Significant Changes to China's CBDT Regulatory Framework

-A Brief Analysis on CAC's new Draft Regulation

Peng Cai

On September 28, 2023, the Cyberspace Administration of China ("**CAC**") issued the Notice to Seek Public Consultation on the *Provisions on Regulating and Facilitating Cross-Border Data Flows (Draft for Public Comments)* ("**Regulations**"). We believe that the Regulations will substantially change the regulatory framework for cross-border data transfer ("**CBDT**") in China, greatly reducing uncertainty faced by multinational companies in their CBDT activities.

Specifically, compared to the *Measures on Security Assessment for Outbound Data Transfer* ("**Security Assessment Measures**") and the *Measures for the Administration of Standard Contracts for Outbound Transfer of Personal Information* ("**Standard Contract Measures**"), the Regulations significantly streamlines enterprises' cross-border compliance responsibilities. By introducing "exemptions" and refining the criteria concerned with initiating cybersecurity assessments, filing standard contracts, and applying for certifications, the Regulations aims to considerably diminish enterprises' compliance overheads, paving the way for creating a more business-friendly environment and relaxing oversight for cross-border data transfers.

In this article, we focus on why the Regulations is rolled out in such an time-efficient manner and provide a guidance for multinational companies on reshaping their compliance strategies within this new regulatory context. Our objective is to offer enterprises clear direction, enabling them to navigate cross-border data activities compliantly under this framework.

1. Background of the Regulations

Under the current CBDT regulatory system, companies not only bear heavier compliance obligations, but also struggle with the lack of clarity in the CAC's review

standards, which has made it difficult for companies to assess what types of data are allowed for cross-border transfer, leading many companies to downsize their business operations in China. The current CBDT regulatory system is likely to weaken China's competitiveness and is inconsistent with China's basic national policy of deepening reform and opening-up and attracting foreign investment.

Relevant policies and milestone events are listed blew in a chronological manner to provide some regulatory background of the Regulations.

Serial Number	Policy or Milestone Events	Date	Content
1.	Opinion on Better Utilizing Data as an Essential Factor	December 2, 2022	Put in place mechanisms to ensure secure, compliant, and orderly flow of data across borders.
2.	President Xi Jinping's keynote speech at the Central Economic Work Conference	December 15, 2022	Emphasize the importance of attracting and utilizing foreign capital more vigorously.
3.	Government Work Report 2023	March 13, 2023	Strengthen efforts to attract and utilize foreign capital.
4.	Central Political Bureau Meeting	April 28, 2023	Discuss and study the current economic situation and economic tasks.
5.	Central Political Bureau Meeting	July 24, 2023	Prioritize attraction of foreign investment and stress the importance of supporting qualified pilot free trade zones and free trade ports.
6.	Premier Li Qiang's speech during his inspection in Shanghai	July 26-27, 2023	Address the significant concerns surrounding cross-border data flow and management.
7.	Opinion on Further	August 13,	Explore streamlined mechanisms for

Serial Number	Policy or Milestone Events	Date	Content
	Optimizing the Foreign Investment Environment	2023	the secure management of cross-border data flows.
8.	State Council Information Office Press Conference	August 17, 2023	Wang Dongtang, Director-general of the Department of Trade in Services and Commercial Services of the Ministry of Commerce, briefs plans to release policy documents on the development of digital trade.
9.	State Council's thematic study on accelerating the development of the digital economy	August 21, 2023	Premier Li Qiang emphasizes the significance of exploring new models for cross-border data management and actively participating in international digital economy collaborations.
10.	Central Political Bureau's thematic study on active participation in WTO reforms	September 27, 2023	President Xi Jinping underscores the importance of fostering a market-oriented, legal, and internationalized business environment.

What is clear is that the Regulations was issued the day after the release of the 27th Central Political Bureau's thematic study.

2. What Changes and What Remains Consistent under the Regulations

The Regulations, the Security Assessment Measures, and the Standard Contract Measures have all been promulgated by the CAC, in case of any discrepancies between them, the Regulations, upon taking effect, shall prevail. The following is our analysis of the key points of changes in the Regulations:

a) Introduction of "exemptions". According to Article 38 of the *Personal Information Protection Law* ("**PIPL**"), enterprises engaged in cross-border transfer of personal information must initiate security assessment, file standard contracts, apply for certifications, or comply with relevant statutes, administrative guidelines, and other CAC directives. On the basis of what is required under the PIPL, the CAC established the Security Assessment Measures and the Standard Contract Measures, which delineate distinct cross-border compliance pathways tailored to enterprises based on their data quantity (for example, entities handling personal data of over 1 million individuals) and the nature of such data (such as key data). Within this framework, the Regulations creatively introduces an "exemption" mechanism, that is, enterprises fulfilling certain criteria will be spared from the procedures of security assessment declarations, standard contract filings, or certification application when partaking in cross-border data transfers:

Entities or transfers that are eligible for "exemptions" under the Regulations	1) An enterprise that transfers personal information of less than 10,000 individuals in a year.
	2) An enterprise that transfers abroad personal information collected outside of China.
	3) Data transfer that is necessary for conclusion and performance of a contract to which the individual (whose data is subject to transfer) is a party.
	4) Transferring employees' personal information abroad that is necessary for conducting human resources management under the labor rules and regulations developed in accordance with the law and collective contracts signed in accordance with the law.
	5) Transferring abroad personal information for the purpose

	of protecting the life, health and property of human beings in emergencies.
	6) Data excluded from the negative list formulated by pilot free trade zones.

b) Alterations to the applicable conditions governing the previous data export compliance mechanism.

Once the Regulations takes effect, enterprises that are not eligible for "exemptions" will no longer be required to look into whether their outbound data transfer meets the conditions provided by the Security Assessment Measures and Standard Contract Measures. Instead, such enterprises should refer to the Regulations and establish their compliance mechanism tailored to their specific business for outbound data transfers:

The conditions where an enterprise should declare a security assessment according to the Regulations:	1) when it transfers personal information of more than one million individuals; 2) when the data that is notified by relative departments and regions or is published as key data to be transferred abroad.
The conditions where an enterprise file standard contracts or apply for certifications according to the Regulations:	3) when it is expected to transfer abroad personal information of more than 10,000 and less than one million individuals.

c) Procedures that Stay Unchanged for Security Assessment, Standard Contracts, and Certifications.

The Regulations modifies the criteria for undergoing security assessments declaration, standard contracts filing, and certifications application, and incorporates an "exemption"

provision. However, the fundamental methods for such requirements remain consistent. For instance, companies, when subject to security assessment requirements under the Regulations, should diligently prepare essential documentation like declaration forms, risk self-assessment reports, and other legal papers in a manner that aligns with the stipulations in the *Security Assessment Measure* and the *Guidelines on Security Assessment Declaration of Outbound Data Transfer (First Edition)*, emphasizing on explanation of the necessity of cross-border data transfers for the business scenarios and fields.

3. Compliance Obligations under the Regulations

The Regulations is currently under public consultation. The finalized version of the Regulations could significantly influence the strategies enterprises may adopt for cross-border data transfer compliance. With the present version of the Regulations as guidance, we offer the subsequent recommendations for enterprises' consideration.

a) Refrain from Using the Current Version of the Regulations as a Ground for "Exemption" during Current Outbound Data Transfer.

The Regulations is under public consultation and is not legally enforceable. The finalized version may make adjustments to certain provisions. Hence, businesses should not rely solely on the current version of the Regulations for outbound data transfers. We advise companies to await the official version, examine it thoroughly, and then determine the appropriate avenues for legally compliant cross-border data transfers. Specifically, companies that have obtained partial approvals for security assessments from the CAC should exercise caution. The CAC has flagged data fields or business scenarios that failed the security assessment but might be exempted under the Regulations. We suggest companies involved in such data fields or business scenarios sit tight and await the finalized version of the Regulations. Should the finalized version offer specific exemptions or other stipulations, companies can then devise their cross-border data transfer compliance strategies accordingly for these data fields or business scenarios.

b) Pay Close Attention to Other Compliance Mandates and Maintain Records.

The Regulations relaxes compliance requirements for cross-border data transfers under certain scenarios. However, enterprises must still obey prevailing laws, administrative regulations, and fulfill their data security obligations, including but not limited to:

(1) Notification Obligation. Per Article 39 of the PIPL, businesses that transfer personal information abroad must inform the concerned individuals of the overseas recipients' details, purposes and methods of data processing, types of data collected, and how individuals can exercise their rights against such recipients. Regardless of any change to legal basis or compliance mechanism, these requirements shall be met.

(2) Personal Information Protection Impact Assessment ("PIA"). Under Article 55 of the PIPL, any entity transferring personal information abroad should first conduct a PIA to analyze the legality, legitimacy, necessity, and potential risks of the transfer, the efficacy of protection measures, and other vital issues. Both the PIA reports and processing logs must be preserved for a minimum of three years.

(3) Ensuring Foreign Recipients Meet PIPL Standards. Article 38 of the PIPL mandates that entities shall ensure the data processing activities of foreign recipients align with the standards stipulated by the PIPL. We advocate that businesses contemplating cross-border transfers formalize agreements with foreign recipients to require the recipients to comply with Chinese laws during their processing activities and monitor their compliance.

(4) Establishing a Data Security Response Mechanism. Articles 9 and 10 of the Regulations underscore data security risk management. Multinational companies should especially institute effective global data security emergency response mechanisms, given their geographically dispersed data processing operations. We urge businesses to craft localized measures responsive to Chinese regulatory mandates for continuous internal oversight and risk mitigation. Special attention should be given to compliance training, emergency response traceability, and prompt risk assessments in case of security incidents. Moreover, it's prudent to report any data security event or detected heightened risk to the CAC.

c) Confirm the Scope of Key Data in Advance.

According to the Regulations, enterprises must declare a security assessment for transfer of what is officially designated by relevant governmental departments or regional governments as "key data". While this provision might aid businesses in discerning what falls under the definition of "key data", it doesn't absolve them from their compliance responsibilities. Given that various industry authorities are working on how to define and categorize key data, and no definition or catalog of key data has been revealed so far, it's prudent for enterprises to proactively engage with relevant authorities to ascertain the classification of their data. It is not advisable to act based on the assumption that there will be no official catalog of key data.

d) Process and Transfer Sensitive Information Concerning the CPC, Chinese Government, or Military Entities.

The Regulations indicates that transferring abroad sensitive information related to the CPC, Chinese government, military, or classified entities shall be in compliance with pertinent laws, administrative rules, and departmental directives. Given the highly sensitive nature of such data, potential leaks could jeopardize national security. We recommend businesses rigorously assess such data, even if it's not categorized as "key data" or doesn't fall under other categories that are subject to assessment or contractual requirements. A stringent evaluation is essential before cross-border transfers of such data.

4. Conclusions

The introduction of the Regulations underscores China's determination to refine data governance while championing the seamless flow of data to bolster economic progression. Against the backdrop of further opening-up and enhanced efforts in attracting foreign investment, effective and secure cross-border data transfers emerge as pivotal economic catalysts.

To sum up, the Regulations not only gives a clear signal that the cross-border flow of data should not be a heavy burden on businesses operating in China, but also offers a more relaxed framework for cross-border data compliance than the GDPR does. It is foreseeable that with the enactment of the Regulations, "ex post facto supervision" will be the new regulatory model for cross-border data governance in China for a long time

to come.