



China to Start Implementing Restrictions on Cross-Border Transfers of Personal Information

IN SHORT

The Situation: China released new regulations and guidelines to clarify the procedural requirements companies must satisfy for the cross-border transfer of personal information under the Personal Information Protection Law ("PIPL").

The Issues: The regulations and guidelines set forth different requirements applicable to different types of personal information handlers ("PI Handlers"), which primarily depend upon the amount and characteristics of the personal data transferred.

Looking Ahead: Companies operating in China should assess their transfer practices, identify the procedural requirements applicable to those practices, and immediately begin strategizing to meet those requirements.

China recently issued several new regulations and guidelines to clarify the procedural requirements for complying with PIPL provisions governing the cross-border transfer of personal information ("PI").

The PIPL provides that, before transferring PI out of China, PI Handlers must satisfy one of the following procedural requirements:

- Passing a security assessment ("Assessment");
- Undergoing a personal information protection certification ("Certification");
- Entering into standard contractual contracts ("SCCs") with the overseas recipient; or
- Meeting other conditions provided in laws, regulations, or by competent authorities.

Recently, PRC authorities released new regulations and draft regulations clarifying how PI Handlers may satisfy the Assessment, Certification, and SCCs requirements, including:

- Measures on State Security Assessment of Cross-Border Data Transfer (the "Assessment Measures"), issued July 7, 2022, and effective September 1, 2022;
- Draft Regulation on SCCs for the Export of PI (the "Draft SCC Regulation") and the sample SCCs, issued June 30, 2022; and
- Practice Guide to Cybersecurity Standards—Technical Guidelines on Certification for Cross-border Processing of PI (the "Practice Guide"), issued and effective June 24, 2022.

Security Assessment

According to the Assessment Measures, an Assessment is mandatory if a PI Handler: (i) plans to transfer important data (i.e., data that could impact national security or China's public interest);

(ii) is an operator of critical information infrastructure and processes the PI of more than 1 million people; or (iii) since January 1 of the previous year (i.e., the relevant period will be between 12-24 months), has cumulatively transferred out of China the PI of 100,000 people, or the sensitive PI of 10,000 people.

Obtaining an Assessment may be a lengthy process. The Cyberspace Administration of China ("CAC") will typically complete the Assessment within 45 working days upon official acceptance but has the ability to extend this without limitation in complex cases. There is a six-month grace period after the September 1, 2022, effective date for companies to bring themselves into compliance and file for a security assessment. This includes companies that have transferred data prior to the effective date of the Assessment Measures whose data transfers meet the mandatory requirements. Companies, therefore, should immediately assess whether their cross-border transfers will require an Assessment.

Certification Requirement

If an Assessment is not required, the PI Handler may choose between two simpler procedures to comply with the cross-border transfer provisions of the PIPL—Certification or use of the SCCs—both of which are still subject to a certain level of government scrutiny.

The PIPL provides that PI Handlers who wish to transfer PI using the Certification requirement must obtain such Certification from a specialized institution recognized by the CAC in advance of the transfer. According to the Practice Guide, the Certification applies to: (i) cross-border data processing between multinational companies or subsidiaries or affiliates of the same business entity; and (ii) PI processing activities described under Article 3.2 of the PIPL, i.e., processing PI of natural persons outside the country for purpose of analysis and evaluation of the behavior of natural persons in the country. Further, the Practice Guide provides that, to obtain the Certification, PI Handlers and overseas recipients must enter a legally binding and enforceable documentation to ensure that the rights and interests of PI subjects are fully protected.

The Practice Guide provides what should generally be included in such legal documentation and does not provide specific details, thereby leaving PI Handlers and overseas recipients with discretion to define each party's rights and obligations for the cross-border transfer of PI.

Use of Standard Contractual Clauses

Although the Draft SCC Regulation and the sample SCCs have not been finalized, companies should consider whether they want to utilize the SCCs. According to the Draft SCC Regulation, PI Handlers who enter into the SCCs must file executed SCCs with the relevant PRC authorities (filing may take place after the PI transfer), after which their implementation of the SCCs will be monitored. This may include responding to authorities' inquiries and cooperating with authorities' inspections on the performance of obligations under the SCCs. Additional obligations under the SCCs include obligations to notify the PI Handler and PRC authorities of a data breach, and to maintain records of the PI processing activities for at least three years. The parties to the SCCs would also have to accept Chinese law as governing law for the SCCs and agree to bring all lawsuits arising from the SCCs before a competent court in the PRC.

In extreme cases, PRC authorities may suspend the PI transfer if the PI Handler fails to comply with the terms of the SCCs. Moreover, while the PI Handlers and overseas recipients may supplement the SCCs, the Draft SCC Regulation provides that the parties may not enter into any clause that conflicts with the SCCs.

Differences and Similarities with EU GDPR SCCs

Unlike the standard contractual clauses for the cross-border transfer of PI under the General Data Protection Regulation ("GDPR Standard Contract Clauses"), which follow a modular approach and are designed to provide safeguards for transfers of PI to third countries (outside of the European Economic Area) in four different transfer scenarios (controller-to-controller, controller-to-processor, processor-to-processor and processor-to-controller), the obligations set forth under the SCCs apply similarly to all forms of transfers between PI Handlers in China and the corresponding overseas recipients. There are, however, certain similarities between the SCCs and the GDPR Standard Contract Clauses, such as: (i) providing for third-party beneficiary rights of PI subjects; (ii) foreseeing a warranty that the parties have conducted a transfer impact assessment; (iii) safeguarding the processing of PI by taking effective technical and management measures to

ensure the security of PI; (iv) allowing for audits by the PI Handler; and (v) accepting joint and several liability for claims brought by PI subjects.

THREE KEY TAKEAWAYS

1. Map and review anticipated and prior cross-border data transfers in light of the requirements in the Assessment Measures, Certification Guidance and Draft SCC Regulation to understand any gaps in compliance with the data transfer requirements.
2. Identify the appropriate cross-border data transfer mechanism considering the business mode, type, and volume of PI involved as well as the recipient countries.
3. Begin immediate implementation of the selected data transfer mechanism and ensure a consistent approach to the extent possible (e.g., description of data transfers as part of SCCs) in light of overall global data protection and data security compliance programs, and document implementation for accountability purposes.



Elizabeth Cole
Singapore, Shanghai



Lillian He
Shanghai



Jörg Hladjk
Brussels



Jerry C. Ling
San Francisco



Lisa M. Ropple
Boston



Undine von Diemar
Munich

*Evelyn Ni of the Shanghai Office
contributed to this Commentary.*

Jones Day is a global law firm with more than 2,400 lawyers on five continents. One Firm Worldwide®

Disclaimer: Jones Day's publications should not be construed as legal advice on any specific facts or circumstances. The contents are intended for general information purposes only and may not be quoted or referred to in any other publication or proceeding without the prior written consent of the Firm, to be given or withheld at our discretion. To request reprint permission for any of our publications, please use our "Contact Us" form, which can be found on our website at www.jonesday.com. The mailing of this publication is not intended to create, and receipt of it does not constitute, an attorney-client relationship. The views set forth herein are the personal views of the authors and do not necessarily reflect those of the Firm.

© 2022 Jones Day
North Point, 901 Lakeside Avenue, Cleveland, Ohio 44114-1190
www.jonesday.com