HAYNES BOONE

December 13, 2024

China Releases Regulations on Network Data Security Management

Authored by: Liza L.S. Mark and Tianyun (Joyce) Ji

On Sept. 24, 2024, China's State Council released the "Regulations on Network Data Security Management" (《网络数据安全管理条例》) (the "**Regulations**"), to take effect on Jan. 1, 2025. The Regulations introduce specific controls for network data processors, focusing on issues concerning personal information (the "**PI**"), important data, and cross-border data transfers. On the legislative hierarchy, the Regulations provide detailed guidance on the implementation of China's trio of laws governing data protection, i.e.: Cybersecurity Law (《网络安全法》) (CSL), Data Security Law (《数据安全法》) (DSL) and Personal Information Protection Law (《个人信息保护法》) (PIPL) (collectively, the "**Data Laws**"), and are superior to the rules issued by the Cyberspace Administration of China (CAC) in relation to specific regulatory matters. The Regulations affect all businesses that process electronic data and are relevant to businesses of all sizes, especially their internal data processing systems.

Here is a summary of the highlights of the Regulations:

1. TAKEAWAYS

The Regulations were finalized after more than three years of lengthy rule preparation and consultation by China's State Council. They address key issues previously left open by China's set of Data Laws, especially with respect to the classification of "Important Data" and relating data protection measures. The Regulations suggest that reporting of data incidents, data protection agreements, record-keeping and compliance assessments/reporting will likely become the new enforcement focus of the CAC.

As such, businesses are advised to conduct at least the following compliance checks before the Regulations take formal effect in 2025:

- Revise and update privacy policies, preferably with a Chinese addendum to reflect the most up-to-date obligations under the PIPL.
- Online platform operators need to constantly monitor in-platform data processing activities to ensure that data and algorithms on their platforms allow for equal access by users and are not abused to discriminate.
- Businesses that process PI and/or Important Data should conduct a comprehensive review of data processing activities and clarify their subject.
- Businesses that have cross-border data transfer necessities should evaluate if their situations would fall within the now-expanded permissible data export scenarios, which exempt the otherwise-required mechanisms of security assessment, certification or the standard contract.
- Businesses should use tools, including risk assessments, compliance audits and annual reporting to fulfil their security management responsibilities as well as to improve their own network data security management capabilities.

2. APPLICABILITY OF THE REGULATIONS

The Regulations define "network data" to be "all kinds of electronic data processed and created through networks," which excludes data processed by physical means, such as on paper. The Regulations further define "network data processor" as "individuals or organizations that decide, on their own, the purpose and processing method of the network data processing activities." Considering the prevailing use of network processing data and digitization, most businesses are therefore subject to the Regulations.

According to Article 2, the Regulations apply to network data processing activities and their safety supervision and management in China. The Regulations also have extra-territorial effects as applying to activities taking place outside China, including processing Chinese individuals' PI, as well as activities that would harm China's national security, public interests or the lawful rights and interests of citizens or organizations. While extra-territorial application was already covered by laws like the PIPL, the Regulations specifically set forth that foreign data processors need to establish a designated organization or appoint a representative in China whose names and contact information are required to be registered with the local CAC.

3. IMPORTANT DATA

For the first time ever, the Regulations provide a clear definition of "important data." This concept is frequently mentioned in China's data security laws and regulations, but never before clearly defined. The Regulations define "important data" as "data in certain fields, for certain groups, from certain regions or that reaches a certain scale or precision, which if compromised, could directly threaten national security, economic stability, social order or public health and safety" ("**Important Data**"). While the definition is quite general, businesses are required to identify and report data that potentially can be categorized as Important Data with relevant authorities (including the local CAC and industrial regulatory authorities, such as the People's Bank of China for the banking industry, etc.) from time to time to determine what is Important Data.

Key obligations relating to Important Data as provided under the Regulations include:

a. Mandatory Risk Assessment

The Regulations mandate that network data processors of Important Data should conduct a risk assessment before providing, commissioning or co-processing Important Data. In addition, such processors should also conduct risk assessments on an annual basis of their network data processing activities and submit reports to the CAC.

b. Dedicated Network Data Security Officer

The Regulations require all network data processors of Important Data to appoint a security officer for network data and establish a data security management organization to perform the following responsibilities: implementing network data security management systems and emergency response plans; conducting regular monitoring, risk assessments, emergency drills and staff training; and handling complaints and reports related to network data security.

The network data security officer must have relevant expertise and experience and must be a member of the processor's senior management who can report directly to the CAC.

c. Important Data Catalogue

Article 29 of the Regulations mandates that a National Data Security Coordination Mechanism under the leadership of China's National Security Commission be established to work with relevant authorities to create an Important Data catalogue. Regional and industrial regulators will be responsible for identifying and safeguarding Important Data within their jurisdictions. Relevant authorities will notify or publish data identified as Important Data, and processors of network data will be required to fulfill their data security obligations if the data they process are deemed Important Data by the government authorities.

4. PROTECTION OF PERSONAL INFORMATION

Chapter 3 of the Regulations is dedicated to setting forth obligations of network data processors in processing PI, especially with respect to "notification and consent" compliance and processors of Important Data.

a. Notification, Consent and Right to Portability

Per PIPL's "notification and consent" requirement, the Regulations list the matters that need to be included in such notice to individuals, which are to: (i) include the specific PI rights, including the rights to inspect, copy, transfer, correct, supplement, delete, restrict the processing of personal information, as well as to deactivate accounts and withdraw consent; (ii) specify the purpose, method and type regarding processing the relevant PI, as well as the information on the data recipient (in the form of a list), if PI is provided to other network data processors; and (iii) clearly define the method for determining the retention period, if a specific retention period is hard to determine.

If the notice sent by the business per PIPL does not contain the foregoing elements, then the business risks such consent being invalid. Additionally, where consent is relied on as the legal basis for PI processing, the Regulations emphasize that such consent shall not be obtained through misleading, fraudulent or coercive means, and the personal information shall only be collected to the extent necessary for providing products and services. [1]

The Regulations also clarify individuals' right to data portability under the PIPL, allowing for easier and more streamlined transition of user accounts across different platforms. Specifically, the network data processor should provide means for a third party designated by the individual to access and obtain relevant PI if the request for PI transfer meets the following criteria: (i) the identity of the individual requester can be verified; (ii) the transfer is of PI that the individual has consented to provide or that has been collected based on a contract; (iii) it is technically feasible; and (iv) the transfer does not infringe upon the legitimate rights and interests of others.

b. Increased Threshold for Certain PI Processors

According to Article 28 of the Regulations, a network data processor handling PI of more than 10 million individuals (raised from the prior 1 million threshold) must comply with certain requirements for processors

[1] A recent decision by the Guangzhou Internet Court of China (Case No.: (2022) Yue 0192 Min Chu No. 6486) sheds light on the judicial perspective regarding cross-border PI transfer for multinational companies. The court highlighted the importance of clear and comprehensive notifications to data subjects and proper separate informed consent, especially for cross-border data transfers where consent is the chosen legal basis for allowing the cross-border data transfer. In particular, the court held that the plaintiff's (a hotel guest) agreement to the defendant hotel group's over-20,000-word privacy policy by checking the box is not a valid separate consent for the defendant to transfer his PI cross-border. The defendant should have sent a separate notice with overseas recipient(s) and processing information as required by Article 39 of the PIPL, and obtain customer consent.

handling Important Data, which reduces the compliance burden of businesses and narrows the scope of entities subject to stricter data protection rules concerning Important Data.

Data processors handling over 10 million individuals' PI are still required to establish a dedicated data security management department and appoint a data protection officer responsible for data security. Additionally, the company must also submit a data disposal plan to regulators to safeguard Important Data in the event of a merger, acquisition, spin-off or insolvency affecting data security.

5. CROSS-BORDER DATA TRANSFER

The Regulations streamline cross-border data transfer under the CAC's existing framework which includes the "Provisions on Facilitating and Regulating Cross-Border Data Flow" (《促进和规范数据跨境流动规定》) (the "**CBDF Provisions**") released in May 2024[2], as well as the "Measures for Data Export Security Assessment" (《数据出境安全评估办法》) and the Standard Contract Measures for Outbound Transfer of Personal Information (《个人信息出境标准合同办法》). It also reiterates that once data export security assessment is obtained for proposed export of PI or important data, the data processor must comply with the "purposes, methods, scope, types and scale" as identified in the assessment.

The Regulations introduce easing measures in addition to the measures provided by the CBDT Provisions. They expand the permissible data export scenarios to now include:

a. Passing the security assessment conducted by the CAC;

b. Obtaining certification by a professional organization for PI protection in accordance with the regulations of the CAC;

c. Filing the standard contract of cross-border transfer of PI;

d. The need to provide PI overseas for the purpose of concluding and fulfilling a contract where the individual is a party;

e. Implementing cross-border human resources management in accordance with established labor rules and collective contracts signed in accordance with applicable laws, and there is a genuine need to provide employees' PI to an overseas entity;

f. The need to fulfill legal duties and/or obligations by providing PI overseas (newly established rule under China's data export compliance regime);

g. The need to protect the life, health and property safety of natural persons in case of emergency by providing PI overseas; and

h. Others as required by laws, regulations or the CAC.

[2] See our previous article at: https://www.haynesboone.com/news/alerts/china-releases-new-rules-to-ease-burden-on-cross-border-transfer-of-data

The introduction of "necessity to fulfill legal duties" as a permissible data export scenario is new to the Regulations. While its interpretation remains to be seen in practice, it is expected that pharmaceutical and biotech companies may benefit from such relaxation when transferring pharmacovigilance data out of China to meet the mandatory requirements under industry regulations.

It is also worth noting that Article 26 of the Regulations reiterates that foreign data processors who directly process PI of individuals in China for the purpose of either (i) providing products and services to individuals in China or (ii) analyzing and assessing the behavior of individuals in China, shall establish a dedicated body or designate a representative in China, and such name and contact information of the body or representative should be reported to the local CAC where the agency or representative is located.

6. SPECIFIC OBLIGATIONS FOR COMPANIES IN CERTAIN INDUSTRIES

a. AI Industry

Currently, automated collection techniques – such as crawling and robotic process automation – are regulated from the perspective of the PRC Anti-Unfair Competition Law. The Regulations specifically require that when using automated tools to access and collect network data, businesses should assess the impact on the data service and not infringe upon other's networks or interfere with the normal network service operation. Article 24 of the Regulations further clarifies the requirements for handling PI through automated collection techniques, that companies should delete or anonymize the PI if automated collection techniques are used to obtain relevant training data.

Article 19 of the Regulations also stipulates that companies providing generative artificial intelligence services shall strengthen the security management of training data and related processing activities, as well as take effective measures to prevent and address network data security risks.

b. Online Platforms

The Regulations impose certain safety oversight and management obligations on network platform services providers. A "large network platform" is defined as a network platform with over 50 million registered users or over 10 million monthly active users, which handles complex transactions and with data processing activities that may have significant impacts on China's national security, economic operations and livelihood[3]. According to the Regulations, providers of large network platform services may not use the data, algorithms or their terms of use to block the access or use of data by users or abuse their position to discriminate against users. They are also required to publish an annual social responsibility report on PI protection.

Notably, European Union (EU)'s Digital Markets Act contains similar designations for "gatekeepers."[4] Gatekeepers are prohibited from undertaking certain practices in respect of their core platform services. This includes dictating the price or conditions business users apply to the same products or services they offer via their platform. Gatekeepers are also prohibited from restricting end users' use of business users' software made available via their platform. Other prohibitions include provisions on using users' PI for targeted advertising or on aggregating the users' data from across the different services they provide without users' consent, etc.

[3] Common examples of a "large network platform" will include WeChat, Alipay, Taobao etc.
[4] On Sept. 6, 2023, the EU designated six gatekeepers, which are: Alphabet, Amazon, Apple, ByteDance, Meta and Microsoft.

7. ENFORCEMENT AND PENALTIES

Depending on the provision violated, which generally includes violations of data security protection, national security and/or rules relating to important data, penalties can be: (i) suspension of the relevant business; (ii) revocation of a permit or business license; (iii) fines up to RMB 10 million (approx. $1.4 million) for a network data processor; and (iv) fines up to RMB 1 million (approx. $140,000) for directly responsible person(s) of the violation.

Notwithstanding, the aforementioned penalty may be reduced or exempted if: (i) the network data processor eliminates or mitigates the harmful consequences of the relevant violation; (ii) the violation is minor and is corrected in a timely manner which has not caused harmful consequences; or (3) the network data processor violates the Regulations for the first time and the harmful consequences are minor and corrected in a timely manner.

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

China Publishes the AI Security Governance Framework, November 26, 2024

China's Data as a Fifth Market Production Factor – an Asset on Your Balance Sheet, September 23, 2024

China Releases New Rules to Ease Burden on Cross-Border Transfer of Data, May 16, 2024

China Increases Filing Thresholds for Antitrust Merger Review, April 2, 2024

China Streamlines Requirements Regarding Data Export in the Greater Bay Area, February 29, 2024

China Releases Regulation on the Protection of Children in Cyberspace, December 5, 2023

China Publishes Interim Measures for the Management of Generative Artificial Intelligence Services, August 7, 2023

Mexico Nearshoring: Opportunity for Manufacturers in China and the U.S., April 5, 2023

China MIIT Releases Data Security Management Measures for Industrial and Information Technology Sectors, February 20, 2023

A New Guideline Added to China's Data Protection Framework, August 17, 2022

China Revises its Anti-Monopoly Law 14 Years After its Initial Implementation, July 26, 2022

China Releases Judicial Interpretation of Anti-Unfair Competition Law, April 28, 2022

Select Proposed Changes to the Company Law of the People's Republic of China, March 22, 2022

A Snapshot of China's Cyberspace Administration and Data Protection Framework, February 9, 2022

China Intensifies Regulations on Cryptocurrency Trading and Mining, November 2, 2021

China's Amended Administrative Penalty Law Took Effect on July 15, October 8, 2021

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 Anti Monopoly Law, November 30, 2020

China Releases Draft Personal Data Protection Law for Comments, November 12, 2020

China Adopts Export Control Law, November 5, 2020

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