SmartSuite

Framework / Data Governance / Global Privacy Regulations

Data Security Law of the People’s Republic of China (DSL) — 2021

China's Data Security Law requires classification and grading of data, stricter control of important and core data, incident reporting and approval of outbound transfers.



What it is

The Data Security Law of the People's Republic of China (DSL) is China's statute for data security. It requires organizations that handle data in mainland China to classify data by importance, run full-process data security management, treat "important data" and "core national data" more strictly, and control outbound transfers and foreign government requests. The National People's Congress Standing Committee adopted it on June 10, 2021 and it took effect on September 1, 2021 (Article 55).

The law applies to data handling within mainland China and, for overseas handling that harms China's national security, public interest or the lawful rights of citizens and organizations, to liability under the law (Article 2). Sector regulators supervise their own fields, public security and state security organs act within their remits, and the national cyberspace and informatization department coordinates network data security (Article 6).

At a glance

PUBLISHER National People's Congress (NPC)	TYPE Framework	VERSION Data Security Law of the People's Republic of China (2021); implementing Decree No. 790 effective January 1, 2025
EFFECTIVE September 1, 2021	DOMAIN Data Governance	FAMILY Global Privacy Regulations
REGION China	ADOPTION MODEL Regulatory Compliance	IMPLEMENTATION COMPLEXITY High

Source: npc.gov.cn/englishnpc/c23934/202112/t20211209_385108.html

Why it matters

- **Tiered protection by importance** Data is categorized and graded, with regions and departments publishing catalogs of important data and applying stricter management to core national data (Article 21).
- **Named accountability** Handlers of important data designate a data security lead and a management body (Article 27).
- **Incident duties** Handlers monitor risks, fix flaws immediately and, after an incident, act, notify users and report to regulators (Article 29).
- **Periodic risk reports** Important data handlers carry out periodic risk assessments and submit reports on data types and volumes, handling activities, risks and countermeasures (Article 30).

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

How SmartSuite supports China DSL

Data Classification and Grading Catalog

Record each data set with its category, grade and whether it falls in a regulator's important data catalog (Article 21).

Data Security Management System

Keep the policies, training records and technical controls of the full-process system, with the designated data security lead and body (Article 27).

Risk Monitoring and Incident Reporting

Log vulnerabilities, incidents, user notices and reports to authorities with dates and owners (Article 29).

Periodic Risk Assessment Reports

Schedule the periodic assessment of important data and keep the report to the competent authority and its supporting evidence (Article 30).

Outbound Transfer and Foreign Request Register

Record each outbound transfer with its approval or assessment status and any foreign data request with its handling decision (Articles 31 and 36).

Data Security Readiness Reporting

Show classification coverage, open risks and assessment status for leadership and counsel on a dashboard.

Common framework mappings

PIPL | COBIT 2019 | GDPR | ISO 27001:2022 | ISO 27701 | NIST Privacy Framework v1.0 | NIST 800-53 Rev.5 | SOC 2

Official resources

China Data Security Law (DSL) Official Text

Provides the full text of the China Data Security Law as enacted by the Standing Committee.

npc.gov.cn/englishnpc/c23934/202112/t20211209_385108.html

Frequently asked questions

What is the China Data Security Law?

It is China's statute for data security, effective September 1, 2021. It requires organizations that handle data in mainland China to classify and grade data, protect important data and core national data more strictly, report incidents and control outbound transfers.

What is important data and core national data?

Article 21 sets categorized and graded protection by the importance of the data and the harm from tampering, destruction, leakage or illegal use. Regions and departments publish catalogs of important data. Data tied to national security, economic lifelines, key livelihoods and major public interests is core national data and is managed more strictly.

What must handlers of important data do?

They designate a data security lead and a management body (Article 27) and carry out periodic risk assessments, sending reports on data types and volume, handling activities, risks and countermeasures to the competent authority (Article 30).

Can a company in China hand data to a foreign court or regulator?

Not without approval. Article 36 says organizations and individuals in mainland China may not provide data stored in mainland China to foreign judicial or law enforcement bodies without approval from the competent Chinese authority.

What are the penalties under the DSL?

Failing the duties in Articles 27, 29 or 30 draws fines of RMB 50,000 to 500,000, or RMB 500,000 to 2 million in serious cases. Unlawful outbound transfers of important data can draw RMB 100,000 to 1 million, or RMB 1 to 10 million in serious cases (Articles 45 and 46).

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

License included / downloadable: Yes The Data Security 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-data-security-law-dsl

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