KOLCUOĞLU
DEMİRKAN
KOÇAKLI

CLIENT ALERT

Public Statement from the Cybersecurity Council Regarding Critical Infrastructure Sectors

MAY 2026

JURISDICTION
Türkiye

PRACTICE AREA
Personal Data
Privacy

At the Cybersecurity Council meeting held on 5 May 2026, current risks to Türkiye's cybersecurity, future threat trends, and the key elements of the national cybersecurity approach were comprehensively addressed.

The meeting emphasized that cybersecurity is an integral part of national security, and identified the protection of critical infrastructure, the security of digital systems, data sovereignty, and capacity building in domestic and national technologies as priority areas.

As part of the Council meeting, decisions were made to strengthen inter-agency coordination and increase domestic, sustainable capacity in critical areas, and the following sectors were designated as "Critical Infrastructure Sectors":

- Digital Infrastructure
- Digital Services
- Electronic Communications
- Energy
- Finance
- Food and Agriculture
- Manufacturing Industry
- Public Services
- Media and Crisis Communication
- Postal and Courier Services
- Healthcare
- Defense Industry
- Water Management
- Transportation
- Space

These decisions by the Cybersecurity Council require data controllers operating in critical sectors to review and strengthen their information security and data protection measures. In this context, it is of the utmost importance that all data controllers — particularly institutions and organizations operating in critical infrastructure sectors — address their obligations under Cyber Security Law No. 7545 through a comprehensive approach and prioritize compliance with regulations, as well as administrative, technical, and organizational awareness initiatives.

Please contact us if you need further information on this matter.