LINKS Law Offices
通力律师事务所

China Releases New Rules on Cross-Border Data Flows

By Sue Sun | Jill Lu

On 22 March 2024, nearly half a year following the release of the *Provisions on Regulating and Promoting Cross-Border Data Flows (Consultation Paper)* ("**Consultation Paper**"), the Cyberspace Administration of China ("**CAC**") officially promulgated the *Provisions on Promoting and Regulating Cross-Border Data Flows* ("**Provisions on Cross-Border Data Flows**"), which became effective immediately upon publication. The Provisions on Cross-Border Data Flows not only uphold the ideas and principles set out in the Consultation Paper and ease the compliance burdens for data handlers by narrowing the circumstances in which the CAC data export security assessment ("**Security Assessment**"), standard contract ("**SCCs**") filing or personal information protection certification ("**PI Certification**") are mandatory, but also further clarify the thresholds for triggering these procedures.

Concurrently with the release of the Provisions on Cross-Border Data Flows, the CAC issued the *Guidelines for Security Assessment Application for Cross-Border Data Transfer (Second Edition)* and the *Guidelines for SCCs Filing for Cross-Border Personal Information Transfer (Second Edition)* (hereinafter collectively referred to as the "**Second Edition Guidelines**"). These guidelines streamline the application materials and introduce an online submission system, thus facilitating data handlers' application for Security Assessment and SCCs filing.

This article aims to provide a concise analysis of the impact of the Provisions on Cross-Border Data Flows and the Second Edition Guidelines on the data compliance strategies of global asset managers.

1. Cross-Border Transfer of Personal Information

The first paragraph of Article 38 of the *PRC Personal Information Protection Law* ("**PIPL**") provides three routes for outbound transfers of personal information, i.e. (1) passing the Security Assessment; (2) entering into the SCCs with the overseas recipient; (3) passing the PI Certification by a professional institution. Based on the Consultation Paper, the Provisions on Cross-Border Data Flows further refine the circumstances under which exemptions from these three routes can be granted. Specifically:

No.	Circumstances	Applying for Security Assessment	Entering Into the SCCs With the Overseas Recipient *or* Passing the PI Certification
1.	Outbound transfers of personal information originally collected and generated overseas and then imported into the PRC for further processing, during which no domestic individuals' personal information is involved	×	×

2.	Outbound transfers of personal information are necessary for concluding and performing a contract to which the individual concerned is a party (such as cross-border deliveries, cross-border remittances, cross-border payments, cross-border account opening, air ticket and hotel reservations, visa processing, examination services, etc.)	×	×
3.	Outbound transfers of employees' personal information are necessary for cross-border human resources management in accordance with lawfully adopted employment policies or lawfully executed collective contracts	×	×
4.	Outbound transfers of personal information are necessary to protect the health and property safety of an individual in an emergency	×	×
5.	For a data handler that is not a critical information infrastructure operator ("**CIIO**"), outbound transfers of personal information (excluding sensitive personal information) of **fewer than 100,000 individuals** since 1 January of the current year	×	×
6.	For a non-CIIO data handler, outbound transfers of personal information (excluding sensitive personal information) of **more than 100,000 individuals but fewer than one million individuals** since 1 January of the current year	×	√
7.	For a non-CIIO data handler, outbound transfers of personal information (excluding sensitive personal information) of **more than one million individuals** since 1 January of the current year	√	×
8.	For a non-CIIO data handler, outbound transfers of sensitive personal information of **fewer than 10,000 individuals** since 1 January of the current year	×	√
9.	For a non-CIIO data handler, outbound transfers of sensitive personal information of **more than 10,000 individuals** since 1 January of the current year	√	×
10.	A CIIO providing personal information abroad, regardless of the sensitivity of the personal information	√	×

We understand that there are a number of issues that global asset managers need to be aware of when implementing the personal information protection measures in accordance with the Provisions on Cross-Border Data Flows:

(1) In determining whether it falls under items 5 to 10 above, the number of individuals involved in the outbound transfers of personal information (including sensitive personal information) based on items 1 to 4 could be excluded (i.e., "deduplication"). For instance, when calculating the number of individuals involved in the outbound transfers, if all data fields of employees' personal information (including sensitive personal information) transferred abroad are necessary for cross-border human resources management as per lawfully adopted employment policies or lawfully executed collective contracts, the number of such employees could be deducted from the total count.

(2) It is crucial to distinguish and count separately individuals involved in the outbound transfers of sensitive and general personal information, and to assess whether the outbound data volume of either category meets the threshold for a specific outbound transfer route. For example, if the personal information being transferred abroad includes data fields related to general personal information and sensitive personal information of candidates, investors, business partners, suppliers, etc., and although the cumulative annual count of individuals involved in the outbound transfers of general personal information does not reach the threshold of 100,000 for the SCCs requirement, the presence of sensitive personal information in the data being transferred abroad, involving fewer than 10,000 individuals, still necessitates the data handler to execute and file SCCs with the provincial departments of the CAC.

(3) The Provisions on Cross-Border Data Flows stipulate that the count of individuals involved in outbound data transfers should reflect the actual cumulative number beginning from 1 January of the current year, which is a shift from the *Measures on the Security Assessment of Outbound Data Transfer* ("**Measures on the Security Assessment**") and the *Measures on the Standard Contract for Outbound Transfer of Personal Information* that considered the cumulative number from the beginning of the preceding year. This update is also captured in the Second Edition Guidelines.

(4) Moreover, even where exemptions from Security Assessment, SCCs, and PI Certifications apply, data handlers should still adhere to the PIPL. This includes informing the individuals of outbound transfer details, securing separate consents, and performing self-assessments to gauge the impact on personal information protection prior to the outbound transfers. Additionally, they must take the necessary steps to ensure that the overseas recipient handles the transferred personal information in accordance with the protection standards prescribed by the PIPL.

2. Cross-Border Transfer of Critical Data

According to the Measures on the Security Assessment, which took effect on 1 September 2022, when a data handler intends to transfer critical data abroad, it shall apply for the Security Assessment to the CAC

through the provincial departments of the CAC. The definition of "critical data" and the process for its identification have been of great interest to the industry.

The Provisions on Cross-Border Data Flows indicate that data handlers should identify and report critical data in accordance with relevant regulations. For data that has not been designated and notified as critical data by the relevant departments or regions, or publicly announced as such, data handlers are not required to apply for the Security Assessment of such outbound data as critical data. As far as the asset management industry is concerned, this means that the PRC subsidiaries of global asset managers are not required to conduct the Security Assessment until the relevant authorities (such as the People's Bank of China, China Securities Regulatory Commission) have explicitly notified them of designating the outbound data as critical data or have published the catalog(s) of critical data.

Significantly, the national standard *GB/T 43697 – 2024 Data Security Technology - Rules for Data Classification and Grading* ("**Rules for Data Classification and Grading**") was officially promulgated on 15 March 2024, and will come into effect on 1 October 2024. The Rules for Data Classification and Grading provide industry authorities with a benchmark for creating data classification and grading standards specific to their domains. Section 6.5 b) of the Rules for Data Classification and Grading elaborates on the principle provisions for identifying critical data and appends a comprehensive guideline for such identification as Appendix G. This includes a variety of principal factors for consideration. For instance, in the financial sector, Appendix G designates data that "reflects the economic operations and financial activities in the overall situation or key areas, relates to the industrial competitiveness, causes public safety incidents or affects the safety of citizens' lives, triggers group events or affects the community emotions and awareness (such as undisclosed statistical data and trade secrets of key enterprises)" as "critical data". We suggest global asset managers pay attention to the progress of critical data catalogs in the field of asset management.

3. Negative List Mechanism of Free Trade Zone ("FTZ")

In addition to the above measures, the Provisions on Cross-Border Data Flows also follow the Consultation Paper in introducing the FTZ negative list mechanism, which aims to further reduce the compliance burden for companies within the FTZs. Specifically, the Provisions on Cross-Border Data Flows allow the FTZs to independently compile a list specifying which data necessitate a Security Assessment, SCCs filing or PI Certification ("**Negative List**"). Consequently, only the data enumerated in the Negative List are subject to the requirements of applying for the Security Assessment, entering into the SCCs or passing the PI Certification. This implies that, when data handlers calculate the number of individuals involved in the outbound transfer of general/sensitive personal information, data not specified in the Negative List could be excluded from the count.

Institutions registered in the FTZs are suggested to diligently track the progress of the Negative List to determine whether their outbound data, including critical data and personal information, is categorized thereon.

4. Other Considerations for Data Compliance Under the New Rules

(1) Should an application for Security Assessment or SCCs filing have been initiated prior to the release of the Provisions on Cross-Border Data Flows and is no longer necessary under the new rules, data handlers may choose to either continue with the pre-existing procedure or withdraw their applications / filings through the provincial CAC departments.

(2) In light of the Provisions on Cross-Border Data Flows which establish different thresholds for the routes of outbound transfers of general personal information and sensitive personal information, global asset managers are advised to enhance the identification of sensitive personal information, sort out the categories of sensitive personal information in different business scenarios and determine the applicable route of outbound transfer based on the number of individuals involved in sensitive personal information and the specific business scenario.

(3) The CAC has introduced the "Data Cross-Border Transfer Application System" (https://sjcj.cac.gov.cn) to facilitate online applications. Non-CIIO data handlers are encouraged to utilize this platform for Security Assessment or SCCs filing application. Nonetheless, the CIIO's Security Assessment application or other circumstances that are impracticable to be declared through the system should continue to lodge their applications offline.

(4) Data handlers required to apply for Security Assessment or SCCs filing should prepare the application materials in accordance with the requirements of the Second Edition Guidelines.

(5) The Provisions on Cross-Border Data Flows provide some flexibility for the free flow of general data (non-personal information and non-critical data) in certain industries. According to Article 3 of the Provisions on Cross-Border Data Flows, data collected and generated in activities such as international trade, cross-border transportation, academic cooperation, transnational production, and marketing, which do not include personal information or critical data, are exempt from applying for Security Assessment, SCCs filing, or PI Certification.

If you would like to know more information about the subjects covered in this publication, please contact:

Sandra Lu
+86 21 3135 8776
Sandra.lu@llinkslaw.com

Lily Luo
+86 21 3135 8732
lily.luo@llinkslaw.com

Sue Sun
+86 21 3135 8661
sue.sun@llinkslaw.com

SHANGHAI	BEIJING	SHENZHEN
19F, ONE LUJIAZUI 68 Yin Cheng Road Middle Shanghai 200120 P.R.China T: +86 21 3135 8666 F: +86 21 3135 8600	30F, Central Tower, China Overseas Plaza, 8 Guanghuadongli, Chaoyang District Beijing 100020 P.R.China T: +86 10 5081 3888 F: +86 10 5081 3866	18F, China Resources Tower 2666 Keyuan South Road, Nanshan District Shenzhen 518063 P.R.China T: +86 755 3391 7666 F: +86 755 3391 7668
HONG KONG	**LONDON**	
Room 3201, 32/F, Alexandra House 18 Chater Road Central, Hong Kong T: +852 2592 1978 F: +852 2868 0883	1/F, 3 More London Riverside London SE1 2RE United Kingdom T: +44 (0)20 3283 4337 D: +44 (0)20 3283 4323	

www.llinkslaw.com

Wechat: LlinksLaw

WE LINK LOCAL LEGAL INTELLIGENCE WITH THE WORLD