PAUL HASTINGS

Stay Current

July 2022

Follow @Paul_Hastings

China Enhances Scrutiny for Cross-Border Data Transfer that would Impact Multinational Companies

By Phoebe Yan, Fengzhen Yu, Shaun Wu, Sarah Zhu, John Tso & Zoey Xie

I. Introduction

China's cross-border data transfer rules are unfolding in real time and taking clearer shape. On July 7, 2022, China's cybersecurity regulatory agency, the Cyberspace Administration of China ("CAC"), issued the long-awaited *Cross-Border Data Transfer Security Assessment Measures* ("CBDT Security Assessment Measures"), which will be effective September 1, 2022, with a six-month grace period for companies to take remedial actions thereafter. The CBDT Security Assessment Measures, along with the regulations and guidelines regarding third-party certification (the Chinese equivalent of GDPR's *Binding Corporate Rules*)[1] and the *Draft Standard Contract Clauses* ("Draft SCCs", the Chinese equivalent of GDPR's *Standard Contract Clauses*) issued last month,[2] provides more detailed guidance of cross-border data transfer rules (for purposes of this article, "CBDT rules") set forth in high-level China data protection laws – see our earlier client alerts about new Chinese Data Security Law ("DSL", an enhanced version of the 2017 Cybersecurity Law) and Personal Information Protection Law ("PIPL", the Chinese equivalent of GDPR).

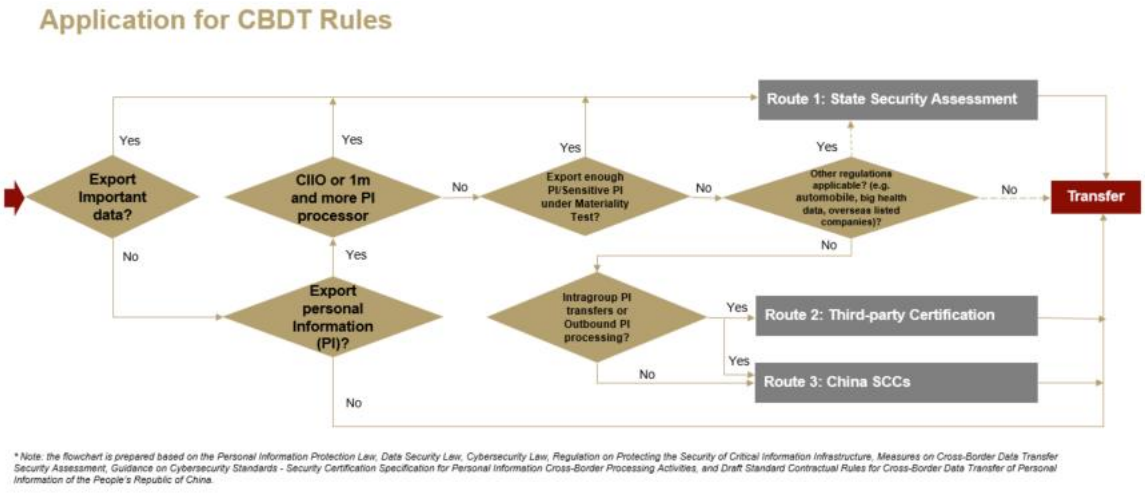
In light of the new CBDT rules in China, multinational companies dealing with very sensitive data or voluminous personal information originating from China will have to act quickly to map their data and devise a long-term plan that not only complies with the Chinese rules, but also takes into account potential conflicts of law risks. Certain previous good practices such as focusing heavily on limiting export but lightly on the accessing and retrieving of data from outside of China will also need to be reconsidered due to the new CBDT Security Assessment Measures.

This article analyzes how the CBDT Security Assessment Measures will work in relation with the other CBDT rules, and provides some timely considerations to questions concerning multinational companies based on knowns and unknowns of the new regulation.

II. Overview of the New CBDT Rules

Practical Steps for Complying with China's new CBDT Rules

CBDT Security Assessment Measures, Draft SCCs and Certification Specification provide a clear indication of the elevated expectation facing data export. Under this current regulatory framework, there are at least three routes for transfers of important data and personal information from China to overseas: 1) a security assessment conducted by the government ("State Security Assessment"); 2) a third-party certification by a professional institution; or 3) a Chinese standard contract ("China SCCs") between data importers and exporters.



1. State Security Assessment

CBDT Security Assessment Measures provide that a state security assessment should be performed by CAC and local agencies if the data processors:[3]

1. Provide important data[4] outside the country;
2. Constitute Critical Information Infrastructure Operators ("CIIO")[5] and data processors that handle personal information of one million and more individuals that provide personal information overseas;
3. Export personal information of an accumulative of 100,000 individuals since January 1 of the previous year, or export sensitive personal information of an accumulative of 10,000 individuals since January 1 of the previous year (the "Materiality Test"); OR
4. Meet other circumstances specified by state cybersecurity authorities.

Before applying for the state security assessment, data exporters are required to conduct a self-assessment and submit the self-assessment report to CAC and local agencies. The self-assessment focuses on the following aspects of a cross-border data transfer:

- Legality, legitimacy, and necessity;
- The impact on national security, public interests, individual/organization's interests;
- The overseas recipient's protection levels and security measures;
- Data loss risks and incident response plan;
- Contracts or other legal documents for data protection between data exporters and recipients; and
- Other relevant matters.[6]

The State Security Assessment will be valid for a period of two years from the date that the assessment results are issued, and the data exporters must apply for another assessment 60 working days before the expiration.

CBDT Security Assessment Measures do not specify the penalties for failure to perform a security assessment, but refer to the penalties under DSL, PIPL, Cybersecurity Law, and Criminal Law for implications.[7] Some of the penalties under these superior laws would require a plus factor (such as an actual data breach or damage) to trigger civil, administrative, and/or criminal liabilities; but there are also penalties attached to general violations of a processor's data or personal information protection obligations. For instance, Article 66 of PIPL provides severe administrative penalties (such as a fine up to either RMB50,000,000 or 5% of the turnover for previous year, suspension of businesses, and revocation of business license or business approval) and even personal liabilities for the person(s) in charge (such as a fine up to RMB1,000,000 and prohibition of holding the positions of director, supervisor, senior manager or the person in charge of the personal information protection).[8]

2. Third-Party Certification

As provided by PIPL, for cross-border data transfers of personal information that do not meet the Materiality Test, a third-party certification is a second route for data processors. Although China has not issued an implementation regulation about this route, a non-mandatory Guidance on Cybersecurity Standards - Certification Specification, effective on June 24, 2022, can shed some light on the certification mechanism.

Under Certification Specification, the certification mechanism is only applicable to (i) cross-border data transfers that occur within a same company group (i.e., intragroup transfers), or (ii) personal information processing activities outside the territory of China if the purpose of the activities is to provide products and services to natural persons in China; analyze or evaluate behaviors of natural persons in China; or other circumstances to be specified by laws and regulations.[9]

3. China SCCs

The last route is China SCCs,[10] which is the least time-consuming route, mainly applicable to smaller-scale data processors. Unlike Standard Contract Clauses under GDPR, China SCCs would apply to all cross-border data transfers of personal information without distinguishing the roles of data exporters and data importers as "controllers" or "processors". In addition, Draft Standard Contract Rules specify that China SCCs apply to scenarios where the personal information processor is not a CIIO and does not reach or exceed the threshold under the Materiality Test.

Knowns and Unknowns Regarding CBDT Rules

Although CBDT rules are comparatively clearer than the high-level principles specified in PIPL and DSL, there are still multiple questions to be further discussed or clarified by regulators when companies implement these rules in practice. Here is a list of knowns and unknowns that we are trying to tackle while awaiting further implementation rules to clarify ambiguities:

1. Is data transfer to Hong Kong and Macau subject to regulation by CBDT Security Assessment Measures?

Although not specified in CBDT Security Assessment Measures, data transfer from Mainland China to Hong Kong and Macau are likely subject to regulation because it refers to transfers "outside of the border," which usually includes the Hong Kong and Macau Special Administrative Regions outside of mainland China's customs. Additionally, another regulation governing cybersecurity review for companies listing overseas changed the expression of application from "outside of the border" in its draft version to "outside of the country" in its final version[11], with commentaries widely understood as excluding companies listing in Hong Kong from the cybersecurity review. Accordingly, it is more likely that CBDT Security Assessment Measures apply to data transfer to Hong Kong and Macau.

2. What kind of data transfer activities are covered by CBDT Security Assessment Measures?

As confirmed in a news conference held by the State Council Internet Office after CBDT Security Assessment Measures were released, the Office said that CBDT Security Assessment Measures would regulate both active transfer and passive access or retrieval of data, i.e., (i) transfer and storage of data collected and generated in the course of an enterprise's operations within China, and (ii) storage of data collected and generated within China and access or retrieval by institutions, organizations, or individuals out of China.

3. How should an enterprise conduct an assessment to comply with requirements under different regulations and rules?

There are other regulations and rules also requiring a security assessment (often starting from a self-assessment) before CBDT Security Assessment Measures are released. For example, CAC requires Chinese network platform operators going listed overseas and holding personal information of more than 1 million users to apply for a cybersecurity review.[12] It is not yet clear how the authorities will handle potentially overlapping requests of security-related review or assessment, and how a company can best react to regulatory requests under the circumstance.

4. Are there any exceptions applicable to CBDT Rules?

A draft implementation rule issued by CAC on November 14, 2021, provides two exceptions to the three routes – specifically, a data processor is allowed to export personal information directly without going through the three routes (including state security assessment) if the processor must provide personal information abroad to enter into and/or fulfill a contract in which the data subject is a party, or must provide personal information abroad to protect the life, health and property safety of the data subject.[13] The first prong of the test could be interpreted to potentially cover employees, but CBDT Security Assessment Measures currently do not provide any exceptions for employee data on the face of the regulation.

5. How to calculate the volume of personal information under the Materiality Test?

Although CAC has not issued detailed guidance on calculating the volume of personal information, the market has interpreted that all types of individuals' personal information that is processed by the companies need to be included, including employees, customers, users, vendors, and distributors (if any). In addition, the starting point of the Materiality Test for calculating accumulative personal information or sensitive personal information should be January 1 of the previous year before applying for state security assessment.

6. How to understand the grace period of CBDT Security Assessment Measures?

CBDT Security Assessment Measures provide a six-month grace period for companies to take remedial actions for any pre-September 1, 2022, data transfer that violates CBDT Security Assessment Measures (i.e., remedial actions should be taken before March 1, 2023). However, it is not clear whether companies are required to pass a state security assessment within the grace period, or they merely need to conduct a self-assessment and apply for a state security assessment if needed within the specified timeline. CAC will probably issue detailed implementation rules to explain this.

III. Potential Challenges and the Road Ahead for Multinational Companies

How to respond to these evolving rules has become a top concern for multinational companies operating in China, especially for those whose daily operations and business mainly rely on cross-border data flows. In addition, most multinational companies establish their information infrastructure as an integrated resource and use a global database for their daily operations. Theoretically, there can be two diverged roads: One road is to localize their data involved in their

operations, products, and services in China. This approach will require the companies to re-organize their global information technology management structure and prepare a separate system specifically for China operations. The other road is to navigate the three options under CBDT rules and execute one or more depending on the companies' industry, the types, and the volume of data that was generated or processed in China. As a threshold question, multinational companies need to consider whether a state security assessment for a cross-border transfer is required, and if so, does the company want to go through such an assessment as it may increase exposure to potential unwanted access.

Certainly, the two roads are not mutually exclusive, and in practice companies will also want to balance other interests such as business priorities, compliance costs, and implementation practicalities, to name a few. To begin with, it would be high time for multinational companies to perform a data health check or data mapping project to understand the nature, volume, and stakeholders of their data processed in China in order to form a strategy (including whether to perform self-assessment and/or state security assessment), and seek advice on how to balance compliance risks for data governance in China with considerations of international compliance interests such as conflicts of law and long-term feasibility. We have helped a few companies to perform such checks and advise how to reconsider their data governance strategy and are actively collecting benchmarking practices.

✧ ✧ ✧

If you have any questions concerning these developing issues, please do not hesitate to contact any of the following Paul Hastings lawyers:

Beijing

Fengzhen Yu
86.10.8567.5358
fengzhenyu@paulhastings.com

Hong Kong

Shaun Wu
852.2867.9088
shaunwu@paulhastings.com

Sarah Zhu
852.2867.9018
sarahzhu@paulhastings.com

John Tso
852.2867.9022
johntso@paulhastings.com

Shanghai

Phoebe Yan
86.21.6103.2939
phoebeyan@paulhastings.com

Zoey Xie
86.21.6103.2701
zoeyxie@paulhastings.com

[1] On June 24, 2022, China issued a non-mandatory Guidance on Cybersecurity Standards - Security Certification Specification for Personal Information Cross-Border Processing Activities ("Certification Specification").

[2] On June 30, 2022, China issued Draft Standard Contract for Cross-Border Data Transfer of Personal Information ("Draft Standard Contract Rules") and Draft SCCs for public comments. The comment period will end on July 29, 2022.

[3] *See* Measures, Article 4.

[4] Important data is defined to be data that, once tampered with, destroyed, leaked or illegally obtained or used, may endanger national security, economic operation, social stability, public health and security, among others, according to Article 19 of the CBDT Security Assessment Measures; it is also similarly defined in other regulations such as Article 21 of the DSL and Article 73 of the Network Data Security Management Regulations (draft for comments issued November 14, 2021, not effective yet).

[5] Pursuant to Article 31 of the Cybersecurity Law and Article 2 of the Regulation on Protecting the Security of Critical Information Infrastructure, CIIO refers to operators of network facilities and information systems that may seriously endanger national security, national economy, people's livelihood, and public interest once they are damaged, lost function, or leaked data; and a list of examples was given under the laws to include energy, finance, transportation, water conservancy, healthcare, education, social security, environmental protection, cloud computing, big data, national defense science and industry, large equipment, chemical industry, food and drug, and news industries.

[6] *See* Measures, Article 5.

[7] *See* Measures, Article 18.

[8] *See* PIPL, Articles 66 and 67; DSL, Articles 45 and 46; Cybersecurity Law, Article 66.

[9] *See* PIPL, Article 3.2.

[10] *See* Draft Standard Contract Rules, Article 4.

[11] *See* Cybersecurity Review Measures (2021), Article 7.

[12] *Id.*

[13] *See* Network Data Security Management Regulations (draft for comments issued November 14, 2021, effective date TBD), Article 35.