Balcıoğlu Selçuk
Eymirlioğlu Ardıyok Keki

Client Alert

Türkiye's New Cybersecurity Law: Key Changes and Implications for Businesses

March 2025

New Cybersecurity Law

The Cybersecurity Law, initially introduced as a draft earlier this year, has been fast-tracked and passed by the Turkish Parliament. It is expected to enter into force shortly after its publication in the Official Gazette, which is anticipated in the coming days. While awaiting the announcement, it introduces changes that IT companies - especially cybersecurity firms - cannot afford to overlook, such as new compliance and licensing requirements.

We are ready to guide you through this new era of cybersecurity legislation in Türkiye.

➢ Key Aspects

1. **Wide scope and regulatory powers**: The Cybersecurity Law introduces a comprehensive framework to strengthen Türkiye's cybersecurity infrastructure, empowering the Turkish Cybersecurity Directorate ("CSD") as the primary regulatory authority. The CSD now has regulatory oversight over all entities whether they are in the public or private sectors, that exist, operate, or provide services in cyberspace, including individuals. The law places special emphasis and imposes obligations on entities providing cybersecurity services in Türkiye. The CSD has also been empowered to determine procedures and principles, as well as to introduce prior licensing requirements for the export of cybersecurity products, systems, software, hardware and services, and to establish cybersecurity incident response teams or require subject entities to do so.

2. **Focus groups**: While the law applies to all entities operating in cyberspace, certain groups require special attention:

    a. Critical infrastructure: Businesses operating in sectors designated as critical infrastructure by the CSD will face stricter oversight and higher compliance standards. These include maintaining an asset inventory, conducting risk analyses, and implementing specific security measures based on the criticality level of their assets, as determined by the CSD and to retain and procure cybersecurity products, systems and services from only authorised and certified cybersecurity experts and firms.

    b. Cybersecurity Firms: Companies providing cybersecurity products and services will be required to undergo approval, licensing, and certification processes established by the CSD, including but not limited to the following:

i. The export of cybersecurity products, systems, software, hardware or services will be subject to a prior license,

ii. Mergers, spin-offs, sales or changes of control of cybersecurity firms.

iii. A license to operate in the cybersecurity field.

c. Overall IT companies: The duties and responsibilities of entities covered by the new law that provide services, collect data, process data and carry out similar activities using information systems, regarding cybersecurity include but are not limited to:

i. Providing data, information, documents, software, hardware, and support to the CSD for the fulfilment of its duties and complying with requests of the CSD during audits and investigations.

ii. Complying with the measures, policies and action plans to be implemented by the CSD and promptly informing the CSD of exposures and cyber incidents they notice in their service areas.

3. **Heavy fines and sanctions**: Non-compliance with applicable regulations may result in the following penalties, depending on the severity of the violation:

a. An administrative fine of up to 5% of gross sales revenue for failing to keep relevant assets and systems accessible for inspection conducted within the scope of the law.

b. Administrative fines of up to TRY 100 million—approximately EUR 2,516,438—for exporting the cybersecurity items mentioned above without a license.

c. Imprisonment and judicial fines for failing to comply with requests for information from the regulatory institution, obstructing access to such data/information, or

d. Restriction of the scope of activity of cybersecurity companies that fail to comply with the certification, authorization or documentation procedures imposed by the CSD within one year of the announcement of such obligations, or even deregistration from the commercial register and liquidation.

➢ **Timeline**

The details of the legislation and any vague points are expected to be clarified through additional regulations and guidelines to be issued by the CSD within the next year following the announcement of the law in the Official Gazette.

In light of these changes, proactive preparation is essential to ensure compliance, maintain a competitive edge, and stay ahead of the curve in the IT and cybersecurity sectors.

Contacts

For more information, to stay informed of further developments and for tailored consultation please feel free to contact us:

Kağan Dora

Partner
Head of Privacy and Cybersecurity

D: +90 212 329 30 35
E: kdora@baseak.com

Safa Cenanoğlu

Counsel

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

Balcıoğlu Selçuk Eymirlioğlu Ardıyok Keki Attorney Partnership
Büyükdere Caddesi Bahar Sokak No.13
River Plaza Kat 11, 34394 Levent, Istanbul Türkiye

P +90 212 329 30 00

www.baseak.com