

Turkish Data Protection Law (KVKK) — Law No. 6698

Cybersecurity and data protection requirements in EMEA and Turkey define obligations for organizations to secure data and protect privacy.



What it is

EMEA Turkey — Regional Cybersecurity and Data Protection Requirements is a regulatory framework that establishes legal obligations for organizations to protect personal data, ensure cybersecurity, and maintain compliance with national laws in Turkey. The framework helps organizations safeguard sensitive information, manage cyber risks, and adhere to privacy requirements.

Issued and enforced primarily by Turkish government authorities, including the Personal Data Protection Authority (KVKK) and the Information and Communication Technologies Authority (ICTA), these requirements apply to both local and international organizations processing personal data or delivering digital services in Turkey. Covered areas include data protection and privacy governance, minimum cybersecurity controls, risk management procedures, breach notification, and retention policies, and align with broader European regulatory expectations.

At a glance

PUBLISHER	TYPE	VERSION
Unknown	Regulation	For "EMEA Turkey — Regional Cybersecurity and Data Protection Requirements," the relevant regulatory instruments include: Cybersecurity Law No. 7545 (enacted 19 March 2025) — this is a specific law, but the title does not inherently include a version or revision identifier; typically for laws, the version is the year of enactment. Personal Data Protection Law No. 6698 (KVKK), enacted 2016, with major amendments effective June 2024. Based on the rules: - The Cybersecurity Law should be represented by its enactment year: **2025**. - The Personal Data Protection Law corresponds to **2016** (with notable 2024 amendments, but those are not framed as a version per se). However, since the Reg Title suggests "Regional Cybersecurity and Data Protection Requirements" (plural), and likely refers to both domains, but the Title itself does not specify which law or regulation, the

How SmartSuite supports KVKK (Law No. 6698)

Data Processing Inventory and Records Maintain records of processing activities, purposes, data categories, and consent requirements.	Privacy Governance and Policy Management Centralize policies, procedures, and approvals aligned to Turkish data protection laws.	Data Subject Rights Workflows Manage access, correction, deletion, and objection requests with full audit trails.
Risk Assessments and Compliance Reviews Track privacy risks and conduct assessments aligned to KVKK obligations.	Breach Management and Notification Workflows Track incidents and manage notification obligations to authorities and affected individuals.	Privacy Posture and Regulatory Readiness Reporting Provide dashboards showing privacy posture, control coverage, and regulatory readiness.

Common framework mappings

CIS Controls v8.1

COBIT 2019

GDPR

ISO 27001:2022

ISO 27002:2022

ISO 27701

NIST CSF 2.0

NIST 800-53 Rev.5

PCI DSS 4.0.1

SOC 2

Official resources

European Union General Data Protection Regulation (GDPR) Provides comprehensive data protection regulations applicable in Switzerland due to EEA relevance. gdpd-info.eu	Turkey Personal Data Protection Law (KVKK) Provides legal framework for data protection in Turkey similar to GDPR. kvkk.gov.tr
European Cybersecurity Act Outlines measures for improving cybersecurity across the EU. eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32019R0881	NIS Directive Provides guidelines for security of network and information systems across the EU. eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016L1148

Frequently asked questions

- What are the EMEA Turkey Regional Cybersecurity and Data Protection Requirements used for?**

These requirements provide a legal and regulatory framework for protecting personal data and securing information systems within Turkey. They are designed to align organizations with national laws, such as the Turkish Personal Data Protection Law (KVKK), and sectoral regulations addressing data confidentiality, integrity, and availability. Organizations use these requirements to mitigate cybersecurity risks and ensure lawful data processing.
- Are the EMEA Turkey Cybersecurity and Data Protection Requirements mandatory?**

Yes, these requirements are mandatory for most organizations operating in Turkey that process personal data or provide information society services. Compliance is enforced by the Turkish Personal Data Protection Authority (KVKK Board) and sector-specific regulators, with significant penalties for violations.
- What is the scope of applicability for the Turkey Regional Cybersecurity and Data Protection Requirements?**

The scope generally covers all entities—both public and private—that process personal data of Turkish citizens or residents, as well as organizations offering critical infrastructure or digital services within Turkey. Applicability extends to data controllers and processors, regardless of their physical location, if they process data relating to individuals in Turkey.

What key concepts or artifacts are required by the Turkey regional requirements?

Key concepts include explicit consent, data minimization, data subject rights, and breach notification. Required artifacts include data processing inventories, privacy policies, consent forms, and records of risk assessments. Technical and organizational security controls must be documented and regularly reviewed.

How do organizations implement the EMEA Turkey cybersecurity and data protection requirements?

Implementation typically involves conducting data mapping, assessing data processing activities, applying technical and organizational controls, and ensuring staff training. Organizations should establish documented policies and procedures, manage third-party risks, and maintain processes for responding to data subject requests and breaches.

How do the Turkey requirements relate to frameworks like GDPR?

The Turkish requirements are closely modeled on the EU General Data Protection Regulation (GDPR) but contain local adaptations specific to Turkish law and regulations. While there is significant overlap in principles and protections, organizations must meet local nuances, such as registration requirements with the KVKK, or differences in breach reporting timelines.

What are the ongoing compliance requirements for Turkey's cybersecurity and data protection regulations?

Ongoing requirements include regular review and updates of security controls, periodic risk assessments, timely breach reporting, continuous staff awareness training, and demonstration of accountability. Organizations must also respond promptly to data subject rights requests and maintain up-to-date compliance documentation.

How would SmartSuite support EMEA Turkey — Regional Cybersecurity and Data Protection Requirements?

SmartSuite can streamline compliance management by providing tools for risk identification and tracking, maintaining centralized control libraries, and organizing evidence for audits. It helps automate processes such as policy reviews, consent tracking, incident management, and compliance reporting, ensuring organizations remain audit-ready and able to demonstrate adherence to Turkey's regulatory requirements.

License included / downloadable: Yes Turkey's Personal Data Protection Law (KVKK) and national cybersecurity regulations are published by the Turkish Grand National Assembly and the Personal Data Protection Authority and are publicly available. License included with platform

Full framework page and mappings: smartsuite.com/frameworks/emea-turkey-regional-cybersecurity-and-data-protection-requirements-kvkk-law-no-6698