SmartSuite

Framework / Cybersecurity / Other

China Cybersecurity Law (CSL) – 2016

China's Cybersecurity Law sets network operator duties, special rules for critical information infrastructure and, since January 1, 2026, higher fines.



What it is

The Cybersecurity Law of the People's Republic of China (CSL) is China's framework statute for network security. It applies to building, operating, maintaining and using networks in mainland China and to cybersecurity supervision there (Article 2), and it sets duties for network operators, special duties for operators of critical information infrastructure (CII), and rules for network products and personal information. The National People's Congress Standing Committee adopted it on November 7, 2016, it took effect on June 1, 2017, and an amendment adopted on October 28, 2025 took effect on January 1, 2026.

The Standing Committee of the National People's Congress enacts the law. Article 8 makes the national cybersecurity and informatization department, the Cyberspace Administration of China, responsible for overall coordination and supervision, while telecommunications authorities, public security organs and other bodies supervise within their own remits.

At a glance

PUBLISHER National People's Congress (NPC)	TYPE Framework	VERSION Cybersecurity Law of the People's Republic of China (2016), as amended October 28, 2025
EFFECTIVE June 1, 2017 (amendment effective January 1, 2026)	DOMAIN Cybersecurity	FAMILY Other
REGION China	ADOPTION MODEL Regulatory Compliance	IMPLEMENTATION COMPLEXITY High

Source: npc.gov.cn/englishnpc/c23934/202112/t20211209_385109.html

Why it matters

- **Duties for every network operator** Article 21 requires a responsible cybersecurity person, technical defenses, monitoring and logs kept for at least six months, data classification, backups and encryption under the multi-level protection system.
- **Real-name and product duties** Article 24 requires real identity information for network access, domain registration, phone access and messaging or publishing services, and Article 22 sets duties for network products and services.
- **Special regime for CII** Operators of critical information infrastructure carry added duties for a security management body, background checks, training, disaster recovery, drills, security review of purchases and data localization (Articles 34 to 38 of the 2017 text).
- **Personal information rules** Articles 40 to 45 of the 2017 text require lawful, proper and necessary collection, consent, security, breach notification and the right to correction or deletion.

Updated Oct 15, 2026 · © 2026 SmartSuite Inc. All rights reserved.

How SmartSuite supports CSL

System Inventory and Protection Level

Record each network and system with its multi-level protection level, responsible person and owner (Article 21).

Logs, Backups and Encryption Controls

Track log retention of at least six months, data classification, backup and encryption controls as linked controls with evidence.

Real-Name and Product Obligations

Hold the real identity verification process and the compliance status of network products and critical equipment (Articles 22 to 24).

CII Duties and Annual Assessment

For designated CII systems, schedule the annual assessment, drills, background checks and security reviews of purchases (Articles 34 to 38).

Incident Response and Reporting

Maintain emergency response plans and log incidents with the reports made to competent departments (Article 25).

Cross-Border Transfer Register

Record data stored in China and each outbound transfer with its security assessment status (Article 37).

Common framework mappings

APEC PF | CIS Controls v8.1 | GDPR | ISO 27001:2022 | ISO 27701 | MLPS 2.0 | NIST CSF 2.0 | PIPL

Official resources

China Cybersecurity Law (CSL) Official Text

Defines the legal requirements for cybersecurity and data protection in China.

npc.gov.cn/englishnpc/c23934/202112/t20211209_385109.html

Frequently asked questions

Who must comply with China's Cybersecurity Law?

Network operators, meaning network owners, managers and network service providers, that build, operate, maintain or use networks within mainland China (Articles 2 and 76). Operators of critical information infrastructure carry additional duties.

What changed in the 2025 amendment?

The NPC Standing Committee adopted the amendment on October 28, 2025, effective January 1, 2026. It raises penalties, including the ceiling for CII operators from RMB 1 million to RMB 10 million, adds a provision on artificial intelligence, aligns personal information liability with the Civil Code and the Personal Information Protection Law, and renumbers the articles.

Does the CSL require all data to be stored in China?

No. Article 37 requires operators of critical information infrastructure to store personal information and important data collected in mainland China domestically. Transfers abroad that are necessary for business need a security assessment under the authorities' measures.

What is the multi-level protection system?

It is the framework in Article 21 under which network operators adopt internal security rules, name a responsible person, use technical defenses, keep network logs for at least six months, and apply data classification, backups and encryption proportionate to the protection level of the system.

What is critical information infrastructure under the CSL?

Infrastructure in key sectors such as communications, energy, transport, water, finance, public services and e-government whose failure or data leakage could seriously endanger national security, livelihoods or the public interest. The State Council sets the specific scope (Article 31).

Updated Oct 15, 2026 · © 2026 SmartSuite Inc. All rights reserved.

License included / downloadable: Yes The Cybersecurity Law is published by the National People's Congress and is included with the platform for reference.

Full framework page and mappings: smartsuite.com/frameworks/china-cybersecurity-law-csl-2016

Updated Oct 15, 2026 · © 2026 SmartSuite Inc. All rights reserved.