July 8, 2021

China Passes Data Security Law to Take Effect in Less Than Two Months

By Liza L.S. Mark and Tianyun ("Joyce") Ji

On June 10, 2021, China's National People's Congress Standing Committee ("***NPC***") passed the Data Security Law ("***DSL***"), to take effect on September 1, 2021. This version of the DSL was fast-tracked after just two drafts for public comments in July 2020 and April 2021, respectively. The DSL will essentially have an impact on all businesses operating in China by imposing various obligations in processing and transferring data. Multinational companies ("***MNCs***") should be particularly mindful of the DSL because of the law's emphasis on cross-border data transfer. Together with the Cybersecurity Law ("***CSL***") passed by the NPC in 2017 and the soon-to-be final Personal Information Protection Law, China's cyberspace administration and data protection framework poses various compliance challenges for businesses with China operations.

Here are some highlights of the DSL:

1. Applicability of the DSL

According to Article 2 of the DSL, it applies to data processing activities in China. "Data" refers to any recording of information by electronic or other means, regardless of online or offline. "Data processing" is broadly defined to include the collection, storage, use, processing, transmission, production, and disclosure, etc. of data. Essentially all businesses operating in China will be subject to the DSL.

Article 2 further provides that the law has extraterritorial reach over data processing activities taking place outside China which undermine China's national security, public interest, or legal interest of citizens and organizations. It does not further specify as to what and how penalties can be imposed on individuals and organizations outside of China.

2. Data Classification Protection System

Article 21 of the DSL mandates that a multi-level data classification protection system be established, which classification will be based on the data's respective importance level in China's national economy, as well as the risk of harm to national security, public interests or the legitimate interests of citizens and organizations if such data is compromised. Although the DSL does not specify how the system will work, we expect it to be similar to the Multi-Level Protection Scheme (MLPS) developed under the CSL by various authorities, including the Cyberspace Administration of China (CAC) and industrial supervising authorities. The DSL also calls for the establishment of a data security review system for data processing activities that may impact national security, which decision becomes final and unappealable once rendered.

In Article 21, the DSL introduces two categories of data: "important data," and "national core data."

a. "Important Data"

The term "important data" was first introduced by the CSL. However, neither the CSL, the DSL nor any other existing laws or regulations has defined "important data." The laws merely provide that data would be considered "important data" if once breached, such data may directly compromise national security, economic development, or social and public interest. According to relevant national standards and identification guidelines, typical

examples of sectors with such data could include: natural resources, electric power, communications, metals, chemical, national defense, transportation, public health, pharmaceutical, finance, statistics, e-commerce, etc. The draft *Data Security Administration Measures* issued by the CAC in May 2019 defines "important data" as data that, if leaked, could directly affect national security, economic security, social stability or public health and safety, such as unpublished government information, or data relating to massive population, generic, geographic, and natural resources, and generally excludes businesses' internal operational and management data, or personal information.

As mentioned, the DSL will take effect September 1, 2021, presumably before any detailed guidelines are published. Therefore, businesses are encouraged to proactively self-assess and map their data profile to see what data may potentially fall into the category of "important data" and start preparing for enhanced compliance obligations.

b. "National Core Data"

Also, the DSL for the first time introduced the concept of "national core data," which is broadly defined as data that relates to China's national security, lifelines of the national economy, important aspects of people's livelihood, major public interests, etc. The DSL calls for even more enhanced protection for "national core data" than "important data", but again, detailed definition of what is "national core data" and detailed implementing rules and guidelines are expected to reveal what and how such data will be determined and regulated.

3. Expanded Restrictions on Cross-Border Data Transfer

According to the CSL, before transferring "important data" overseas, businesses that are considered a "critical information infrastructure operator" ("***CIIO***") are required to first go through a security assessment by measures adopted by the CAC together with relevant authorities. Practically speaking, such requirement essentially forces CIIOs to localize their data collection and processing activities within China. The DSL now expands the restriction of the transfer of "important data" to be applied to non-CIIOs and mandates that detailed measures governing non-CIIO's handling of "important data" to be further enacted. This new mandate in DSL suggests businesses which are not CIIO or in certain highly-regulated sectors (such as pharmaceutical and energy) in general may soon be required to localize their "important data" and be subject to export assessment obligations.

In addition, Article 36 of the DSL explicitly prohibits individuals and organizations from providing ***any data*** that is stored within China to foreign judicial or law enforcement authorities, without the approval of relevant Chinese authorities. Such requirement can have significant compliance implications on MNCs with cross-border legal proceeding and/or regulatory enforcement actions. The situation is still ambiguous right now, but it is certainly possible that the DSL will require MNCs' Chinese subsidiaries to first seek the Chinese government's approval before providing evidence and data in response to enforcement actions by foreign governments, such as FCPA, antitrust, or even SEC disclosure filings by public companies. [1]

[1] In addition, in 2018, the U.S. congress modified the Stored Communications Act ("SCA") through the Clarifying Lawful Overseas Use of Data Act ("CLOUD Act"), which expressly allows U.S. law enforcement through a warrant, subpoena or court order (collectively, "SCA Warrant") to access electronically-stored communications data located outside the United States provided that the information sought is relevant and material to an ongoing criminal investigation. Under the DSL, businesses that are subject to an SCA Warrant will need to seek approval from relevant Chinese authorities before complying with such warrant and transferring requested data.

4. Potentially Hefty Penalties

Violating the DSL can result in severe consequences for both the businesses and responsible individuals according to Articles 45 through 48. Potential penalties on businesses including suspension of the business, revocation of the business license, fines of up to RMB 10 million (approximately US$1.5 million), and potential criminal penalties. In addition, individuals directly responsible for violations may be subject to fines of up to RMB 1 million (approximately US$156,000) and potential criminal penalties. Entities may be punished for a failure to cooperate with the Chinese authorities' data requests, and for providing data to foreign judicial or law enforcement authorities without approval from relevant Chinese authorities.

5. Key Takeaways for Businesses

As with many other Chinese laws, the DSL merely sets out the general framework of China's new data security protection scheme without much detailed implementation rules and measures. Nonetheless, with the DSL soon to be effective in September, businesses (especially MNCs) should be prepared to do the following to ensure compliance:

- Conduct due diligence on the organization's existing data collected and processed in China and identify if any of the data may potentially be categorized as "important data," or even "state core data."
- Have dedicated personnel carry out and implement data security protection.
- Establish a sound data security management system and provide regular training to all employees within the organization.
- Evaluate the likelihood of providing data to foreign judicial or law enforcement agencies. If the possibility is beyond *de minimis*, consider how you want to store and process data to mitigate the risk of triggering the DSL.
- Closely monitor the progress of implementing regulations and measures of the DSL, and guidelines published by industrial regulatory authorities.

For more information, please visit our China Updates page or see the following resources:

- China Issues New Rules Regulating Personal Information Collection by Mobile Apps, April 28, 2021
- A New Gateway to China – Recent Policy Developments in the Hainan Free Trade Port, April 6, 2021
- China Issues Measures for the Security Review of Foreign Investments, February 9, 2021
- China Patent Law Fourth Amendment—Impact on Foreign Companies, January 26, 2021
- China Regulators Remove Restrictions on Insurance Fund Investment, December 14, 2020
- China Adopts Interim Provisions on the Review of Concentrations of Business Operators for the AntiMonopoly Law, November 30, 2020
- China Releases Draft Personal Data Protection Law for Comments, November 12, 2020
- China Adopts Export Control Law, November 5, 2020

haynesboone

- China Releases New QFII/RQFII Rules, October 27, 2020
- China Releases Provisions on Strengthening the Supervision of Private Equity Investment Funds (Draft), October 15, 2020
- China Releases Provisions on the Unreliable Entity List, October 5, 2020
- China Releases Revised Measures on Handling Complaints of Foreign-Invested Enterprises, September 23, 2020
- China Releases Administrative Measures for Strategic Investment by Foreign Investors in Listed Companies, September 10, 2020
- China Releases Draft Data Security Law, September 8, 2020
- China Releases Circular on Further Stabilizing Foreign Trade and Foreign Investment, August 24, 2020
- China Releases Draft Measures for the Administration of Imported and Exported Food Safety, August 18, 2020
- U.S. Listed Chinese Companies: Regulatory Scrutiny and Strategic Options, July 30, 2020
- China Passes Controversial Hong Kong National Security Law, July 9, 2020
- China's Relaxed Financial Sector May Aid Foreign Investors, June 18, 2020
- Is There a Law in China Similar to the US Defense Production Act?, May 8, 2020
- Coronavirus Brings Force Majeure Claims to LNG Contracts, March 4, 2020
- The Rise of China, March 4, 2020
- Coronavirus Fears Cast Cloud Over Dealmaking, February 27, 2020

Additional questions? Please contact Haynes and Boone lawyers Liza L.S. Mark and Tianyun ("Joyce") Ji.