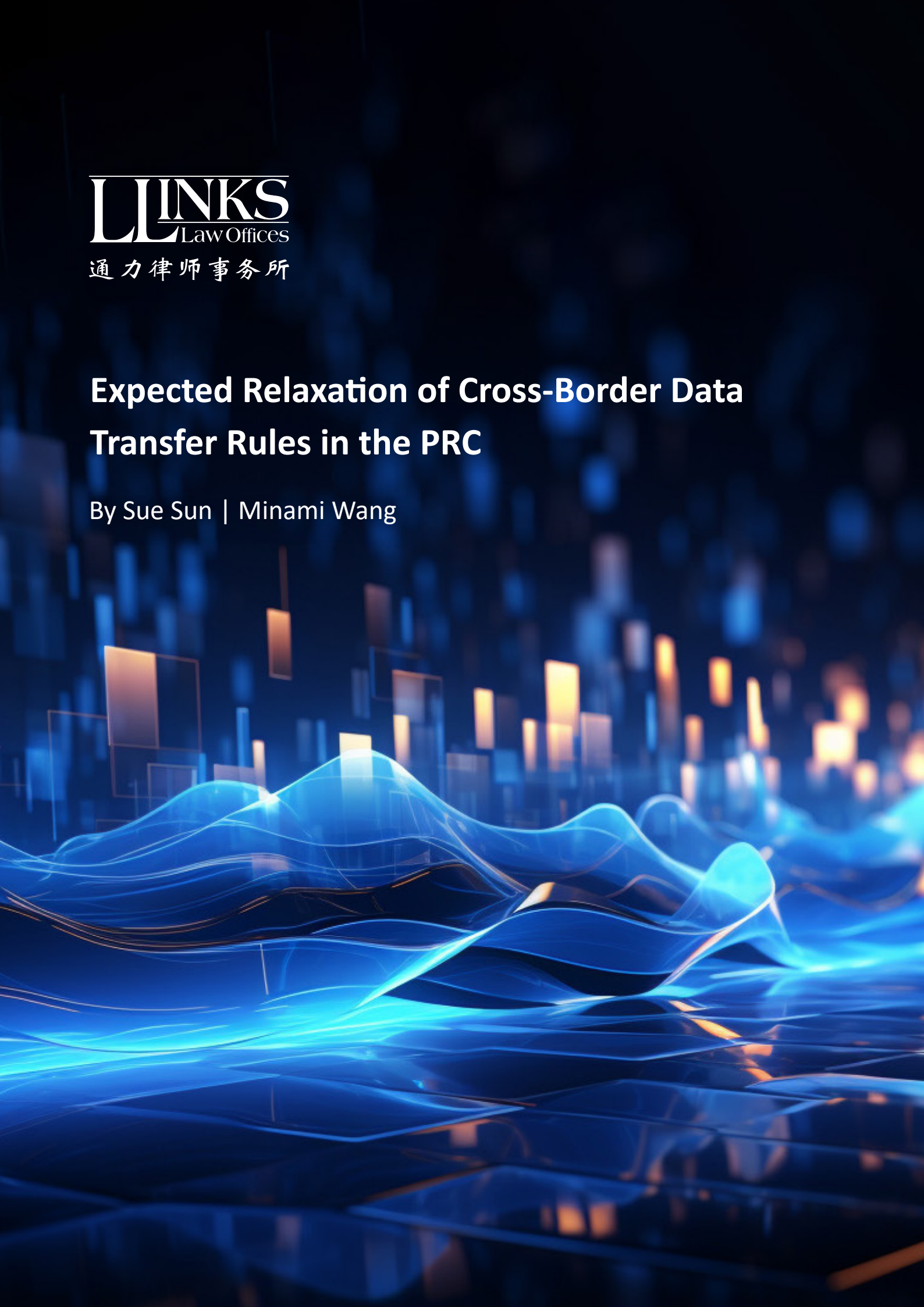
LINKS Law Offices
通力律师事务所

Expected Relaxation of Cross-Border Data Transfer Rules in the PRC

By Sue Sun | Minami Wang



On 28 September 2023, the Cyberspace Administration of China ("**CAC**") promulgated the *Provisions on Regulating and Promoting Cross-Border Data Flows (Consultation Paper)* (规范和促进数据跨境流动规定(征求意见稿), "**Draft Provisions on Cross-Border Data Flows**"), seeking public comments till 15 October 2023. The main impact of the Draft Provisions on Cross-Border Data Flows, when compared to the existing rules, is that it limits the scope of personal information export activities where CAC data export security assessment ("**Security Assessment**") or standard contract ("**SCCs**") filing is required, clarifies the rules for the identification of critical data, and effectively responds to the practical problems previously encountered in the Security Assessment and SCCs filing projects. This article intends to outline the key rules of the Draft Provisions on Cross-Border Data Flows from the perspectives of outbound transfer of personal information and critical data, as well as to provide follow-up suggestions for global asset managers' consideration.

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 personal information transfer, i.e. (1) passing the Security Assessment; (2) going through the personal information protection certification by a professional institution; (3) entering into the SCCs with the overseas recipient. Under the Draft Provisions on Cross-Border Data Flows, the following outbound personal information transfer activities are exempted from having to adopt one of the above three routes:

1. Exemption for specific scenarios of outbound personal information transfer, including:

    - Where it is necessary to transfer personal information abroad for the purpose of concluding and performing a contract to which the individual concerned is a party (such as cross-border shopping, cross-border remittance, air tickets and hotel reservations, visa processing, etc.);

    - Where it is necessary to transfer the personal information of employees abroad for human resources management in accordance with lawfully passed labor policies or lawfully executed collective contracts;

    - Where it is necessary to transfer personal information abroad to protect the health and property safety of a natural person in an emergency.

2. Exemption for outbound transfer of personal information generated and collected outside the territory of PRC.

3. Exemption for the situation where it is expected to export personal information of less than 10,000 individuals from the PRC within one year[1].

For the commercial presences set up by global asset managers in PRC (e.g. WFOE PFM, QDLP/QDIE, WFOE FMC, JV WMC, Securities Firm and Research WFOE), the cross-border transfer of personal information of employees, candidates, onshore investors and business partners may be involved in the course of their business operation to varying degrees, depending on the respective regulatory requirements. And in practice, most of the global asset managers choose the way of entering into the SCCs for the cross-border transfer of personal information. If the Draft Provisions on Cross-Border Data Flows takes effect without any changes, it is suggested that the global asset managers follow the criteria below to assess whether their onshore presence is subject to the SCCs filing:

1. Firstly, estimate whether the number of all the personal information subjects (including internal employees and external personnel such as investors) whose personal information is exported within the next year will be less than 10,000. If the number of such personal information subjects is less than 10,000, then the SCCs filing is not required per the Draft Provisions on Cross-Border Data Flows;

2. If it is estimated that the number of all the personal information subjects in point 1 above will be more than 10,000, it is advised to further assess whether the number remains more than 10,000 after excluding the number of employees. If the number still be more than 10,000 after the exclusion of employees, the SCCs filing is required; if the number falls below 10,000 after the exclusion, it is advised to follow point 3 below to assess whether the export of employees' personal information meets the necessity test;

3. For employees' personal information export, it is advised to scrutinize all the data fields that are being exported in all human resources management scenarios (including the onboarding process, remuneration management, KPI, promotion and training, etc.), and assess whether each data field meets the criteria of "necessity for human resources management and there is an absolute need to export such personal information". If the necessity test is fully met, then the number of employees can be excluded from the total number of personal information subjects, and if the number is less than 10,000, the SCCs filing is not required. However, if the necessity test is not fully met, then the number of employees should be included in the total number, and as the number is more than 10,000, the SCCs filing is required.

[1] According to Article 6 of the Draft Provisions on Cross-Border Data Flows, if it is estimated that in a given year, the personal information handler will transfer overseas the personal information of more than 10,000 but less than 1 million individuals, and the personal information handler has concluded the SCCs with the overseas recipient and completed the SCCs filing with the provincial departments of the CAC, or has passed the personal information protection certification, it is not required to apply for the Security Assessment; however, if the personal information of more than 1 million individuals will be transferred abroad, the Security Assessment will be required.

It is worth noting that even if the requirements of entering into the SCCs and filing are explicitly exempted after the Draft Provisions on Cross-Border Data Flows formally take effect, the PRC subsidiaries of global asset managers, as the personal information handlers, should still fulfill the corresponding obligations under the PIPL, including:

1. Complete the personal information protection impact assessment ("**PIA**") before providing personal information abroad, and document the relevant data handling activities.

   PIA is the most significant work for the SCCs filing. Although the Draft Provisions on Cross-Border Data Flows exempt the personal information handler from entering into the SCCs with the overseas recipient and making the filing with CAC under certain circumstances, per Article 55 of the PIPL, it is still obligated to conduct the PIA in advance for outbound personal information transfer, and document the relevant data handling activities. Nevertheless, there are still uncertainties as to whether the PIA must be conducted per the current guidelines issued by the CAC;

2. Obtain personal information subjects' separate consent if the outbound personal information transfer is based on consent;

3. Take necessary measures to ensure that the personal information handling by the overseas recipient meets the personal information protection standards stipulated in the PIPL.

In addition, the Draft Provisions on Cross-Border Data Flows stress again that data handlers should fulfill data security protection obligations when transferring critical data and personal information abroad, and ensure the security of the outbound data transfer. Local CAC will also carry out the post-supervision and may require data handlers to make rectifications if significant risks are identified during the outbound data transfer activities or data security incidents occur.

Cross-Border Transfer of Critical Data

According to the *Measures for the Security Assessment of Outbound Data Transfer*, 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 via provincial departments of the CAC. For what is critical data, most of the current effective laws and regulations only provide a general definition, and few industry sectors have identified a specific catalog of critical data. In practice, data handlers often need to identify critical data by themselves with reference to the general principles, which brings a great deal of uncertainty to their compliance work.

According to Article 2 of the Draft Provisions on Cross-Border Data Flows, for data that has not been designated and notified by the relevant departments or regions as critical data, 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 publicly released the catalog(s) of critical data.

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

In addition to the abovementioned measures, the Draft Provisions on Cross-Border Data Flows also introduced the FTZ negative list mechanism, which will further ease the compliance burden imposed on enterprises in the FTZs. Specifically, the Draft Provisions on Cross-Border Data Flows allows the FTZs to independently formulate a list of data, listing the scope under which it will be necessary to apply for the Security Assessment, conclude the SCCs, or pass the personal information protection certification ("**Negative List**"). This is to say that only data in the Negative List shall be subject to the requirements of applying for the Security Assessment, entering into the SCCs, and passing the personal information protection certification. Institutions registered in the FTZs are advised to closely follow the legislative trend of such Negative List and assess whether the outbound data (including critical data and personal information) falls into the Negative List.

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