FANGDA PARTNERS
方達津師事務所

NEW ERA OF CHINESE COMPLEX DATA PROTECTION LAWS - Introduction of China's Data Security Law

Authors:

Kate Yin
Partner, Fangda Partners
kate.yin@fangdalaw.com

Gil Zhang
Partner, Fangda Partners
gil.zhang@fangdalaw.com

China's Data Security Law ("**DSL**") was promulgated on June 10, 2021 and will come into force on September 1, 2021. To supplement China's existing Cyber Security Law, this new important legislation introduces various new principles and rules on data processing and data protection. With less than three months to get prepared for compliance with various new requirements on data processing, companies in China - including affiliates and subsidiaries of multinationals - should consider data and processes mapping exercises to complete the fact-finding of their data processing activities and analyze the gaps in order to ensure compliance with data protection laws in China.

Territorial scope of the DSL

The DSL applies to any data processing activity, as well as supervision of data processing, in the territory of China. "Data" is not limited to personal data; rather, it is broadly defined as any information that is recorded in electronic or other means or forms. Processing as defined by DSL includes, but is not limited to, collection, storage, use, process, transmission, provision and disclosure, which is similar to the processing in the GDPR and the latest draft of the China's Personal Data Protection Law ("**PIPL**").

The DSL applies extra-territorially to data processing that takes place outside the territory of China and damages the national interest, public interest of China or any lawful interest of the organizations or citizens of China. The building block of "damages the national interest, public interest of China or any lawful interest of the organizations or citizens of China" may be open to interpretation.

Supervisory authorities

The DSL does not provide an omnibus regulator to supervise and regulate data security within China. Instead, the DSL provides that the leading national security authorities of the Chinese central government (e.g. Ministry of State Security, Ministry of Public Security and Cyberspace Administration of China) are in charge of the planning and coordination of overall national data security matters and strategy. Each sectoral authority and local government has the authority to implement data security regulation within the sector or province, respectively.

The Cyberspace Administration of China ("**CAC**") is authorized to regulate the security of data and coordinate among the central government ministries. The sectoral regulators will continue to play an important role in data security within the sector.

National data classification and protection of "important data" and "core data"

Article 21 establishes the national data classification system. This requires data to be classified and protected based on the importance of data in relation to economic and social development, as well as the potential damage to national security, public interest, or lawful rights and interests of citizens or organizations should the data be compromised.

Following the data classification, the DSL reiterates the protection of "important data" and introduces a new concept of "national core data". "National core data" is defined as data that is related to national security, the national economy, and critical social well-being and material public interest. Both "important data" and "national core data" require a higher level of protection than has previously been applicable. That said, the DSL does not yet provide clarity on the approach as top what constitutes "important data" and "national core data", nor are the rules clear on processing and retention of such important data and national core data. Despite this, Article 45 of the DSL provides administrative penalties for breach of the provision on protection of the core data, including a fine up to RMB10 million, suspension of business, the imposition of a rectification order and even, at the most punitive, revocation of business licenses.

The "important data" is subject to the following special requirements in addition to data security obligations:

1) Article 27 requires the important data processor to designate specific individual(s) or department(s) to be in charge of data security.
2) The important data processor is required to report periodically to relevant authorities, filing a risk assessment report on the processing of important data. The risk assessment report shall include the categories of important data, amount, processing activity and the potential risks and mitigation measures.
3) Article 31 reiterates the requirements relating to cross-border data transfer by the critical information infrastructure operator ("**CIIO**"). The CIIO is required to carry out a security assessment for any cross-border transfer of the important data that is generated or collected within China.
4) For non-CIIOs, the DSL only authorizes the CAC to coordinate with other ministries to make rules for the cross-border transfer of important data.

Export control on data and national security review of data processing activities

The data related to the restricted items that are subject to export control restrictions under Chinese laws is also subject to export controls, which means that such data cannot be freely transferred outside China in the absence of approval from relevant Chinese authorities.

Certain data processing activity that impacts or may impact the national interest could be subject to national security review under the DSL. It is not yet clear what the threshold is or the applicable mechanism for carrying out such a national security review in relation to data processing activity.

Protective obligations of data security

Chapter 4 of the DSL sets out various data-protective obligations on companies and individuals in relating to the processing of data, as well as setting out the principles of social morality and ethics that apply to data processing activity and development of new technologies. The DSL also reiterates the protection of network and implementation of multiple-level protection system. The DSL also provides that companies should have set up training progams and IT structures to ensure compliance with the new regulations, including those related to risk monitoring and contingencies.

Failure to comply with these requirements on protection of data will result in administrative penalties, including rectification orders, warnings, suspension of business, revocation of licenses and fines of up to RMB2 million. Where such offenses are committed, those directly responsible may be fined, with fines ranging from RMB50,000 to RMB200,000.

Pre-approval for the provision of data to foreign authorities or judicial bodies

Article 36 provides that, in the absence of pre-approval by supervisory authorities of the Chinese government, any organization or individual in China shall not provide data that is stored in the territory of China to foreign authorities or judicial bodies. Failure to comply will result in warning by the supervisory authorities, a fine of between RMB100,000 and RMB1 million, or, in the event of a serious offense, of between RMB 1 million and RMB5 million, and suspension of business or revocation of business license; those personnel found to be directly responsible for any such breach may face being fined up to RMB 500,000, in the event of serious offense.

It is not clear at this stage which ministry will be responsible for coordinating the pre-approval and making further implementation measures for Article 36 and what the specific process is for obtaining pre-approval. This provision will clearly have an impact on the internal investigation process related to sending data used in multinational companies and providing and submitting data to foreign courts in litigation, as well as on how companies respond to the law enforcements and investigation by foreign authorities (e.g. investigations initiated by SEC or DOJ in the US).

Many building blocks of this provision require further clarity from the authorities, such as what is meant by "supervisory authorities", "organizations and individuals in China", "foreign authorities and judicial bodies", "provision of data", and "data stored in the territory of China". Will foreigners on short-term visits in China to conduct investigation and provide data to the foreign authorities for self-disclosure be subject to pre-approval? Similarly, does scope of data mean information in any form? Will employees or consultants who are outside China but employed by companies in China fall within Article 36? What data can or cannot be provided to foreign authorities or judicial bodies? These questions and others need to be addressed. In the meantime, companies need carefully how best to respond to foreign litigation or law enforcement in the context of the DSL.

Other important rules

Article 26 provides that where any country or region that implements discriminatory measures against China to restrict or prohibit Chinese companies or individuals from data processing and data and technology utilization and development, China can respond by implementing countermeasures against such country or region. It is worth watching whether China will impose or require similar scrutiny and supplementary measures when personal data is transferred from China to EU given that EU specifically called out China as one of the countries that warrants more stringent measures when transferring European Economic Area (EEA) personal data to China.

What's next?

The DSL lays good foundation for many rules to come. As many provisions of the DSL are largely principle-based we expect the regulators will provide more clarity and implementation measures shortly after the DSL comes into force. The measures on protection of CIIO and data security implementation measures are already on the Chinese central government's agenda for 2021. Now that the PIPL is expected to be in force within three months, companies in China that are likely to be impacted should initiate data mapping processes and analyze where there are gaps in terms of compliance with data protection laws. They are strongly urged to plan ahead.

Planning ahead is all the more important, given that the Chinese government – as reflected in the DSL – has put a high priority on the development of a digital economy and, therefore, on data as an asset. It is worth watching the space how China will open up the market of data brokerage and open the data generated from the public services and administration.

**Our associate Huihui Li also contributed to this article.*

Beijing

27/F, North Tower
Beijing Kerry Centre
1 Guanghua Road
Chaoyang District
Beijing 100020, China

Tel: +86 10 5769 5600
Fax:+86 10 5769 5788

Guangzhou

17/F, International Finance
Place, 8 Huaxia Road,
Zhujiang New Town
Guangzhou 510623, China

Tel: +86 20 3225 3888
Fax:+86 20 3225 3899

Hong Kong

26/F, One Exchange Square
8 Connaught Place, Central
Hong Kong

Tel: +852 3976 8888
Fax:+852 2110 4285

Shanghai

24/F, HKRI Centre Two,
HKRI Taikoo Hui
288 Shi Men Yi Road
Shanghai 200041, China

Tel: +86 21 2208 1166
Fax:+86 21 5298 5599

Shenzhen

17/F, Tower One, Kerry Plaza
1 Zhong Xin Si Road
Futian District
Shenzhen 518048, China

Tel: +86 755 8159 3999
Fax:+86 755 8159 3900