Client Alert

March 2024

New Rules to Facilitate and Standardize Cross-Border Transfer of Data Outside China

Contents

On March 22, 2024, the Cyberspace Administration of China ("**CAC**") issued the long-waited **Provisions on Facilitating and Standardizing Cross-Border Data Flow** (the "**New CBDT Rules**"), which took effect from the same date.

As background, CAC released the draft **Provisions on Standardizing and Facilitating Cross-Border Data Flow** on September 28, 2023 for solicitation of public comments. Those draft rules were aimed at responding to the concerns and complaints raised by many companies operating in China (especially those foreign-invested ones) about the sweeping and onerous obligations imposed by CAC on their outbound data provision/cross-border data transfer ("**CBDT**") and the lengthy and opaque administrative formalities and processes for CDBT security assessment applications. The draft rules were expected to be and were actually finalized by CAC before the end of November 2023. However, presumably due to the controversies around policy orientation towards regulation and relaxation of CBDT activities, the finalized rules (i.e., the New CBDT Rules) were not published until very recently. With the New CBDT Rules being promulgated, the Chinese government finally released positive signals with moderate relaxation of its stringent control over CBDT activities since the promulgation of the **Personal Information Protection Law of the PRC** (the "**PIPL**") in 2021, and the implementation of CBDT security assessment and China Standard Contract for Cross-Border Transfer of Personal Information starting from late 2022.

We set out below a few highlights of the New CBDT Rules and certain changes brought by the New CBDT Rules and the implementation guidelines thereof concurrently released by CAC.

1. Specified what data is regulated under the CBDT control regime.

The New CBDT Rules and CAC's relevant official responses to the press reiterate that the requirements for the security administration of CBDT activities only apply to two categories of data: (a) personal information and (b) important data. Export of any data other than such two categories of data in the course of various cross-border activities would not be subject to any of the following requirements of CBDT formality (the "**Formality Requirements**"):

i. application for a CBDT security assessment ("**Security Assessment**");

ii. conclusion and filing of a standard contract for personal information export ("**China SCCs Filing**"); or

iii. application for a personal information protection certification ("**Certification**").[1]

The uncertainty around the exact scope of "important data" has been puzzling companies operating in China for a long time. The good news brought by the New CBDT Rules is that unless certain data (a) has been clearly identified by competent governmental

[1] Details of the Formality Requirements are stipulated in CAC's prior rules. We will not elaborate those details in this article.

authorities as important data, or (b) falls into any published catalogues of important data,[2] a data processor[3] may treat its data as non-important data.

2. Specified certain scenarios where the Formality Requirements can be exempted.

Firstly, in terms of export of important data, no exemptions would apply. Each data processor in China must pass the Security Assessment and obtain clearance from both of the provincial and central offices of CAC, as long as any important data needs to be exported.

Secondly, in terms of export of personal information, a personal information processor ("**PIP**") in China would be exempted from any of the Formality Requirements in any of the following scenarios (the "**Exempted Scenarios**"):

i. **Exemption for Data-in-transit**: the personal information exported is limited to personal information collected and generated outside China and transmitted into China for domestic processing, during which no personal information or important data collected or generated within China is incorporated into the personal information exported (i.e., pure storage of overseas personal information in China or transit of overseas personal information through China);

ii. **Contracting Exemption**: the data processor exports personal information where it is necessary to do so for the purpose of concluding or performing a contract to which the individual is a party, such as for cross-border shopping, cross-border posting and delivery, cross-border fund remittance, cross-border payment, cross-border account opening, air ticket ad hotel booking, visa application, examination services, etc.;

iii. **HR Management Exemption**: the data processor exports employees' personal information where it is necessary to do so for the purpose of implementing cross-border human resources management in accordance with labor rules and policies formulated in accordance with laws and collective contracts concluded in accordance with laws;

iv. **Emergency Exemption**: the data processor exports personal information where it is necessary to do so for the purpose of protecting life, health and property safety of individuals under emergency conditions; and

v. **Small-scale Data Exporter Exemption**: the data processor is not a critical information infrastructure operator ("**CIIO**") and it has exported non-sensitive personal information of less than 100,000 individuals since January 1 of the current year.

In terms of whether a data processor is a CIIO (which is subject to more stringent requirements such as localization of personal information and important data and the Security Assessment requirement for its CBDT activities), to avoid uncertainties, CAC clarified that a CIIO will be notified by competent governmental authorities of its status of CIIO. That means if a data processor has not received a clear and formal notification on its status of CIIO, it can assume that it is not a CIIO.

Data processors in China should carry out a prudent assessment (including a sensitivity check of each data field of the exported personal information and an export necessity test) to determine whether they can be eligible for those Exempted Scenarios and whether the Formality Requirements would be not applicable to them.

For example,

- regarding the Contracting Exemption, data processors should consider their business models (whether "to B" or "to C"); if they operate both business models and if such Exempted Scenario applies, the "to C" part may be carved out for the purpose of calculating the number of China data subjects whose personal information is exported;
- regarding the HR Management Exemption (which may be relevant to most foreign-invested enterprises in China), it remains to be tested whether in practice CAC would take a literal approach in applying such Exempted Scenario or would otherwise interpret and apply this Exempted Scenario in a much narrower manner (as CAC has been doing in the past months in respect of the transfer of China employees' personal information by quite a number of multinational

[2] Currently, only a small number of central ministries/regulators have issued their lists of important data applicable to specific types of companies under their regulation, and other central ministries and regulators are yet to formulate their respective catalogues of important data. That being said, Appendix G "Guides for Identification of Important Data" of "**Data Security Technology – Rules for Data Classification and Grading**", a recommended national standard issued by T260 on March 21, 2024 will be the primary guides for the central ministries and regulators as well as companies to assess and identify the likely scope of important data in their respective industries, sectors and/or businesses.

[3] Under the PIPL, the Cybersecurity Law of the PRC and the Data Security Law of the PRC, a data processor (or sometimes translated as "data handler") is akin to a data controller commonly known in the data privacy laws in many jurisdictions.

companies in their Security Assessment applications); hence, before CAC provides more clarifications on this, data processors should carefully consider whether export of their employees' personal information (including each relevant data field) is truly needed or necessary for cross-border or global/centralized human resources management and whether their employment policies or collective contracts (if any) have been formulated/concluded in accordance with the China employment laws and have incorporated sufficient wording to justify the application of such Exempted Scenario.

3. Empowered authorities in various free trade zones in China to publish negative lists to further ease CBDT activities

Under the New CBDT Rules, authorities in various free trade zones in China have been empowered to issue their respective negative lists to further ease CBDT activities within the national framework of data classification and grading, to the effect that for those data processors located in the free trade zones, only those CBDT activities that fall into the negative lists would be subject to the applicable Formality Requirements. Local authorities in those free trade zones must obtain clearance from competent authorities at both provincial and central levels before the negative lists formulated by them can be released to the public for implementation. For the time being, authorities in free trade zones in Lingang, Shanghai, and Tianjin are reported to be in the process of negative lists formulation and their negative lists are expected to be made available to the public in the near future.

4. Substantially raised the thresholds of the Formality Requirements

Under the New CBDT Rules, CAC has substantially raised the thresholds of (i) the Security Assessment and (ii) the China SCCs Filing or the Certification, respectively. Those changes will result in the exemption for more data processors from the Security Assessment requirement or even from all Formality Requirements. The detailed thresholds under the New CBDT Rules are set out in the matrix at the end of the appendix of this article.

Meanwhile, CAC has provided some guidance (which is far from crystal clear) how to calculate the number of individuals for the purpose of determining the applicability of the Formality Requirements, which is summarized below:

- First, the counting period commences from January 1 of a the most current year, until the date of the submission of the Security Assessment application. If the Security Assessment is not triggered and applicable, we believe that the ending date could be the date of the submission of the Contracting Filing or the Certification application.
- Second, a single individual should not be counted twice (i.e., data processors should deduplicate the individuals whose personal information is exported).
- Third, individuals whose personal information is exported under those Exempted Scenarios (except for the Small-scale Data Exporter Exemption where the number of individuals is the decisive factor) can be carved out.

5. Other highlights

   i. Under the New CBDT Rules, the validity period of a Security Assessment has been extended from 2 years to 3 years, commencing from the date when the data processor receives CAC's final clearance of the Security Assessment. Upon application and on the conditions that no circumstance triggering a new Security Assessment has arisen, the validity period can be extended for additional 3 years.

   ii. In the updated implementation guidelines for the Security Assessment and the China SCCs Filing released by CAC concurrently with the New CBDT Rules, CAC has amended and clarified the requirements for certain application materials, and to some extent lowered the granularity requirements for relevant risk/impact assessment reports that are required to be submitted.

   iii. Interestingly, the updated implementation guidelines mentioned above also specify that overseas personal information processing activities that are governed by the extra-territorial application provision under the PIPL (i.e., Article 3 Paragraph 2 of the PIPL) should constitute CBDT activities. It seems to imply that overseas data processors, when collecting and processing personal information of individuals located in China for certain purposes prescribed by the PIPL (without involving data exporters located in China), may also be obliged to fulfil the applicable Formality Requirements. However, how the Formality Requirements may apply to those overseas PIPs is subject to CAC's further clarification.

   iv. CAC clarified that those data processors that have already submitted Security Assessment or China SCCs Filing applications before the issuance of the New CBDT Rules may continue the processes, or withdraw their applications, if they are now exempted from complying with the relevant Formality Requirements under the New CBDT Rules.

v. Regardless of the applicability of the Formality Requirements or the Exempted Scenarios, each data processor is still obliged to perform the statutory obligations when processing data in China and conducting CBDT activities. In other words, even if a data exporter is eligible to be exempted from the Formality Requirements, it still needs to notify the individuals of its collection and processing of their personal information, obtaining separate consent for CBDT (if applicable) and conducting and preparing personal information protection impact assessment ("PIPIA").

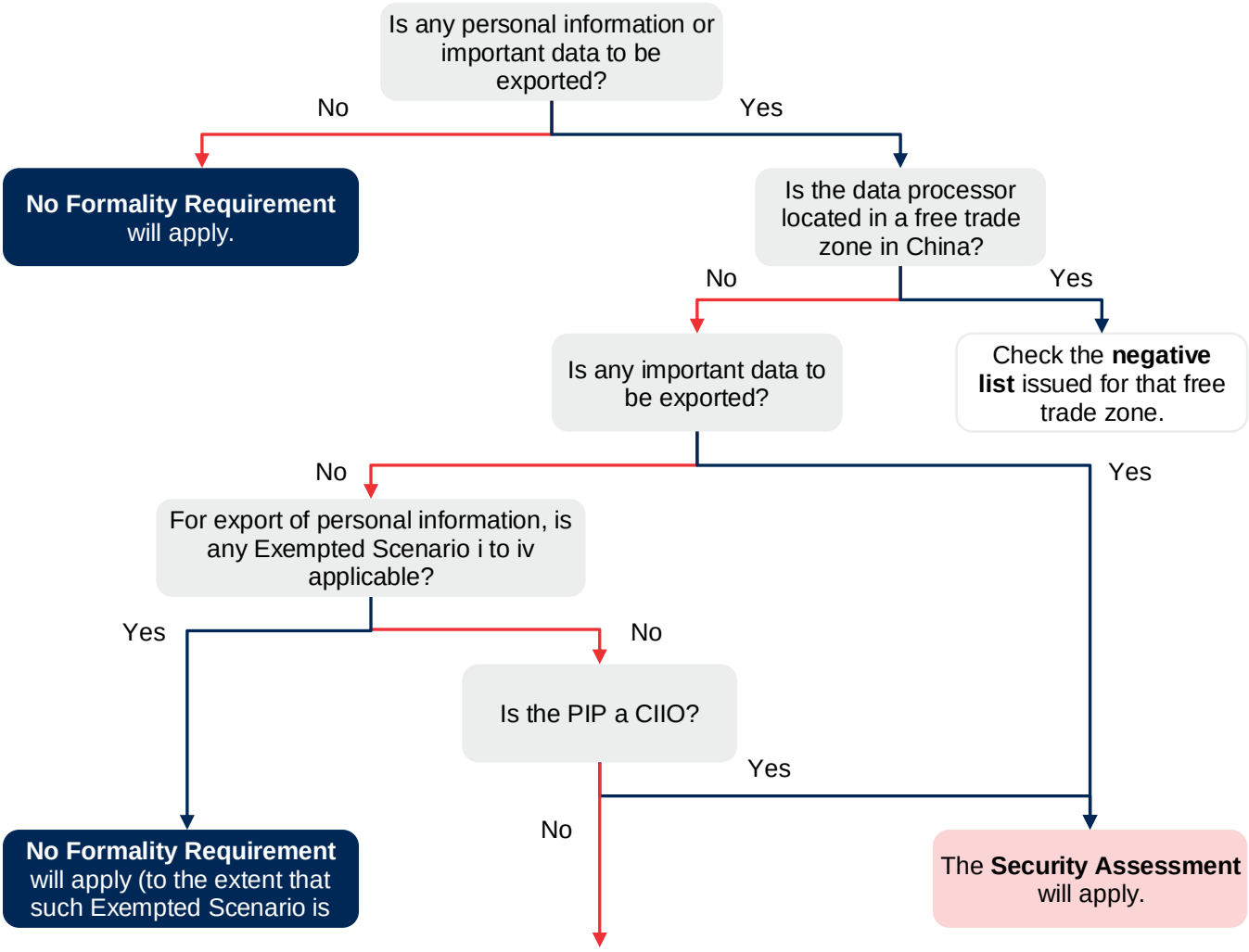
6. Recommendations

The New CBDT Rules have brought rather important changes to the CBDT control regime in China, which would be highly relevant to most foreign-invested data processors in China.

Those data processors who have not taken any actions to assess and fulfil the Formality Requirements should (a) conduct necessary internal checks on their CBDT activities to determine whether they should comply with any Formality Requirements under the New CBDT Rules and (b) conduct review and checks on their compliance with the statutory requirements concerning data processing and CBDT activities and prepare the relevant PIPIA reports even if they conclude that they are eligible for the Exempted Scenarios. As and when the rules proposed by CAC on audit of compliance with the PIPL are finalized and implemented, such review and checks as well as the PIPIA reports would be supporting evidence for those data processors that conclude they are exempted from the Formality Requirements.

Those data processors who have already initiated the relevant CBDT formality but have not yet completed the applicable Formality Requirements should now re-assess the applicability of such Formality Requirements and, if any of the Formality Requirements is still applicable, update the corresponding application documents required for the applicable Formality Requirements according to the New CBDT Rules and the updated implementation guidelines issued by CAC.

Appendix: Steps to Determine the Applicable Formality Requirement for CBDT Activities



Please refer to the matrix below to determine the applicable Formality Requirement.

Number of individuals[4]		Individuals whose **personal information (whether sensitive or not)** is exported		
		1 – 99,999	**100,000 – 999,999**	**1,000,000+**
Individuals whose **sensitive personal information** is exported	0	N/A	China SCCs Filing or Certification	Security Assessment
	1 – 9,999	China SCCs Filing or Certification	China SCCs Filing or Certification	Security Assessment
	10,000+	Security Assessment	Security Assessment	Security Assessment

[4] See CAC's calculation guidance in Section 4 of this article.

Contact Us

Zhenyu Ruan
Partner
zhenyu.ruan
@bakermckenziefenxun.com

Chris Jiang
Counsel
chris.jiang
@bakermckenziefenxun.com

Xi Chen
Associate
xi.chen
@bakermckenziefenxun.com

Michael Wang
Associate
michael.wang
@bakermckenziefenxun.com