ALLEN & OVERY | 朗悦
LANG YUE | 安理国际律师事务所

New PRC Data Security Law

China's Latest Step in Building its Comprehensive Data and Cybersecurity Regime

Speed read

- ✓ Adds key items to China's existing data system
- ✓ Re-affirms clear hierarchy of responsibility of different parties in respect of the handling and protecting of important data collected and generated in China
- ✓ Imposes new restrictions on exporting data in response to requests from foreign judicial or enforcement bodies – impact on MNCs and parties who must comply with foreign data production obligations
- ✓ Penalties articulated for violation
- ✓ Becomes effective on 1 September 2021

Background

The Standing Committee of the National People's Congress (NPCSC) enacted the Data Security Law of the People's Republic of China on 10 June 2021 (Data Security Law). The law provides an overarching legislative framework for data security in the PRC, broadly defined, but will run parallel to other legal regimes, such as those relating to cyber security, archives, and the administration of state secrets and classified information. The Data Security Law will take effect on 1 September 2021.

Key Definitions

The term for data (数据) is defined expansively under the new law to include "any record of information in electronic or other forms". As such, under this law, data includes both electronic data (data stored electronically), as well as hard copy documents, among records stored in other forms. Likewise the term "data processing" (数据处理) is defined quite broadly to include the collection, storage, use, processing, transmission, provision, or disclosure, etc., of data. Data security refers to the implementation of necessary measures to ensure the state of effective protection and lawful utilization of data, as well as having the capacity to ensure a sustained state of security.

While the Chinese government is responsible for administering the data security regime, the new law re-affirms that all individuals, companies, and organisations have various degrees of responsibility for data security. Specific industries will have measures applicable to their industries as they already do in many sectors. The new law suggests multiple competing regulators at the central and local level, with perhaps some overlap in enforcement responsibility. This adds a further layer to the existing CIO, NIO structure established in the Cybersecurity Law.

Cross-border Data Transfer in Response to Requests from Foreign Judicial and Law Enforcement Bodies

One aspect of the new law that is getting a fair amount of initial attention from legal commentators is Article 36 and its corresponding penalty provisions set out in Article 48. Article 36 requires a company or individual in China to seek permission from "competent organs of the PRC" before data can be transferred outside of China when certain circumstances apply, discussed below. Article 36 provides in translation:

> *The competent organs of the People's Republic of China will, in accordance with relevant laws and international conventions or agreements to which the PRC has acceded, or in accordance with the principles of equality and reciprocity, handle the requests from foreign judicial or enforcement*

organs which concern the provision of data. Without the approval of the competent organs of the People's Republic of China, organisations or individuals within the territory [of the PRC] must not provide data stored within the territory of the PRC to foreign judicial or enforcement organs.

The precise meaning of the prohibitions contained in Article 36 is unclear and may be developed over time by implementing regulations or judicial interpretations. Moreover, whether Article 36 would be applicable to a particular situation will likely depend on the specific facts and require a careful analysis.

From the language used in the provision, together with an examination of related provisions in Chinese law, Article 36 certainly appears to cover formal requests from a foreign court or enforcement agency, such as a subpoena directed to a company in China by a U.S. court or regulator in connection with a criminal probe in the United States. In this respect, Article 36 tracks the approach outlined in Article 4 of the PRC International Criminal Judicial Assistance Law and Article 177 of the PRC Securities Law.

But how broadly the provision will ultimately be interpreted remains to be seen. For instance, purely internal investigations do not appear initially to fall within Article 36's scope, but what about investigations conducted where a party is cooperating with a foreign regulator? Or how will party-compelled discovery requests in U.S. civil lawsuits be evaluated under the statute? How will Chinese regulators respond if the Chinese party objects? These are important questions that may put MNCs in a bind as they navigate competing legal regimes.

Moreover, whereas previous Chinese blocking statutes lacked enforcement mechanisms, violation of Article 36 may lead to serious consequences, including fines of up to RMB5,000,000 (approximately US$750,000), orders to stop relevant operations or suspend operations for rectification, and revocation of relevant operational permits or business licenses. How these penalties will be implemented in practice also raises significant questions. Are fines to be viewed per occurrence, or more generally based on an overall event of non-compliance? It is also unclear which organ(s) of the PRC will be responsible for processing requests for clearing data transmissions to foreign courts or law enforcement, but we expect this will be developed in time and may depend on the type of case in which requests are made.

Mechanism for Protecting Important Data

Another significant aspect of the Data Security Law is the extensive protection mechanism for important data (重要数据) – scattered across Articles 21, 30, and 31. Unlike the Cybersecurity Law, which provides a general requirement that the critical information infrastructure operator localise important data while not defining the term "important data", the Data Security Law: (a) specifically calls for central and local government authorities to promulgate important data catalogues, which should give data processors more clear guidance on the scope of important data for purpose of implementation; (b) extends the cross-border transfer security administration to all processors of important data that is collected or generated in China; and (c) expressly requires all processors of important data to carry out a periodic risk assessment of its data processing activities and submit a risk assessment report to the competent authorities. As such, we anticipate catalogues and implementing rules in the near future. Those companies that engage in a substantial amount of data export activity (such as MNCs with Chinese subsidiaries, online companies, and hi-tech companies) may be faced with having to quickly adjust their data compliance policies and the underlying IT infrastructure deployment.

One additional feature of this law is the substantially increased penalties for non-compliance, as compared to those under various prior legislation. For instance, the administrative fine for failure of notification to competent authorities in the event of data breach is now up to RMB2,000,000, ten times that set out under the Cybersecurity Law; or up to RMB10,000,000 for illegal export of important data, twenty times higher than the maximum penalty enumerated under the Cybersecurity Law. This could foreshadow increased law enforcement activity in this area in the future.

International clients with operations in China will need to be mindful of how the new Data Security Law interacts with other laws that cover similar areas, such as the Cyber Security Law, and various laws and regulations concerning data privacy, state secrecy, bank secrecy, business archives, and accounting work papers. In addition, any company with Chinese operations – whether in the state or the private sector – and which may be caught up in an investigation or proceeding overseas, regardless of the subject matter (US sanctions, anti-corruption, antitrust or customs investigations, etc.), will need to pay careful attention to how it shares China-based data.

FOR MORE INFORMATION PLEASE CONTACT

Allen & Overy

Victor Ho
Managing Partner of A&O LLP in Beijing and Shanghai
Registered Foreign Lawyer, Hong Kong
victor.ho@allenovery.com

Richard Qiang
Counsel, Beijing
richard.qiang@allenovery.com

Richard Wagner
Registered Foreign Lawyer, Hong Kong
richard.wagner@allenovery.com

Eugene Chen
Registered Foreign Lawyer, Hong Kong
eugene.chen@allenovery.com

Jack Wang
Partner, Shanghai
jack.wang@allenovery.com

Jane Jiang
Partner, Shanghai
jane.jiang@allenovery.com

Shanghai Lang Yue Law Firm

Melody Wang
Partner, Shanghai and Beijing
melody.wang@allenoveryly.com

Ran Chen
Counsel, Beijing
ran.chen@allenoveryly.com