GDR NEWS

China’s new Data Security Law – one month to implementation

30 July 2021

*Morgan Lewis & Bockius Shanghai partner **Todd Liao** and associate **Sylvia Hu** analyse how companies can comply with China’s new data security framework.*

China’s new Data Security Law (DSL) comes into effect on 1 September 2021.Its broad scope will potentially affect all organisations with a presence in China, including multinational corporations. It entails more expansive and restrictive requirements on data localisation, mandatory security level certification, and severe penalties for unauthorised foreign transfer of data. We take a closer look at these requirements, the background to the law being passed in addition to the implications for those impacted.

Background

First published on the *Global Data Review* website, July 2021

The DSL was passed by the Standing Committee of the National People's Congress on 10 June 2021. It followed two rounds of drafts for public comments and left around one month for businesses operating in China to accommodate to the new regime. According to Article 3 of the DSL, it regulates a wide range of data-related activities, which apply to any data processing activities including “collection, storage, use, processing, transmission, provision and disclosure” of data in both electronic and non-electronic forms. Article 3 also provides a broad definition of “data security”. It refers to “adopting necessary measures to ensure that data is effectively protected and legally used, as well as maintaining the capacity to ensure a sustained state of data security.”

China’s Cybersecurity Law (CSL), already in effect since 2017, established several of the principles that are covered and enhanced by the DSL. For example, the DSL introduced a new concept, “national core data”, which brings stricter protection mechanisms than those for “important data”. The CSL had already set up a multilevel protection scheme (MLPS); the DSL now re-emphasises its importance and also enhances data security obligations. The DSL also steps up penalties where there is unauthorised foreign transfer of data.

Under Article 21 of the DSL, China will establish a “categorical and hierarchical system” based on the “importance of the data in economic and social development as well as the extent of harm to national security, public interests, or lawful rights and interests of individuals or organisations that would be caused once the data is tampered, destroyed, leaked, or illegally obtained or used”. On this basis, some special data including “important data” and “national core data” are protected by stricter regulatory measures.

Article 2 of the DSL sets out its extraterritorial reach – which governs not only data processing activities within China, but also those carried out outside China that harm “the national security, public interests, or lawful rights and interests of citizens and organisations in China”.

First published on the *Global Data Review* website, July 2021

Important vs National Core Data

Important Data

The CSL and other previous data protection regulations provide stricter requirements for the protection of important data, but fail to concisely define what important data is. In the absence of a clear definition, business operators in China have to determine on their own whether the data they process constitutes important data.

The DSL attempts to address this uncertainty by providing that the Chinese government will publish an important data catalogue at the national level; each region and department shall also determine their own "catalogues of important data" based on the national catalogue of important data. This means the Chinese government will set official criteria for important data, rather than allowing business operators to decide the scope of important data at their discretion. After the catalogue is released, a framework of procedures to recognise important data will be developed. The establishment of these catalogues will better assist companies to navigate their specific compliance obligations.

Under the DSL, if business operators process data that falls under the important data catalogues, the following requirements will apply:

- **Designation of a responsible person**. Companies processing important data should designate persons responsible for data security and establish data security management bodies to ensure compliance with their data security obligations (Article 27).
- **Risk assessments**. Companies processing important data should periodically carry out risk assessments for their data processing activities and submit a risk assessment report to the relevant government authority (Article 30).

National core data

"National core data," a new category of data, is introduced by the DSL. According to the DSL, China will "implement a stricter management system" for national core data, which is defined as "data related to national security, the lifeline of the

national economy, important aspects of people's livelihoods, and major public interests" (Article 21).

Companies violating the management system of national core data will face severe penalties, including a fine of up to 10 million yuan (US$1.54 million), cancellation of business licences, and even criminal penalties (Article 45). Nonetheless, the definition of "national core data" and its management system are still very general under the DSL and need further interpretations.

Data localisation and national security

Under the CSL, all personal information and important data collected or generated by critical information infrastructure operators (CIIOs) within the territory of China should be stored within China. CIIOs are entities engaged in critical information infrastructure industries (eg public communications and information services, energy, transportation, water conservation, finance, public services, etc) whose network system and information systems would seriously harm China's national security, national economy, people's livelihoods, or public interests if they were damaged, malfunctioned or suffered a data leak. If there is a specific business requirement for a CIIO to transfer data outside China, such transfer should undergo a security assessment approved by the Cyberspace Administration of China (CAC) or other designated government authorities.

The CSL imposes data localisation requirements on CIIOs only but provides no additional information for other companies. The DSL attempts to bridge this gap by providing that the government will further formulate relevant regulations on the cross-border transfer of important data by companies other than CIIOs. Based on the provisions of the DSL, it seems that even if companies do not squarely fit within the CIIO description, they may also be subject to restrictions on cross-border transfers if they process data that falls under the important data categories.

National security obligations

The State Security Law enacted in 2015 established a national security review and oversight management system. As data security is a crucial part of national security, Article 24 of the DSL builds up a system for "data security reviews" to

examine any data activities that may be deemed to pose risks to national security. In addition, Article 25 also empowers the government to impose export control measures on data related to the protection of national security and interest and China's performance of international obligations.

Further clarity is required here both in relation to CIIO, and on Articles 24 and 25 looking at the data security review system and export control measures. We are expecting additional guidance from the Chinese government on the implementation of these aspects of the DSL.

Multilevel Protection Scheme Requirements

The MLPS was a technology and information security system previously established by the CSL. Article 27 of the DSL re-emphasises the importance of the MLPS. The DSL states that the MLPS should be the fundamental ground of data processing through the information network, which means all entities carrying out data processing activities should comply with the data security requirements under the MLPS.

Under the MLPS certification system, companies must have a thorough assessment of the risks and the conditions of their information and network systems with servers located in China. And based on the assessment and the complicated classification standard set by the MLPS, companies are required to evaluate and determine the level to which the company's information and network systems belong – from the lowest Level 1 to the highest Level 5 – according to their relative impact on national security, social order, and economic interests if the system is damaged or attacked. Networks that do not affect national security, social order, and public interests are usually classified as Level 1, while networks that may affect social order and public interest are classified as Level 2 or above. Systems or applications with higher degrees of impact are more likely to be classified as Level 3 or even Level 4. Level 5 is usually reserved for state-owned military systems. Companies will be subject to various technical requirements depending on the classification of the systems. More administrative procedures are required if a company is classified as level 2 or above.

The DSL also imposes multiple obligations for data security based on the ground of MLPS requirement, including establishing and improving a data security

management system; organising data security training; taking technical and other necessary measures to ensure data security; enhancing risk supervision; and taking appropriate measures to prevent data breaches, etc. Violations of data security obligations may result in a fine of up to 2 million yuan (US$307,000) and a suspension of related business, and a fine of up to 200,000 yuan (US$31,000) on responsible persons.

Inspections by Chinese government authorities

The DSL regulates Chinese government authorities' data collection activities.

Article 35, on the one hand, states that organisations and individuals shall cooperate with "public security organs and state security organs in data collection to preserve national security or investigate crimes according to laws". It is not only an emphasis on organisations and individuals' duty in domestic judicial or administrative proceedings, but also implicates DSL's extraterritorial reach. For example, if domestic organisations or individuals engage in cross-border telecommunications fraud or online gambling activities, relevant authorities can require them to provide the data they produced outside China. In addition, multinational companies may also face authorities' request, in judicial investigations under Chinese law, to obtain their data stored abroad. Under these circumstances, even if the data activities are conducted in a foreign jurisdiction, organisations or individual may still be required to comply with their duties prescribed by Article 35, otherwise they may be subject to a fine of up to 500,000 yuan (US$77,000); the directly responsible person may also face a fine of up to 100,000 yuan (US$15,000).

On the other hand, government authorities are prohibited from collecting data in an arbitrary manner. Article 35 requires authorities to "follow relevant state provisions and complete strict approval formalities in data collection". Furthermore, companies should also be aware of their rights to request proof of investigators' identities and authority when faced with governmental data collection.

First published on the *Global Data Review* website, July 2021

Data transfer to foreign authorities

The US CLOUD Act expanded the ability of law enforcement authorities in the US to obtain foreign data – prompting concerns that such access could infringe foreign governments' data sovereignty. The International Criminal Judicial Assistance Law of China, promulgated in 2018, created a mandatory pre-approval process before evidentiary materials relating to criminal proceedings could be exported out of China. The Securities Law, amended in 2019, also provided a similar clause from the perspective of securities finance.

In light of this background, Article 36 of the DSL also requires domestic organisations and individuals to obtain approval from competent government authorities before providing data stored within China to foreign judicial and law enforcement agencies. Compared to the previous regulations that covered only the fields of securities finance and international criminal assistance, Article 36 seems to be a catch-all provision that prevents unpermitted data leakage to foreign authorities – covering civil, administrative, criminal, and any other foreign judicial and law enforcement proceedings.

Entities providing data stored in China to foreign authorities without government approval may be subject to a fine of up to 1 million yuan (US$154,000), and the directly responsible person may be subject to a fine of up to 100,000 yuan (US$15,000). If the violation is serious, entities may be subject to a fine of up to 5 million yuan (US$768,000) and cancellation of business licences, and the directly responsible person may be subject to a fine of up to 500,000 yuan (US$77,000).

Transaction agents

Given the high-speed development of the market of data transaction intermediary services, the DSL creates additional duties for data transaction agents. According to Article 33 of the DSL, when providing agent services for data transactions, agents "shall require the data provider to explain the source of data and shall review and verify identities of both parties to the transactions and maintain proper records of the verifications and transactions."

First published on the *Global Data Review* website, July 2021

For data transaction agents that fail to perform their duties, they will be subject to punishments including “request for rectification, confiscation of the unlawful gains, cancellation of business licences,” and a fine of up to 10 times the value of the unlawful gains or a fine of up to 1 million yuan (US$154,000) if there are no unlawful gains. Additionally, the directly responsible person will also be subject to a fine of up to 100,000 yuan (US$15,000) under Article 47.

As with many Chinese laws, certain provisions in the DSL only provide a general framework and details will be set out in implementation rules that have yet to be issued. We await further guidance on several areas set out by the DSL – but organisations with operations in China should take heed and take appropriate steps to review their data collection and processing practices in China.

First published on the *Global Data Review* website, July 2021