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 organizations to protect important data, manage security risks, and regulate cross-border data transfers.

What it is

China Data Security Law (DSL) is a national regulation that establishes requirements for data security management, cybersecurity risk mitigation, and data protection within China. Its primary goal is to safeguard important data, protect personal information, and ensure the lawful, orderly use and cross-border transfer of data by organizations operating in or interacting with China.

The DSL was enacted by the Standing Committee of the National People's Congress of the People's Republic of China and applies to both domestic entities and foreign organizations handling data related to China. The law sets out obligations related to data classification, risk assessment, data localization, and incident response, focusing on sensitive and critical data relevant to national security, economic stability, and individual privacy.

At a glance

PUBLISHER National People's Congress (NPC)	TYPE Framework	VERSION Data Security Law of the People’s Republic of China
EFFECTIVE September 1, 2021	DOMAIN Data Governance	FAMILY Global Privacy Regulations
REGION China	ADOPTION MODEL Regulatory Compliance	IMPLEMENTATION COMPLEXITY High

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

Why it matters

- **Strengthen data protection practices** Enhance processes for classifying, handling, and securing sensitive or important data to reduce unauthorized access and data misuse risks.
- **Improve regulatory alignment** Ensure business operations comply with China's evolving data security and privacy requirements, reducing the likelihood of regulatory violations and penalties.
- **Enhance risk management capabilities** Support systematic risk assessments and robust internal controls to proactively identify, mitigate, and monitor data security threats.
- **Support responsible cross-border data transfers** Enable accountable and lawful management of data transfers between China and other countries, ensuring business continuity and compliance.

Updated Sep 26, 2026 · © 2026 SmartSuite Inc. All rights reserved.

How SmartSuite supports China DSL

Data Classification and Governance Framework

Structure data categories, sensitivity levels, and governance requirements aligned to DSL.

Data Lifecycle and Handling Controls

Track data collection, processing, storage, transfer, and disposal practices.

Data Risk Evaluation and Protection Controls

Manage data risk evaluations and implement controls to protect important data assets.

Cross-Border Data Transfer Management

Track approvals, assessments, and safeguards for transferring data outside China.

Data Security Incident and Authority Notification

Monitor data security incidents and manage notification obligations to authorities.

DSL Data Risk and Compliance Readiness Reporting

Provide dashboards showing data risk posture, control coverage, and DSL compliance readiness.

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 (DSL) used for?

The China Data Security Law (DSL) establishes a regulatory framework for the protection, management, and lawful use of data within China. It is designed to safeguard personal information, protect critical and important data, and ensure that organizations manage data in a way that supports national security, economic stability, and individual privacy.

Is compliance with the China Data Security Law (DSL) mandatory?

Yes, compliance with the DSL is mandatory for both domestic and foreign entities that process, store, or transfer data related to China. Non-compliance can result in regulatory penalties, restrictions on business operations, and reputational risk.

Who does the China Data Security Law (DSL) apply to?

The DSL applies to organizations operating within China as well as foreign organizations that handle or process data originating from China. This includes businesses, government agencies, and any entity involved in collecting, storing, or transferring important or personal data related to Chinese citizens or organizations.

What key concepts and artifacts are required for DSL compliance?

Key concepts under the DSL include data classification (distinguishing important, critical, and personal data), mandatory risk assessments, incident response plans, data localization requirements, and records of cross-border data transfers. Artifacts include classification inventories, risk assessment reports, incident logs, and compliance documentation.

How does implementation of the China Data Security Law (DSL) work in practice?

Implementing DSL involves inventorying all data, classifying it according to sensitivity, establishing technical and organizational safeguards, and conducting regular risk assessments and impact analyses. Organizations must document controls, monitor for compliance, respond to incidents, and address regulatory obligations.

© 2026 SmartSuite Inc. All rights reserved.

How does the China Data Security Law (DSL) relate to other data protection frameworks?

The DSL is often implemented alongside other data protection and cybersecurity frameworks such as the Cybersecurity Law of China and global privacy laws like the GDPR. Organizations commonly integrate DSL requirements into broader information security management systems to ensure consistent data governance and regulatory alignment.

What are the ongoing compliance requirements for the DSL?

Ongoing compliance requires organizations to continually monitor data handling activities, update data inventories, conduct periodic risk assessments, maintain incident response capabilities, and submit compliance reports as required by regulators. Regular reviews and updates to policies and controls are essential to remain compliant.

How would SmartSuite support China Data Security Law (DSL)?

SmartSuite supports DSL compliance by providing centralized risk tracking, mapping controls to regulatory clauses, and maintaining comprehensive evidence collections. It enables organizations to manage audit readiness, workflow remediation actions, and automate compliance reporting. Dashboards and linked risk registers facilitate ongoing monitoring and streamlined oversight to demonstrate compliance with the DSL.

License included / downloadable: Yes The Data Security Law of the People's Republic of China is publicly available through official Chinese government publications.

Full framework page and mappings: smartsuite.com/frameworks/china-data-security-law-dsl

Updated Sep 26, 2026 · © 2026 SmartSuite Inc. All rights reserved.