China Issues Data Security Law

Article By
Hunton Andrews Kurth’s Privacy and Cybersecurity
Hunton Andrews Kurth
Privacy and Information Security Law Blog-Hunton Andrews Kurth

Related Practices & Jurisdictions

- Administrative & Regulatory
- Communications, Media & Internet
- Consumer Protection
- Corporate & Business Organizations
- Global
- China

Wednesday, June 16, 2021

After two rounds of public comments, the Data Security Law of the People’s Republic of China (the “DSL”) was formally issued on June 10, 2021, and will become effective on September 1, 2021.

Compared to previous drafts of the law, the final version of the DSL differs with respect to:

- establishing a work coordination mechanism and clarifying the duties of each governmental authority;
- establishing an administration system for state core data;
- encouraging data development and use to make public service more intelligent and requiring consideration of the needs of the elderly and people with disabilities when providing intelligent public services;
- protecting the security of government data; and
- increasing the punishment dynamics for violations of the law.

Jurisdiction

The DSL not only governs data activities conducted in China, but also regulates data activities conducted by organizations and individuals outside of China that harm China’s national security or public interest, or the legal interests of citizens and organizations in China.

Applicable Scope

The DSL will apply to data recorded in electronic and other forms.

Data Security Policies

The DSL is the fundamental law for data security, and it designs a series of policies – including those regarding data categorization and classification, data risk controls, contingency responses for data security, data security reviews, export controls and anti-discrimination – to ensure data development and use, as well as industry development. The specific rules for implementing these policies are expected in the future, and may include supporting laws, regulations and guidelines.

In accordance with Article 21 of the DSL, a data protection policy based on the hierarchical classification and categorization of data and an “important data catalogue” (expected to be defined in future implementing rules) must be established at the national level. Each region and department must stipulate its own relevant and detailed industrial and sectoral catalogue of important data. In addition, Article 21 also stipulates that state core data, which is data that relates to national security, the lifeblood of the national economy, people’s livelihoods and major public interests, is subject to stricter regulation.

With respect to industry-specific rules currently available (e.g., those applicable to industrial data, securities and futures-related data and personal financial data), data categorization and classification systems already have been established. In light of the coming enforcement of the DSL, data categorization and classification systems are expected in more industries in the future, especially for those industries that bear the responsibility of supervising data security under Article 6 of the DSL (e.g., telecommunications, transportation, natural resources, hygiene and health, education and technology). Companies in the above-mentioned industries may keep a close eye on legislative developments with respect to data categorization and classification systems in their respective industries.

Data Security Obligation

Section 4 of the DSL imposes multiple obligations for data security, including but not limited to establishing and improving a data security management system; organizing and performing data security education and training; taking technical and other necessary measures to ensure data security; providing graded cybersecurity
protection; enhancing risk supervision; and taking appropriate measures against data breaches.

The data processors that process important data are subject to stricter regulation. They must explicitly appoint personnel and an administrative department to be in charge of data security, conduct periodic risk assessments and submit reports to the competent authority.

**Cross-border Data Transfer**

Article 31 differentiates how the cross-border transfer of important data is to be treated by critical information infrastructure (“CII”) operators as opposed to other data processors. Specifically, the Cybersecurity Law of China would apply to the administration of transfers of important data collected and generated by CII operators during their operations in China. The Cyberspace Administration of China, together with the relevant department(s) of the State Council, would make relevant rules to govern cross-border transfers of important data by other data processors.

If the data to be transferred outside of China is related to the protection of national security, national interests and the fulfillment of international obligations in accordance with law, and regards controlled items, such transfer will be subject to export controls and approval will be required before exporting data.

In addition, reciprocal measures for cross-border data transfers may be imposed if any country or region adopts discriminatory bans, limitations or other similar measures against China with respect to data related to, e.g., investment or trade and technology for data development and use.

In the case of any request made by foreign judicial or law enforcement organs for data stored in China, domestic organizations and individuals are prohibited from providing such data without the approval of the competent authority.

**Licensable Data Processing Service**

Service providers must obtain permits for relevant data processing services, as required by laws and regulations. The types of data processing services that will require licenses will be identified in future implementing rules.

**Agent Service for Data Transaction**

An agent that provides data transaction services must request that the data provider identify the source of data, check both parties’ identities for a data transaction and keep a record of both the review and the transaction.

As the fundamental law governing data security, the DSL provides more principles and policies but lacks detailed and practical rules. We believe a series of implementing rules will be introduced in the near future, which will provide more practical guidance for the purpose of compliance.

Copyright © 2022, Hunton Andrews Kurth LLP. All Rights Reserved.
Source URL: https://www.natlawreview.com/article/china-issues-data-security-law