours and must be approved within 48 hours. Otherwise, the materials collected shall be destroyed, and the seizure shall be lifted.
- **Inspection Authority:** The Directorate can perform or commission on-site inspections of the activities and transactions of institutions, organizations, and individuals.
- **Audit Scope:** Auditors can examine electronic data, documents, systems, devices, and software, take copies or samples, request explanations, and inspect facilities. Entities under audit ensure that all relevant systems and infrastructure are available and functional for inspection within specified timeframes.

Prohibitions: Any information, documents, or similar data obtained regarding the practice conducted by the Directorate, will not be published, or disclosed, unless authorized by the Directorate.

Cybersecurity Products and Companies: The sale of cybersecurity products and services developed with public funding to foreign countries requires the approval of the Directorate. This approval is also needed for company mergers, divisions, share transfers, or sales involving these products. The Directorate sets the procedures for these approvals and can request information from public institutions about the products and companies involved. The Directorate will issue a regulation to regulate this process.

Administrative Fines and Penal Provisions: The Proposal introduces new administrative fines and penal provisions to those who fail to provide the requested, please find the highlighted provisions:

- **Failure to Provide Information:** Imprisonment of 1 - 3 years and judicial fines of 500 - 1500 days for failing or obstructing to provide requested information, data, or documents.
- **Unauthorized Operations**: Imprisonment of 2 - 4 years and judicial fines of 1000 - 2000 days for operating without required approvals or permits.
- **False Data Breach Claims**: Imprisonment of 2 – 5 years for creating false perceptions regarding cyber breaches.
- **Inadequate Cybersecurity Measures:** Fines range from TL 1,000,000 to TL 10,000,000 for (i) failing to take prescribed measures, and report vulnerabilities, and (ii) procure certified cybersecurity products, and fines range from TL 10,000,000 to TL 100,000,000 for non-compliance with notification requirements are foreseen in the Proposal.

Application of the Administrative Fines: Before imposing administrative fines, the concerned party will be asked for a defense. If the defense is not provided within 30 days of notification, the right to defense will be deemed waived.

Delegating Powers: The Information Technologies and Communication Authority, delegates its power regarding cybersecurity matters to the Directorate.

Compliance Provisions: Companies, federations, associations, and foundations that are in the scope of the Proposal will be required to comply with the Proposal within one year after the Proposal's effective date. Otherwise, their activities will be ceased.

Conclusion

If the Proposal is enacted, it will constitute Turkey's first holistic cybersecurity legislation. Entities falling within the scope of the Proposal, as defined by its provisions, may be subject to audits, administrative fines, and imprisonment.

You may access the Proposal in Turkish language through the following link: **The Proposal of Cybersecurity Law**

Key Contacts

Kağan Dora
Partner, Head of Intellectual Property, Data and Technology
D: +90 212 329 30 35
E: kdora@baseak.com

Safa Cenanoğlu
Counsel
D: +90 212 708 93 97
E: scenanoglu@baseak.com

Anıl Mert İçintek
Associate
D: +90 212 708 94 23
E: aicintek@baseak.com