July 12, 2021

China Adopts Data Security Law

Attorneys
Katherine Wang
David Chen
Xiwen (Rose) Wang

On June 10, 2021, the Standing Committee of the National People's Congress of the People's Republic of China adopted the Data Security Law (DSL), which will become effective on September 1, 2021. Together with the Cybersecurity Law (CSL) and the Personal Information Protection Law (Second Draft) (PIPL), these legislative developments demonstrate China's effort to build a comprehensive regulatory system to address the protection and processing of data with an increased focus on national security.

Scope and Extraterritorial Applicability

The DSL regulates all types of data processing activities carried out within the territory of China, including the collection, storage, use, refining, transmission, provision, and disclosure of data. For data processing activities performed outside of China, the DSL also applies to both foreign and Chinese organizations and individuals if they conduct the above data-related activities that could jeopardize national security, the public interest or the legitimate rights and interests of citizens and organizations in China.[1] Under the DSL, "data" is defined as all electronic and non-electronic records of information.[2]

The DSL authorizes the State to conduct national security assessments on data processing activities that affect or may affect national security, and stipulates that the security assessment determination made in accordance with law will be final.[3] As the State has broad authority to interpret the legal basis for conducting a security assessment, the practical ability to challenge or appeal an adverse determination appears to be quite limited. The use of security assessments in the DSL follows a similar approach taken in the CSL and the PIPL, which utilize security assessments as a way to legitimize cross-border data transfers for Critical Information Infrastructure Operators (CIIO) and personal information processors that are subject to data localization requirements.

The DSL imposes data security obligations similar to those already required under the CSL, including engaging in risk monitoring, immediately taking remedial measures against data security vulnerabilities and data security incidents, and timely notifying users and reporting to relevant regulators of data security incidents.[4] However, like the CSL, the DSL does not specify what is a data security incident that requires notification to users and reporting to regulators, nor the timing of when such notification and reporting needs to be made.

Hierarchical Classification and Categorization of Data

The Chinese government intends to classify and regulate data based on its importance to economic and social development, and the degree of harm to national security, the public interest, and the legitimate rights and interests of individuals and organizations if it is misappropriated.[5]

Certain sectoral regulators have already experimented with data classification as an approach to data governance. In March 2020, the Ministry of Industry and Information Technology (MIIT), released the Classification and Grading of Industrial Data (Trial), which provides guidance for the classification of data generated and applied throughout the life cycle of industrial products and services. MIIT's classification categorizes data into three levels according to the potential impact that the data may have on industrial production and economic benefits if misappropriated.[6] In the financial sector, under the Financial Data Security – Guidelines for Data Security Classification released by the People's Bank of China (PBOC) in September 2020, financial data-defined as various types of data that are collected or generated by financial institutions in the course of their operations-is to be classified into five levels based on the impact on national security, the public interest, the interests of personal information subjects, and the lawful interests of enterprises

if such data is damaged. Regulators in other sectors, including health care and telecommunications, are also expected to develop their own data classification standards and requirements.

Under the new DSL and the existing CSL, any data processing activities through information networks including the Internet will need to comply with the new data classification and data security obligations for data under the DSL and the existing multi-level protection scheme for network security established under the CSL.[7]

Important Data and Core State Data

The DSL includes a legal mandate to the central and local governments to enhance their oversight over important data and core state data. The concept of important data was first introduced in the CSL and remains a vaguely defined but important concept-as it is linked to data localization requirements and enhanced network and data security obligations for CIIOs under the CSL. The DSL further builds out the governance framework for important data by delegating the determination of what is important data to local governments and departments through the establishment of important data catalogues.[8] This decentralized approach raises concerns that different local governments and departments will develop different catalogues of important data, making compliance more costly and challenging. Notably, the DSL introduces a new category of data-core state data-a vaguely defined term that includes data that relates to national security, the lifeline of the national economy, people's livelihoods and major public interests, for which central and local governments are required to apply more stringent regulatory control. It remains unclear what the requirements are for businesses in respect of core state data.

The DSL also requires processors of important data to regularly conduct risk assessments and submit risk assessment reports to regulators.[9] These risk assessments reports are required to include the types and quantities of important data processed, details of the data processing activities being undertaken, and data security risks and countermeasures.[10] This new requirement expands regulation of important data-which under the CSL was limited to CIIOs-to all businesses that process important data. Consequently, in order to comply with the requirements of the DSL, it will be necessary for businesses to determine whether they process important data, to monitor the important data catalogues that are expected to be published by local governments and departments, and to ensure risk assessments and reporting thereof to regulators are performed. Businesses will also potentially have to disclose to regulators business-sensitive or network-security-sensitive details regarding their processing of important data.

Cross-Border Data Transfer

The DSL introduces separate frameworks for the regulation of cross-border transfers of important data by CIIOs and non-CIIOs.[11] For CIIOs, the export of important data collected and generated in China is governed by the CSL and requires passing a security assessment by relevant regulatory authorities. For non-CIIOs, the DSL specifies that the rules regulating the export of important data collected and generated in China will be developed by the Cyberspace Administration of China (CAC)-China's top cyberspace regulator-in conjunction with the relevant departments of the State Council. Since what constitutes important data remains unclear, the expansion of the regulation of cross-border transfers of important data to cover non-CIIOs under the DSL creates significant uncertainties to Chinese and multinational businesses that rely heavily on cross-border data transfers for their business operations and for their existing data-sharing arrangements.

In the case of any request made by foreign judicial or law enforcement agencies for data stored in China, domestic organizations and individuals must obtain an advance approval from the relevant Chinese governmental authorities in order to release such data. The DSL provides little detail on which Chinese authorities are responsible for issuing approvals and the approval procedures, and so it is unclear how businesses can meet this requirement without additional implementing regulations, measures or guidelines.[12] Moreover, the requirement could put businesses at odds with judicial and law enforcement agencies in their home jurisdictions as it relates to data stored in China, increasing legal compliance

risks. It is worth noting that the PIPL proposes a parallel prohibition on transferring personal information that is stored in China to judicial or law enforcement agencies outside of China without approval.[13]

Organizations and individuals directly in charge or directly liable for non-compliance can be fined for violations of these requirements at amounts specified in the DSL, which can be significant.

Government Data Access, Export Control and Geopolitical Tensions

The initial draft of the DSL was released at the beginning of July 2020 just after India banned TikTok and WeChat, citing data privacy and security concerns. The United States quickly followed with corresponding bans on similar grounds. The geopolitical tensions underlying these events are reflected in the DSL, which includes provisions that expand China's export control regime to cover the export of data[14] and provide a legal basis for China to impose reciprocal measures on any country or region that imposes discriminatory prohibitions, restrictions or other similar measures against China in terms of investment and trade related to data and data development and use technologies.[15] Accordingly, the DSL lays the foundation for the active use of data sovereignty by the Chinese government to protect its national security and to achieve its industrial and foreign policy objectives. The traditional focus of export control regimes has been technology, but the export control of data under the DSL clearly reflects the growing strategic importance of data globally.

Ongoing concerns around the Chinese government's access to data of businesses are likely to persist with the DSL. The DSL includes specific provisions requiring businesses and individuals to cooperate with public security and State security bodies that need to access data for the purpose of safeguarding national security or investing crimes.[16] Organizations and individuals directly in charge or directly liable that fail to cooperate can be fined for any violations at amounts specified in the DSL. Consequently, the legal bases for exporting data to China from jurisdictions that require strong legal protections against government access to personal information in the destination country will need to be reviewed in light of the DSL.

Penalties

The DSL introduces a dual penalty system for violations. Both organizations in violation and individuals directly in charge or directly liable can be fined.[17] For breach of data security obligations, organizations in breach could face a fine of up to CNY 2 million, as well as suspension of the relevant business and/or revocation of the relevant business license. Responsible individuals can face fines of up to CNY 200,000. For violations of the national management system for core state data, violators can face fines of up to CNY 10 million, as well as suspension of the relevant business and/or revocation of the relevant business license. Criminal liability may also apply if such activities constitute a crime. For violations of the requirements for the cross-border transfer of important data, organizations can face fines of up to CNY 10 million, suspension of the relevant business and/or revocation of the relevant business license, and criminal liability if such activities constitute crimes. Responsible individuals can also face fines of up to CNY 1 million. For unauthorized provision of data to overseas law enforcement or judicial authorities, organizations can face fines of up to CNY 5 million, and responsible individuals can face fines of up to CNY 500,000.

What to Expect

The new DSL represents a strategic move by the Chinese government to regulate the processing and cross-border transfer of data and assert its data sovereignty. However, many of the requirements and concepts require further implementation and clarification from regulators. We expect that in the upcoming months, relevant governmental authorities in China will issue a series of ancillary measures, regulations and policies to interpret and implement the provisions of the DSL. Foreign businesses that need access to or process data stored in China, or that process data relating to their China operations offshore, should pay close attention.

1. DSL, Article 2.
2. DSL, Article 3.
3. DSL, Article 24.
4. DSL, Article 29.
5. DSL, Article 21.
6. Classification and Grading of Industrial Data (Trial), Chapter 3 (available at http://www.cac.gov.cn/2020-03/08/c_1585210563153197.htm).
7. DSL, Article 21
8. DSL, Article 21.
9. DSL, Article 30.
10. DSL, Article 30.
11. DSL, Article 31
12. DSL, Article 36.
13. PIPL, Article 41.
14. DSL, Article 25.
15. DSL, Article 26.
16. DSL, Article 35.
17. DSL, Chapter 6.