New PRC Regulations on Cross-Border Transfer of Data

Skadden

08 / 23 / 22

If you have any questions regarding the matters discussed in this memorandum, please contact the following attorneys or call your regular Skadden contact.

Steve Kwok
Partner / Hong Kong
852.3740.4788
steve.kwok@skadden.com

Bradley A. Klein
Partner / Washington, D.C.
202.371.7320
bradley.klein@skadden.com

Siyu Zhang
Associate/ Hong Kong
852.3740.4816
siyu.zhang@skadden.com

One Manhattan West
New York, NY 10001
212.735.3000

42/F, Edinburgh Tower, The Landmark
15 Queen's Road Central, Hong Kong
852.3740.4700

Editor's note: ***On August 31, 2022, the Cyberspace Administration of China issued detailed guidance on how to file a cross-border data transfer security assessment with the authority.***

The Chinese regulatory authorities have published several new regulations and proposals in the past two months seeking to clarify the requirements of the Chinese Personal Information Protection Law (the PIPL) that came into legal effect in 2021. These developments confirm that the People's Republic of China (PRC) authorities remain focused on strengthening the rules for handling and exporting data originating in China or involving Chinese data subjects. Multinational companies with operations in China should assess their data practices to ensure compliance with these newly enacted PRC regulations.

Background

The PIPL provides that personal information can be transferred out of China only after the data subjects have given their informed consent, the data transferor has conducted a personal information protection impact assessment and at least one of the following conditions has been satisfied:

i. the data transferor has applied for and passed a security assessment by the Cyberspace Administration of China (the CAC);

ii. the data transferor has obtained a Personal Information Protection Certificate from a duly authorized data security assessment institution or authority;

iii. the data transferor has adopted standard contract clauses prescribed by the CAC in its data transfer agreement; or

iv. the data transferor has fulfilled conditions stipulated in other laws or regulations.

As explained below, the new draft and final regulations published by the PRC authorities elaborate on the requirements to meet the first three of the four conditions set forth above.

I. CAC Security Assessment

On July 7, 2022, the CAC issued the final version of the Measures for Security Assessment for Cross-Border Data Transfers (the Security Assessment Measures), which will take effect on September 1, 2022. The Security Assessment Measures provide that before engaging in any further cross-border data transfer activities, the following categories of data handlers will need to pass a security assessment conducted by the CAC:

- "Critical Information Infrastructure Operators" or data handlers that handle "over one million individuals' personal information";
- companies that transfer "important" data overseas; or
- since January 1 of the preceding year, companies that have exported "over 100,000 individuals' personal information or over 10,000 individuals' 'sensitive personal information.'"

The definitions of key terms follow those under the PIPL. "Personal information" is broadly defined to cover "any information related to identified or identifiable natural persons stored in electronic or any other format." Under this definition, even if the information itself is not sufficient to identify a specific individual, as long as the information is "related to identified or identifiable natural persons," the PIPL still applies, unless the information has been irreversibly anonymized, in which case, the sanitized information would not constitute personal information. "Sensitive personal information" includes a data subject's biometrics, religious beliefs, health data, financial metrics and travel records, as well as young children's information. The Security Assessment Measures define "important data" as "data that,

once tampered with, destroyed, leaked, illegally obtained or illegally used, may endanger [Chinese] national security, economic operation, social stability, public health and safety, and so forth." Nonetheless, a number of ambiguities remain. For example, while the Security Assessment Measures provide that companies that export data above certain numerical thresholds "since January 1 of the preceding year" need to pass a CAC security assessment before effectuating any further cross-border transfers of data, the measures do not specify the cutoff date for purposes of calculating the volume of exported data — *i.e.*, December 31 of the preceding year, the time that the CAC conducts the security assessment, the expiration of the grace period for compliance with the new law in March 2023 (see *Implications* below) or some other date. It is also unclear what rationales would be deemed sufficient to justify the export of data.

In the application materials submitted to the CAC to initiate its data security assessment process, in addition to the application form, the data handler must include for the CAC's review and approval: (i) a self-assessment report and (ii) the cross-border data transfer agreement signed with the foreign recipient. For the self-assessment, data handlers must evaluate the proposed cross-border data transfer from the perspectives of both the PRC data transferor (*e.g.*, the purpose, necessity, scope and method of the proposed data transfer) and the foreign data recipient (*e.g.*, the data security protection measures taken by the recipient and the relevant policies and regulations of the recipient's jurisdiction). For the cross-border data transfer agreement, data handlers must ensure that the agreement specifies, among other things, the PRC data transferor's and the foreign data recipient's data protection obligations, whether the data will be further disseminated by the data recipient and what and how foreign law may apply to the data in question. The agreement must also provide for adequate legal remedies in the event either party breaches the data transfer agreement.

II. Cross-Border Data Transfer Certification

In place of completing the CAC security assessment, the second way to effectuate cross-border transfers of personal information out of China under the PIPL is to obtain a cross-border data transfer certificate from a qualified institution. On June 24, 2022, the Secretariat of the National Information Security Standardization Technical Committee issued the Technical Specification for Certification of Cross-Border Transfers of Personal Information. This document provides guidance to duly authorized data security assessment institutions or authorities in the PRC to help them evaluate whether data handlers that intend to transfer data overseas meet prescribed data security requirements and thus whether to issue the requested certificates authorizing the transfer. However, the list of authorizing institutions and authorities have not yet been released. Therefore, using this option in lieu of passing a CAC security assessment is currently available only in theory, and the extent to which companies can rely on this certification process to effectuate cross-border data transfers remains to be seen.

III. Draft Measures on Standard Contract Clauses

A third way to effectuate cross-border transfers of personal information out of China under the PIPL is to incorporate standard contract clauses prescribed by the CAC into data transfer agreements with foreign recipients. On June 30, 2022, the CAC issued the draft Provisions on Standard Contract for Cross-Border Transfer (Provisions) for public comment. From the data handler's perspective, this is likely the most user-friendly approach to qualifying a data transfer because this option does not require approval or review by the CAC or by any third-party assessment institution. Instead, no later than a month after the effective date of the cross-border data transfer agreement, data handlers need only to file with the CAC the cross-border data transfer agreement along with a "personal information protection impact assessment report." However, this third option is available only to data handlers that are not Critical Information Infrastructure Operators, that handle fewer than one million individuals' personal information and that transfer only a small amount of data overseas — *i.e.*, since January 1 of the preceding year, personal information of no more than 100,000 individuals or "sensitive personal information" of no more than 10,000 individuals.

The draft Provisions, which are expected to become final in the coming months, include a template contract with standard clauses for data handlers' reference. These standard clauses require, among other things, that the PRC data transferor attest that the data in question was collected and processed in compliance with PRC laws, that the requisite consent has been obtained from the relevant data subjects, that the data handler has completed a personal data protection impact assessment and that the data to be transferred abroad is limited to only that which is necessary to accomplish the purpose of the data transfer. The PRC data transferor must also agree to answer inquiries from PRC regulators regarding the data processing activities to be undertaken by the data recipients. The foreign data recipient must, among other things, undertake that it will implement safeguards to ensure data security; refrain from transferring the received data further unless certain prescribed conditions are met; in case of a data leak, notify the sender, the data subjects and the relevant PRC authorities and take prompt remedial actions; and accept a data audit from the data transferor regarding the data processing activities that are the subject of the cross-border data transfer agreement.

New PRC Regulations on Cross-Border Transfer of Data

Implications

For large multinational companies operating in China, the data export thresholds that would trigger the Security Assessment Measures appear quite low. Even if a company "de-identifies" certain personal data (*e.g.*, by replacing individuals' names with serial numbers) and transfers only the nonidentifiable parts of the data overseas, the above-described requirements may still apply as long as the data has not been irreversibly anonymized such that no amount of reconstruction can trace the sanitized data back to specific individuals — a stringent requirement that companies are unlikely to meet given the needs and realities of most business operations.

The Security Assessment Measures provide a grace period of six months after the effective date, *i.e.*, until March 2023, for companies to address any noncompliance issues. Companies that fail to meet that deadline would be prohibited from engaging in further cross-border data transfer activities. To reduce the risk of business interruptions, multinational companies, particularly those operating in data-heavy or data-sensitive industries, should consider initiating self-assessments without delay to determine which of the eligibility criteria under the PIPL they can most readily satisfy and what data protection enhancements are needed to meet the applicable eligibility criteria to ensure that the exportation of China-origin data critical to their business operations can continue uninterrupted after the expiration of the grace period in March 2023.