The Asset Management Industry
SERVING INDIVIDUAL INVESTORS
INVESTMENT COMPANY INSTITUTE

MEMO# 33734

August 23, 2021

China's Data Security Law and Implications to Foreign Asset Managers

[33734]

August 23, 2021

TO: ICI Global Members
Global Regulated Funds Committee
Global Regulated Funds Committee - Asia SUBJECTS: International/Global
Operations RE: China's Data Security Law and Implications to Foreign Asset Managers

On 10 June 2021, the Standing Committee of the National People's Congress (NPC), China's top legislative authority, enacted the Data Security Law of the People's Republic of China[1] (DSL). The DSL will take effect on 1 September 2021.

The DSL regulates all types of data processing and data security administration activities carried out within the territory of China. This legislation, together with the Cybersecurity Law of the People's Republic of China(Cybersecurity Law)[2] and the Personal Information Protection Lawof the People's Republic of China (PIPL)[3] will provide the fundamental framework of laws that regulate cybersecurity and data security protection in China.

The DSL is broadly applicable to and will impact all parties doing business in or with China that engage in the processing of all types of data. While the DSL only sets out very broad principles, and industry regulators such as the People's Bank of China (PBoC) and the China Securities Regulatory Commission (CSRC) are yet to promulgate detailed implementing rules for their respective industries, foreign asset managers should be aware of the DSL's implication for their data processing activities both within and outside China (see section 1 below).

This memo provides a brief overview of the key provisions of the DSL and highlights the potential implications to foreign asset managers with operations in China.

Scope of Application and Extraterritorial Effect

The DSL broadly defines "data" as any record of information in electronic or other forms, including hard-copy written records of information. Data processing activities regulated by the DSL include, but are not limited to, the collection, storage, use, processing, transmission, provision and disclosure of data (DSL Chapter 1, Article 3).

The DSL applies to and regulates data processing activities and data security administration within China. It also imposes legal liability in respect of data processing activities conducted outside China that have the effect of harming the national security or public interests of China or the lawful rights and interests of any Chinese citizen or organization (DSL Chapter 1, Article 2).

Multi-tier Data Classification Framework

Under the DSL, data is classified and protected based on its importance to China's economic development, national security and public interest, the legitimate rights and interests of Chinese citizens and organizations, and also in accordance with the degree of potential harm that might result from any data breach.

The DSL refers to two special categories of data - "Important Data" and "National Core Data." National Core Data is defined as data relevant to national security, the lifeline of the economy, important parts of people's livelihoods and major public interests (DSL, Chapter 3, Article 21). Such data is subject to enhanced management and protection. "Important Data," on the other hand, is not defined under the DSL, but the DSL directs local governments and industry regulators to formulate their own categories of Important Data and measures to protect such data for their respective industries (DSL, Chapter 3, Article 21). It is expected that, based on the general data classification framework stipulated under the DSL, the PBoC/CSRC will issue industry-specific rules/requirements in relation to data classification for the financial industry.

Data will be subject to export control if it falls within the scope of items restricted from export either due to China's international obligations to protect such data or for the protection of national security (DSL, Chapter 3, Article 25).

Data Security Requirements

The DSL stipulates that the Multi-Level Protection Scheme (MLPS)[4], a process established under the Cybersecurity Law for assessing technology systems and their risks, shall form the basis for discharging data security protection obligations with respect to data processing activities (DSL, Chapter 4, Article 27). In other words, all entities carrying out data processing activities should comply with the data security requirements under the MLPS. In addition, data processing activities that affect or may affect China's national security will be subject to a national security review in accordance with the data security audit system established by the government (DSL, Chapter 3, Article 24).

Companies that process Important Data are required to conduct a periodic assessment of data processing activities and submit a report to the regulatory bodies. The report shall include information on the types and volume of Important Data, the collection, storage, processing and use of such data; and the data security risks and corresponding measures to address such risks (DSL, Chapter 4, Article 30). These companies are also required to appoint a data security officer and designate a management department to take responsibility for data protection (DSL, Chapter 4, Article 27).

Cross-border Data Transfers

The ability to transfer data outside China remains a major concern for multinational companies with businesses or employees in China. The DSL affirms the local storage requirement stipulated under the Cybersecurity Law, which requires an operator of critical

information infrastructure (CII)[5] to locally store personal information and Important Data gathered and produced during its operation within the territory of China. In relation to non-CII operators, the Cyberspace Administration of China (CAC) will formulate and issue separate cross-border transfer rules applicable to any Important Data collected and generated by such non-CII operators (DSL, Chapter 4, Article 31).

For the cross-border transfer of data for legal proceedings, the DSL explicitly prohibits companies from providing any data stored in China to foreign law enforcement agencies or other foreign judicial authorities without obtaining prior approval from the Chinese government (DSL, Chapter 4, Article 36).

Penalties

Non-compliance with the DSL may subject companies to significant fines and penalties, which vary depending on the types and severity of the violation (DSL, Chapter 6). These violations include failure to establish and complete a data security management system and risk monitoring measures, or perform periodic risk assessments, and failure to obtain prior approval for data transfer to foreign judicial or law enforcement bodies. The fines could be imposed on both the business operator and the managerial staff with direct responsibility for managing the data security. The authorities, in serious cases, may also order suspension of operations, cessation of business for rectification, or revocation of operation permits or business licenses (DSL, Chapter 6, Articles 45 and 46).

Next Steps

Although detailed implementation rules/guidelines specific to asset managers are yet to be released by the CSRC, foreign asset managers may wish to start the groundwork in preparation for the new regime. This could include reviewing their governance structures and systems covering all aspects of data handling, understanding the types of data collected and the processing cycle, and identifying potential areas for further evaluation or enhancement.

ICI Global will continue to monitor and keep members appraised of the relevant developments.

Alexa Lam
Chief Executive Officer, Asia Pacific
ICI Global

Irene Leung
Regional Lead, Member Relations and Research, Asia Pacific
ICI Global

Lisa Cheng
Research Analyst
ICI Global

endnotes

[1] See Data Security Law of the People's Republic of China, available (in Chinese only) at: http://www.npc.gov.cn/npc/c30834/202106/7c9af12f51334a73b56d7938f99a788a.shtml.

[2] The Cybersecurity Law came into effect on 1 June 2017. It is the first law addressing cybersecurity issues in China. It stipulates cybersecurity obligations for network operators and operators of critical information infrastructures (CII) in China. Under the Cybersecurity Law, personal information and other important data collected by the CII operators must be stored within the borders of China. Security assessments and approval from industry regulatory bodies are required for their transfer outside mainland China. See Cybersecurity Law of the People's Republic of China, available (in Chinese only) at: http://www.cac.gov.cn/2016-11/07/c_1119867116.htm.

[3] The PIPL, which adopts principles broadly similar to those in the EU's General Data Protection Regulation (GDPR), will come into effect on 1 November 2021. The PIPL is China's first comprehensive law on the protection of personal data, regulating how personal information is collected, stored, used, and shared in China.

[4] Under MLPS, all network operators are required to assess the current state of their information and operations technology systems and the risks associated with them. They should propose a defined protection level for their network based on the potential impact of a data breach or system compromise. Level ranges from 1 to 5, with 5 reserved for sensitive government facilities and systems. Higher levels have more stringent security requirements. Systems classified as Level 2 or above require an independent assessment by a recognized independent expert. Final certification will be issued by the region-level Public Security Bureaus.

[5] CII refers to information infrastructure in important industries and sectors which, in the event of damage thereto, loss of function thereof or leak of data therefrom, could seriously jeopardize national security, national economy and people's livelihoods, or the public interest. This includes public communications, information services, energy, transportation, water conservancy, finance, public services, electronic public services and defense technology.