1994-2024

FANGDA PARTNERS
方達津師事務所

China promulgated the Provisions on Promoting and Standardizing Cross-Border Data Flows

Authors:

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

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

Sherman Deng
Partner, Fangda Partners
sherman.deng@fangdalaw.com

Patrick Guo, David Ye, Kaixian Zheng, Yanbin Liu and other members in Fangda data protection practice also contributed to this article.

On March 22, 2024, the Cyberspace Administration of China (**CAC**) finally released the long-awaited *Provisions on Promoting and Standardizing Cross-Border Data Flows* (《促进和规范数据跨境流动规定》in Chinese, the "**Provisions**"). The Provisions were accompanied by revisions to the *Guideline for Cross-border Data Transfer Security Assessment* and the *Guideline for Standard Contract Filing for Cross-border Transfer of Personal Information*. The CAC also released the second version of these guidelines. This alert aims to summarize the major changes to the existing regulations on cross-border data transfer (**CBDT**) resulting from the Provisions, highlight the issues that still need clarification from regulators, and provide suggestions on how to comply with CBDT requirements under Chinese laws.

1. Relaxation and exemption to the CBDT Mechanisms

The Provisions have introduced relaxation and exemptions to the mechanisms for CBDT (i.e., security assessment for CBDT ("**Security Assessment**"), filing of standard contract for cross-border transfer of personal information ("**SCC Filing**"), and personal information protection certification ("**Certification**")), collectively referred to as "**CBDT Mechanisms**" , under the *Measures on the Security Assessment for the Cross-border Data Transfer* and the *Measures on the Standard Contract for the Cross-border Transfer of Personal Information*. The exemptions provided by the Provisions follow the same structure as the draft for comments released by the CAC on September 28, 2023 ("**Draft Provisions**"), but there are some changes in the detailed rules.

1) **Company-wide Exemption/De Minimis Exemption**: If data handlers[1] other than the Critical Infrastructure Information Operators (**CIIOs**) have collectively shared less than 100,000 individuals' personal information (excluding sensitive personal information) outside of China since January 1 of that year, they are not obligated to follow CBDT Mechanisms. Unlike the Draft Provisions, the Provisions specifically exclude CIIOs from this company-wide exemption due to their unique characteristics and the data localization and Security Assessment requirements stated in the *Cybersecurity Law and Personal Information Protection Law* (**PIPL**).

2) **Scenario-based Exemptions**: The scenario-based exemptions are largely the same as the Draft Provisions with minor adjustments.

a) Exemption for cross-border nature business scenario: Exemption for cross-border nature business scenarios includes situations where individuals need to provide personal information outside of China in order to enter into and fulfill a contract they are a party of. This includes activities such as cross-border shopping, mailing, fund transfers, payments, account opening, air ticket and hotel bookings, visa applications, and taking exams, among others. However, it is important to note that it is still unclear whether this exemption applies to B2B cross-border e-commerce, e.g., the cross-border transfer of business contact information in connection with an overseas-based CRM system.

b) Exemption for HR management necessity on employees' data: In cases where it is required to disclose employees' personal information outside of China for the purpose of managing cross-border human resources in compliance with labor laws and regulations, as well as collective contracts established by law. But this exemption does not extend to the transfer of personal information of job applicants, the reason being job applicants are not considered legally employed individuals.

c) Exemption for protection of vital interest: In situations of emergency, where it is imperative to disclose personal information outside of China to safeguard the life, health, and property of individuals.

2. Changes to the numerical thresholds for CBDT Mechanisms

The provisions have also made changes to the numerical threshold used to determine the applicable CBDT Mechanism. Additionally, the calculation period has been modified to start from January 1 of the current year. Furthermore, a numerical threshold of "10,000 sensitive personal information" has been introduced for the Security Assessment.

The amended numerical thresholds are summarized as below:

Subject Type	Number of cumulative data transferred overseas since January 1 of the current year	Applicable CBDT mechanism
CIIOs	≥ 1 individual's personal information	Security Assessment
Data handlers that are not CIIOs	> 1 million individuals' personal information (excluding sensitive personal information)	Security Assessment
	> 10,000 individuals' sensitive personal information	Security Assessment
	100,000 – 1 million individuals' personal information (excluding sensitive personal information)	Either SCC Filing or Certification
	1 – 10,000 individuals' sensitive personal information	Either SCC Filing or Certification
	<100,000 individuals' personal information without any sensitive personal information	Exempted from applying for any CBDT Mechanisms

In addition, in a media release of the official Q&A of the Provisions dated March 22, 2024 (the "**Q&A**"), the CAC has specifically clarified that in the process of calculating the number of cumulative data transferred overseas mentioned above, the corresponding amount of data transferred in exempted scenarios does not need to be taken into account.

3. Exemptions applicable to Free Trade Zone

The Provisions have adopted the exemption of Free Trade Zones (FTZs) and require them to adhere to the national framework for data categorization and classification when preparing Negative Lists for certain data fields or CBDT Mechanisms. Any CBDT that is not included in this Negative List will be exempt from CBDT Mechanisms. These Negative Lists will outline the CBDT cases that are subject to CBDT Mechanisms and must be approved by the respective provincial CAC and filed with the central CAC. The *Action Program for Solidly Promoting High-Level Opening-up to the outside World and Greater Efforts to Attract and Utilize Foreign Investments* (《扎实推进高水平对外开放更大力度吸引和利用外资行动方案》), released on March 19, 2024, also emphasizes the need to properly define important data and facilitate cross-border data flow. For instance, Tianjin FTZ has introduced a policy for data categorization and classification, while the Lin Gang area in Shanghai FTZ is piloting initiatives to promote cross-border data flow. Considering these developments, it is anticipated that the scope of important data will become clearer in 2024, and companies may benefit from future FTZ data categorization and classification rules, which will exempt general data from certain regulations.

4. Approach on the identification of important data

Article 2 of the Provisions stated that if the data processed by data handlers has not been notified or officially classified by the relevant departments or regional authorities as important data, the data handlers are not required to include the data in the Security Assessment as important data. This means that the regulator will either publish a catalog of important data or issue circulars or notices to inform specific companies and sectors about what data is considered important. Therefore, companies do not need to speculate or guess whether the data they process falls under the category of important data.

It is important to note that a national standard on data classification, *GB/T 43697-2024 Data Security Technical Data Classification and Grading Rules*, was officially released on March 15, 2024, and will come into effect on October 1, 2024. This recommended national standard not only specifies the classification of data into general data, important data, core data, and other levels based on sensitivity, importance, and potential risks, but also provides "Guidelines for Identifying Important Data" in the appendix. These guidelines are expected to offer valuable assistance to companies in identifying and safeguarding important data, taking into account the specific rules of different regions, industries, and fields.

5. Changes to the effective term of Security Assessment approvals

The Provisions offer a three-year effective term for Security Assessment approvals, alleviating the need for companies to undergo frequent assessments. It allows for a three-year extension of the approval if the CBDT needs to continue and no circumstances requiring re-submission for security assessment have arisen.

6. Emphasis on the separate consent requirement

In contrast to the Draft Provisions, which acknowledge that the CBDT could be based on consent or other lawful bases, the Provisions removed this qualifier and placed specific emphasis on obtaining separate consent in accordance with laws and regulations. However, the second version of the *Guideline for Cross-border Data Transfer Security Assessment* clarifies that if the CBDT falls within sub-paragraph 2-7 of paragraph 1, Article 13 of the PIPL (i.e., alternative lawful bases for processing personal information other than consent, such as contractual necessity, etc.), no consent is required. It is important to note that in practice, local CAC tends to prioritize proof of separate consent and may not engage in legal arguments regarding alternative lawful bases for processing in general.

7. Questions that require further clarification from authorities

1) **Regarding the thresholds and volume calculation**, it is important to clarify whether the number of "personal information cumulatively provided outside of China since January 1 of the current year" includes personal information that was already transferred before this year. If the Provisions state that only the increment should be counted, without considering the historic number of personal information transfers, such as the number of new job applicants or new customers since January 1 of this year, then more companies will be relieved from the requirement of SCC filing or Security Assessment. It is crucial for companies to monitor this aspect and observe the practices of the local CAC after the implementation of the Provisions.

2) **What is the relationship between the previously approved Security Assessment/SCC Filing and the Provisions?** If a company received conditional approval before the Provisions were issued, with certain data fields prohibited from transfer, will those rejected data categories be allowed if they also fall under a scenario-based exemption like cross-border HR management? In the Q&A, CAC mentioned that the data handler could consider SCC Filing or Certification but didn't expressly state that they are outright exempted. On a related note, for previously approved CBDT activities, they will remain valid. For CBDT applications in the pipelines, the data handlers can continue with the application or withdraw the application and re-submit under a different CBDT Mechanism.

3) **Applicability of special policies for Free Trade Zone (FTZs)**. According to the Provisions, data handlers in the FTZs can be exempted from CBDT Mechanisms if they transfer data that is not on the Negative List. However, it is unclear whether only companies registered in FTZs will be eligible for this relaxation. There is a possibility that the FTZs relaxation could be extended to companies outside the FTZs if there is a connection to such FTZs, such as using third-party data centers within the FTZ. However, any regulatory attempt and breakthrough in this regard would require consideration and approval from the central CAC.

8. Recommended compliance measures

In view of the Provisions, we would suggest that MNCs in China implement the following compliance measures:

1) **Establishing a long-standing mechanism to calculate the number of data transferred:** Companies that transfer personal information outside of China should establish a consistent mechanism to calculate the amount of data being transferred. This mechanism should include monitoring the CBDT and conducting regular data mapping to ensure that the number of individuals whose personal information is involved in the CBDT is accurately recorded. This should include both the "incremental" and "historical" volumes of personal information, as the volume of data is crucial in determining the exemptions that may apply. Companies should also document this process to comply with future personal information protection compliance audits and verification of the applicable CBDT Mechanism.

2) **Updating the submission materials based on the applicable CBDT Mechanism:** When companies are allowed to switch from one CBDT Mechanism to another in accordance with the Provisions, such as changing from the Security Assessment to the SCC Filing, they must update all submission materials according to the Provisions and the guidelines for the applicable CBDT Mechanism. This includes removing any exempted scenarios and revising the self-assessment report or DPIA report using the new template provided in the second version of the *Guideline for Cross-border Data Transfer Security Assessment* or the *Guideline for Standard Contract Filing for Cross-border Transfer of Personal Information*. Only after making these updates should the materials be submitted to the CAC.

3) **Keeping internal compliance records:** Companies that are exempted from the requirement to complete the CBDT Mechanism are still obligated to fulfill certain requirements under the PIPL. This includes notifying individuals, obtaining separate consent (if required), conducting DPIA, and more. These companies should implement the necessary obligations and maintain appropriate records to comply with future personal information protection compliance audits related to CBDT compliance.

Furthermore, the Provisions appear to have alleviated the obligation to sign the China SCC and file it with the relevant authorities. However, it remains uncertain whether the signing of the China SCC and adequate compliance documentation to meet the DPIA requirement under Article 59 of the PIPL will be a focal point of inspection or audit during subsequent regulatory inquiries or audits conducted by the CAC. It is advisable to establish an intra-group data transfer agreement and include the China SCC as an appendix, signing it when requested by regulators.

[1] The concept of data handler under Chinese law is similar to data controller in the GDPR context.

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

66/F, Guangzhou CTF
Finance Centre
6 Zhujiang East 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

Nanjing

38/F, Asia Pacific Business Building
2 Hanzhong Road
Gulou District
Nanjing 210005, China

Tel: +86 25 8690 9999
Fax:+86 25 8690 9099

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

9/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