Development of PRC Regulations on Cross-border Data Transfer

I. Background

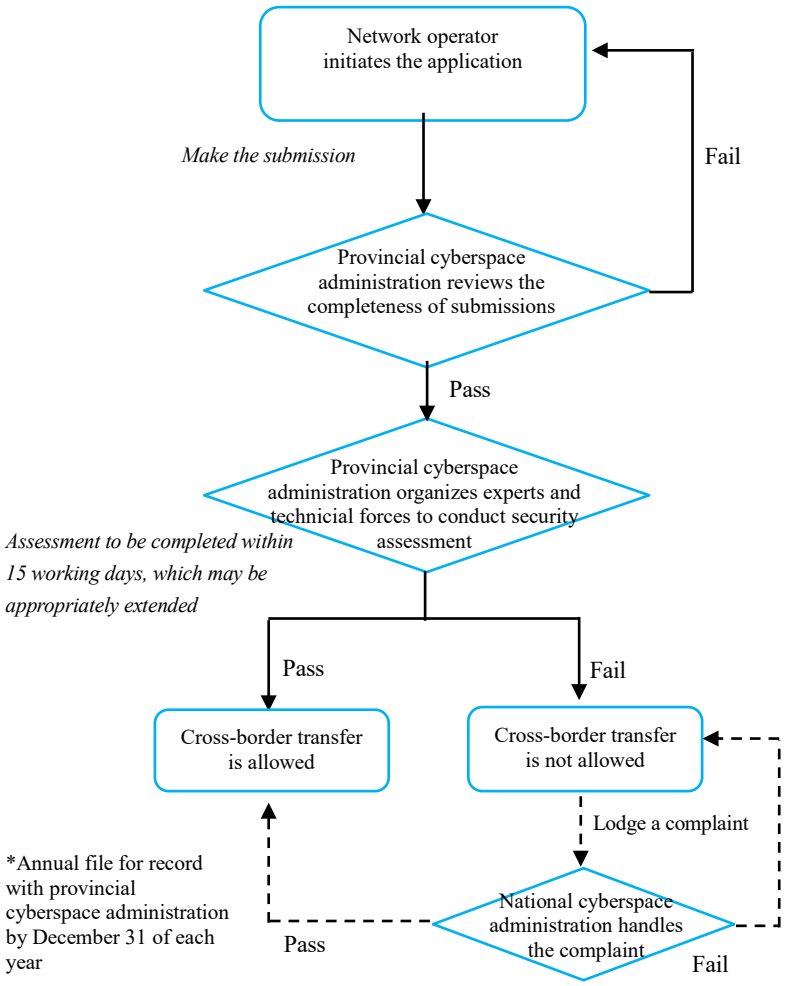
Early on the morning of June 13, 2019, Cyberspace Administration of China ("**CAC**") issued the Measures for Security Assessment for Cross-border Transfer of Personal Information (Draft for Comment) (the **"Draft Measures**"). The Draft Measures makes significant adjustments to the Measures for Security Assessment for Cross-border Transfer of Personal Information and Important Data (Draft for Comment) released on April 11, 2017. In terms of the structure, cross-border transfer of personal information and important data is likely to be regulated separately and no longer governed by a single legislation in the future. This can be seen obviously from the Administrative Measures for Data Security (Draft for Comment) previously issued by CAC and is further confirmed by the issuance of the Draft Measures[1]. In terms of the regulatory approaches, on the one hand, the Draft Measures innovatively regulates network operators and overseas recipients through contract concerning their cross-border transfer of personal information to protect the security of such transfer. On the other hand, the Draft Measures also establishes a full-coverage and comprehensive application for approval mechanism for cross-border transfer of personal information.

We understand that the Draft Measures reflects the latest regulatory trends and indicates certain alignment of data protection ideas with the spirit of the cross-border data transfer protection laws in other jurisdictions, especially the provisions regarding standard contractual clauses under Article 46 of GDPR. Overall, due to the wide scope of application, the Draft Measures will have a significant impact on the compliance of enterprises.

II. Assessment Procedures

In accordance with the Draft Measures, prior to cross-border transfer of personal information, a network operator shall make application to the provincial cyberspace administration of the place where the network operator is domiciled for security assessment for cross-border transfer. To be specific, please refer to the security assessment procedures illustrated as below:

[1] Article 28 of Administrative Measures for Data Security (Draft for Comment) provides that: "[n]etwork operators shall assess the potential security risks prior to releasing, sharing or selling important data or transferring such data abroad, and shall report to the competent regulatory department for approval. If the competent regulatory department is unclear, network operators shall report to the provincial cyberspace administrations for approval. Provision of personal information abroad shall be implemented in accordance with the relevant provisions."

Stage	Diagram of Procedures
Initiation of Application Review of Completeness Security Assessment Cross-border Transfer/Complaint	

III. Key Q&As

1 Do network operators have the obligation of data localization?

No explicit requirements. We recommend enterprises to assess the pros and cons of data localization taking into consideration of business scenarios and global commercial modes.

In accordance with Article 37 of the Cybersecurity Law of the People's Republic of China (the "**Cybersecurity Law**"), the operator of a critical information infrastructure is explicitly required to store, within the territory of the People's Republic of China, personal information and important data collected and generated during its operation within the territory of the People's Republic of China. This provision sets forth the requirement of "data localization". The Measures for Security Assessment for Cross-border Transfer of Personal Information and Important Data (Draft for Comment) issued by CAC on April 11, 2017 once extended such requirement to all network operators. However, we note that current version of the Draft Measures places no explicit requirements on network operators in respect of local storage.

Comment:
Compared with the Measures for Security Assessment for Cross-border Transfer of Personal Information and Important Data (Draft for Comment), the Draft Measures provides for no explicit requirements of data localization. However, at present, a large number of enterprises transfer data abroad in day-to-day operations, and there are great uncertainties whether they can obtain a pass regarding the security assessment for such outbound transfer from the competent cyberspace administration in a smooth and timely manner. In order to ensure their business stability, enterprises may need to further consider the feasibility of local data storage with controllable costs. On one hand, data localization can meet the required "local storage" obligation if they can possibly be identified as an operator of a critical information infrastructure; on the other hand, it can secure their business continuity as a general network operator.

2 Does application for security assessment for cross-transfer of personal information apply to all network operators?

Yes.

Comment:
The Draft Measures adopts a same definition of "network operator" as the one provided in the Cybersecurity Law, and includes no limitations or exemptions regarding the scale, industry, business scope of the "network operator" who shall be subject to application for security assessment for cross-border transfer. Theoretically, all network operators will be required to obtain prior approval from the competent provincial cyberspace administration regardless of in whichever means they transfer personal information abroad (e.g. email, video or business system). For multinational companies, cross-border transfer and centralized management of personal information of their employees will also need to meet the requirements of the Draft Measures.

3 What contents shall be included in the contract between a network operator and a data recipient?

The Draft Measures provides for the contents concerning cross-border data transfer to be included in the contract between a network operator and a recipient from the following three aspects: (i) the basic information on cross-border transfer of personal information and the distribution of the relevant obligations and liabilities (Article 13); (ii) obligations and liabilities to be assumed by the network operator (Article 14); and (iii) obligations and liabilities to be assumed by the recipient (Article 15).

Comment: The provisions of the Draft Measures concerning the execution of a contract for cross-border transfer of personal information between a network operator and a recipient are compatible with the legislative ideas reflected in the standard contractual clauses under GDPR. In another word, the contractual arrangement ensures that the parties provide appropriate security protection measures for cross-border transfer and that the adequate safeguards for the rights of personal information subjects will not be impaired due to cross-border transfer.

In addition, the Draft Measures grants personal information subjects a special right of access, i.e. he or she may request a copy of the contract. Given that the contract between a network operator and a recipient may contain sensitive business information inappropriate to be disclosed, it may be necessary to choose what disclosures are to be made in practice.

4 What if personal information is transferred to a third party after cross-border transfer?

In order to ensure to be actually implemented in practice, the Draft Measures clearly limits onward transfers after transferring aboard. Specifically, pursuant to Article 16 of the Draft Measures, the network operator and the recipient shall sign a contract under which the recipient is explicitly required not to transfer any personal information received to a third party unless specific conditions have been met.

Comment: Article 16 distinguishes between personal information and sensitive personal information. For transfer of personal information to a third party, it is required that the personal information subject's right to object shall be safeguarded based on the full protection of his or her right to be informed. In other words, when the personal information subject requests to stop the transfer, it shall be stopped immediately and the third party shall be required to delete the data. In the scenarios involving sensitive personal information, the consent of the personal information subject shall be obtained before the transfer. In addition, the cross-border data flow may itself involve multiple parties. For example, the network operator transfers data abroad to Recipient A for transit who then transfers the same to Recipient B. In this scenario, it is unclear whether it should carry out security assessment for twice as the recipients are different or whether such practice constitutes onward transfer within the same cross-border data transfer.

5 What are the special requirements for foreign enterprises doing business in China?

Pursuant to Article 20 of the Draft Measures, if foreign organizations collect personal information of domestic users through the internet or other means in their business activities, they shall fulfill the responsibilities and obligations of network operators laid down in the Draft Measures through their legal representatives or institutions in China.

Comment: It is inevitable for foreign enterprises registered and carrying out business activities in China to "collect personal information of domestic users through the internet or other means" in their business activities. The China branches or subsidiaries of these foreign enterprises may need to fulfill application obligations for cross-border transfer of personal information in accordance with the requirements of Article 20.

It is worth noting that even network operators not registered in China may be deemed to provide products or services in the territory of China and thus subject to the jurisdiction of the Cybersecurity Law[2]. In accordance with the requirements of this Article 16, if such foreign network operators collect personal information of domestic users through the internet and other means, for example, cross-border e-commerce platforms or foreign group companies collect personal information of domestic customers through their official websites for registration, online shopping and delivery, etc. , they shall establish new institutions or appoint legal representatives in China and complete application regarding cross-border transfer of personal information as required above. This is in line with Article 27 of GDPR, which provides that data controllers or processors not established in the Union shall designate in writing a representative in the Union.

6 What is the content of the security assessment?

Compared with the Measures for Security Assessment for Cross-border Transfer of Personal Information and Important Data (Draft for Comment), the Draft Measures provides for, among others, additional contract-related assessment requirements. For one thing, it requires a substantive review of the terms of the contract in order to assess whether they provide adequate protection of the legitimate rights and interests of the personal information subjects. For another, it is required to assess the enforceability of the contract from the perspective of contract performance.

Comment: For enterprises involving cross-border transfer of personal information, if they have already entered into a contract for data transfer with overseas recipients, they may need to review the existing terms and the performance of their contract so as to assess whether it can meet the requirements of the Draft Measures. If there is no specific arrangement for the cross-border data transfer, it is necessary for those enterprises to negotiate and agree upon the supplementary terms with the overseas recipients in

[2] Pursuant to Note 1 to Article 3.2 of the Information Security Technology - Guidelines for Data Cross-border Transfer Security Assessment (Draft for Comment), "[n]etwork operators not registered but carrying out business or providing products or services in the territory of the People's Republic of China, shall be considered as operating in the territory of the People's Republic of China."

accordance with the requirements of the Draft Measures.

7 What are the subsequent obligations for enterprises following the completion of security assessment for cross-border data transfer?

The security assessment for cross-border data transfer is not "once and for all". After the completion of such assessment, the enterprises shall appropriately keep the relevant records (Article 8), submit annual reports by the specified date (Article 9), establish the internal emergency response system to ensure the timely report to the provincial cyberspace administrations upon the occurrence of any major data security incidents(Article 9), and identify the changes, if any, to such outbound data transfer and determine whether the reassessment is required (Article 3).

8 Which party shall make the application if cross-border transfer of personal information involves multiple parties?

The Draft Measures does not address which party shall make the application when multiple parties are involved in the cross-border transfer of personal information, or the distribution of obligations and liabilities among the parties.

Comment: Regarding the security assessment for cross-border transfer of personal information, the Information Security Technology - Guidelines for Data Cross-border Transfer Security Assessment (Draft for Comment) issued by National Information Security Standardization Technical Committee on August 25, 2017 specifies which party is to take major liabilities and which party is to cooperate in the typical multiple-party cloud service scenarios. It provides that, "[w]hen a cloud service client proactively requests the cross-border data transfer from the cloud service provider, such provider shall cooperate with the cloud service client to conduct the security self-assessment and the cloud service client shall take corresponding liabilities. When the provider proactively offers such outbound data transfer, the cloud service client shall cooperate with the cloud service provider to conduct the security self-assessment and the provider shall take corresponding liabilities."

It calls for further clarification as to whether the Draft Measures will adopt the concept of "the party which requests the cross-border data transfer shall be liable for the security assessment" reflected in the above guidelines.

9 Is there any grace period for the compliance of enterprises after the official implementation of the Draft Measures?

We have not noted any similar provision in the current text of the Draft Measures, as the two-year grace period provided in GDPR.

Comment: Enterprises that may be recognized as network operators may need to take action to get fully prepared for the official implementation of the Draft Measures as

soon as possible (please refer to the **Part V. Recommendations** for details).

IV. Issues Deserving Further Consideration

In the context of global data flows, scenarios and demands for outbound transfer of personal information are diversified. If the application for security assessment for cross-border transfer of personal information applies without exceptions and exemptions, great impacts will be imposed on business continuity and compliance cost of enterprises. Issues deserving further consideration include:

- When the personal information is transferred to a jurisdiction which requires a relatively high level of protection of data security, considering that the risk of data breaches is relatively controllable, can the application obligation for the security assessment be exempted?
- Referring to the practice of GDPR, will CAC subsequently release any standard model clauses on cross-border transfer of personal information, so as to reduce the risk of non-conformity of enterprises' self-drafted contract?
- It is advisable for CAC to include exemptions to application for security assessment for cross-border transfer of personal information in some explicitly inapplicable scenarios, such as a scenario where cross-border transfer is sporadic, only limited personal information subjects are involved; and at the same time, data controller has already assessed all circumstances related to data transfer, and provided appropriate measures for personal information protection in accordance with the assessment.

V. Recommendations

In consideration of the relevant requirements in the Draft Measures, if enterprises operating in China transfer personal information abroad, they are recommended to focus on below matters in compliance:

- To comprehensively identify scenarios which may involve cross-border transfer of personal information in the course of business;
- To communicate with the overseas data recipient on terms and execution of the contract. The terms on cross-border transfer of personal information can be separated from the main business contract to facilitate the future possible provision of a copy to personal information subjects;
- To prepare the report on the analysis of security risk and protection measures on outbound transfer of personal information and other materials required for application pursuant to the assessment requirements;
- To prepare and properly maintain records on cross-border transfer of personal information;
- After completion of security assessment for cross-border transfer of personal information, to identify the scenarios requiring reassessment in the course of cross-border transfer;

- For enterprises having business activities which in nature involve intensive cross-border transfer of personal information, such as cross-border cloud computing service, to prudently assess the compliance cost of cross-border transfer and local processing cost.

To sum up, the Draft Measures establishes a cross-border transfer security assessment and review mechanism focusing on the contract for cross-border transfer of personal information to be entered into between the network operator and the data recipient. It manifests a similar approach as that of GDPR on cross-border transfer of personal information. Accordingly, when the enterprises deploy their structure of global data flows, they are recommended to examine and integrate the similarities and differences among the jurisdictions on the requirements for local storage and cross-border transfer of data, so as to achieve comprehensive compliance on data protection in the most efficient way.