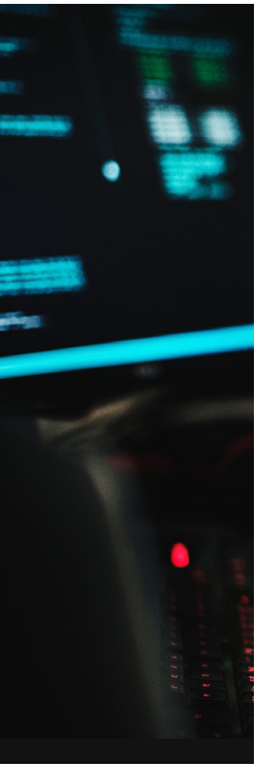
Rainer Burkardt
Founder and Managing Director
Burkardt & Partner Shanghai

Ondrej Zapletal
Legal Advisor
Burkardt & Partner Shanghai

CROSS-BORDER DATA TRANSFER

How to Transfer Your Data Out of China

With the issuance of the 2017 PRC Cybersecurity Law, the 2021 PRC Data Security Law, and the 2021 PRC Personal Data Protection Law (“PIPL”), cross-border data transfer became one of the key compliance topics for international companies doing business with, or having subsidiaries in, the People’s Republic of China (“PRC”).



The PRC cross-border data regime set out in these laws is based on the principle of data localization, i.e., certain data must be stored within the PRC and may be provided abroad only under specific conditions. As elaborated below, these conditions depend on different factors, such as the type and volume of data processed, or data transferred abroad.

None of the above-stated laws provides a definition of "cross-border data transfer." However, it should be noted that not only the actual data transfer by the data processor from the PRC to an overseas recipient will be considered cross-border data transfer, but also access of the overseas recipient (e.g., the parent company of the PRC subsidiary) to data stored in the PRC.

General preconditions for cross-border transfer of personal information ("PI") are regulated in the PIPL, according to which a PI processor who genuinely needs to provide PI to parties outside the PRC due to business or other needs, shall:

1. Pass a security assessment organized by the State Cyberspace Administration of China ("CAC")

2. Pass a PI protection certification by a qualified institution in accordance with the provisions of the CAC

3. Conclude a contract with the overseas recipient according to the standard contract formulated by the CAC ("Standard Contract"), or

4. Satisfy other conditions stipulated by the laws, administrative regulations, or the CAC.

Considering the above, data is allowed to be transferred overseas based on one of the three following legal options:

1. CAC Security Assessment

Based on the PIPL, PI processors that process PI exceeding the threshold prescribed by the CAC shall store the PI collected and generated within the PRC in principle in the PRC. Where such PI is genuinely necessary to be provided overseas, the security assessment organized by the CAC shall be passed. Currently, the term "genuinely necessary" is not defined under PRC law.

On September 1, 2022, the Measures for Cross-Border Data Transfer Security Assessment ("Measures"), which implement and refine the cross-border data transfer rules under the above three laws, took effect. The Measures specify the threshold for cross-border transfer of PI under the PIPL and regulate the so-called data export risk self-assessment procedure, as well as the data export security assessment before the CAC.

Under the Measures, data processors are required to apply for a data export security assessment with the CAC in case of:

1. Transfer of PI by "critical information infrastructure operators" to a recipient outside of the PRC;

2. Transfer of PI by data processors, processing PI of more than one million data subjects to a recipient outside of the PRC;

3. Transfer of PI of more than 100,000 data subjects or transfer of "sensitive PI" of more than 10,000 data subjects on a cumulative basis since January 1 of the preceding year.

In addition to the above-listed conditions referring to PI, the Measures also apply to the cross-border transfer of "important data" to a recipient outside of the PRC, and other circumstances stipulated by the CAC.

Before applying for a data export security assessment with the CAC, the data processor must conduct a data export risk self-assessment. The Measures specify a catalog of indications on which data processors shall focus during risk self-assessment.

In addition to the application form, the risk self-assessment report, and other application documents required by the CAC, the applicant must provide the CAC with an agreement concluded with the data recipient abroad, e.g., data processing agreement, the minimum content of which is specified in the Measures. The entire procedure of the data export security assessment before the CAC takes at least 57 working days, although the time period may be extended by the CAC in complex cases.

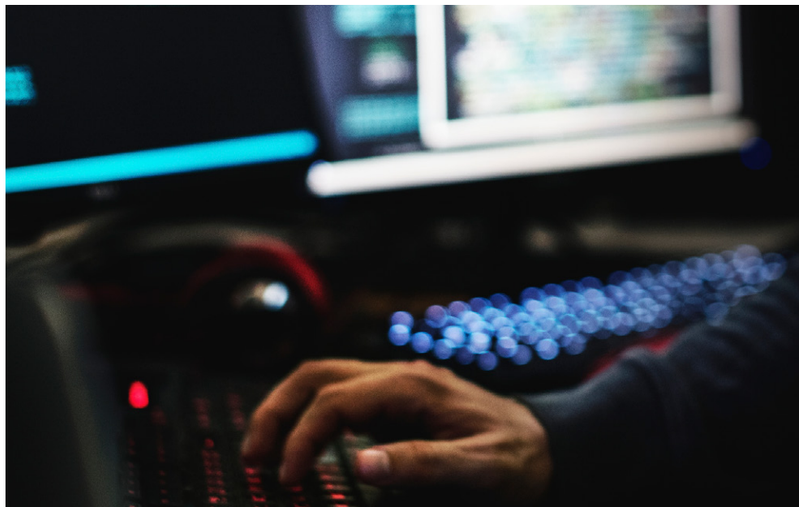
The validity of the data export security assessment is two years. No later than 60 working days before the expiration of the validity period, the data processor must apply for a new data export security assessment. However, if any of the special circumstances described in the Measures occur during the validity period, data processors are required to reapply for the data export security assessment during the two-year period.

It is noteworthy that the Measures prescribe a 6-month transition period for cross-border data transfers that occurred *before* the Measures' effective date on September 1, 2022. As a result, companies must make corrections within six months from the effective date of the Measures to ensure that cross-border data transfer conducted before September 1, 2022, complies with the requirements set forth in the Measures.

2. Personal Information Protection Certification

Data processors transferring PI to a recipient outside of the PRC may apply for a personal information protection certification ("PIPC") by a qualified institution. It is noteworthy that this option applies only to the cross-border transfer of PI, and under the condition that a data export security assessment as described above is not required.

The Guidelines on Cyber Security Standards — Security Certification Specifications for Cross-border Processing of Personal Information



Chinese subsidiaries shall analyze the data to be transferred to or to be made accessible by their overseas parent companies, including data classification, data quantification, and cross-border data flow analysis.

("Specifications"), which regulate the application scope, principles, obligations, and requirements for PI cross-border transfer and rights of the data subject, were issued by the National Information Security Standardization Technical Committee (TC260) on June 24, 2022. The Specifications provide non-mandatory guidance for evaluating the fulfillment of cross-border data transfer requirements and conditions for PIPC issuance.

According to the Specifications, the PIPC may be applied only to two scenarios, namely to (1) cross-border PI transfer between multinational corporations, subsidiaries, or affiliated companies of the same economic or institutional entity (in this case, the PRC entity, which transfers PI abroad, shall apply for the PIPC), and (2) processing PI of natural persons in the PRC from abroad as stated in the PIPL. In the case of the PIPL, a designated representative or dedicated entity established within the PRC shall apply for the PIPC.

Before applying for the PIPC, the data processor and overseas recipient shall conclude a legally binding document, appoint a person responsible for data protection, establish a data protection department, formulate PI cross-border processing rules, and conduct a PI protection impact assessment.

At the publication date of this article, neither qualified institutions nor the certification process have been specified. It is also not clear whether the PIPC constitutes a legal basis for cross-border transfers of PI under PIPL. Therefore, using PIPC as a mechanism for PI cross-border transfer in practice remains unclear for now and requires further clarification.

3. Standard Contract

The third option for cross-border data transfer, especially relevant to SMEs, is the conclusion of a contract with the overseas recipient according to the Standard Contract. Similar to the PIPC, this option is applicable to the cross-border transfer of PI only, and under the condition that a data export security assessment is not required.

On June 30, 2022, the CAC issued the Draft Provisions on the Standard Contract for Outbound Transfer of Personal Information for public comments ("Draft Provisions"), which stipulates the minimum content of Standard Contracts. Further contents are specified in the template attached to the Draft Provisions providing definitions, obligations of the data transferor and the overseas recipient, data subject's rights, liabilities for the Standard Contract breach, applicable law and dispute resolution, etc. Parties may agree on further contents, which shall not contradict the minimum content of the Standard Contract.

Apart from concluding a Standard Contract, the data processor shall conduct a PI protection impact assessment, draft an assessment report, and file it together with the effective Standard Contract with the CAC on a provincial level, before transferring PI to a recipient outside the PRC.

The Standard Contract shares many similarities with the standard contractual clauses under the GDPR ("EU-SCC"), but also differ in some respects and leaves some key questions unsolved, such as the form and content of the Standard Contract, governing laws, and jurisdiction. According to the Draft Provisions, other contracts signed between the PI processor and an overseas recipient must not conflict with the Standard Contract. This might be a challenge, especially in terms of the coexistence of a Standard Contract and the EU-SCC.

Conclusion

Chinese subsidiaries transferring data to their overseas parent companies, which save or mirror such data on their servers hosted outside of the PRC or provide their parent companies access to their data stored in the PRC, shall assess if and which of the three above-described options fits best to their data processing activities.

In the first step, Chinese subsidiaries shall analyze the data to be transferred to or to be made accessible by their overseas parent companies, including data classification, data quantification, and cross-border data flow analysis, to find out whether such data is permitted to be transferred to or accessed by the recipient outside of the PRC with or without any restrictions.

Most of the foreign-invested SMEs in the PRC, especially smaller manufacturing enterprises, are unlikely to be classified as "critical information infrastructure operators" or to meet the thresholds for PI cross-border transfers under the Measures. However, foreign-invested SMEs may also, regardless of the amount of data transferred to their overseas parent company, be required to apply for a data export security assessment when transferring "important data" overseas. For this reason, it is essential that SMEs verify if they transfer "important data" abroad. In this case, they need to pay attention to the 6-months deadline for the data export security assessment application.

Fines of up to RMB 50 million or 5% of the annual turnover can be imposed on companies violating cross-border data transfer regulations. The "responsible person" and "other directly responsible persons" can be given a fine of up to RMB 1 million and can be held liable under the PRC Criminal Law.

Rainer Burkardt is the Founder and Managing Director of the PRC-licensed law firm Burkardt & Partner Rechtsanwälte in Shanghai. Having been living and working in China for 24 years, Mr. Burkardt belongs to the few German lawyers who possess long-lasting, on-the-ground China experience. His expertise lies in providing practical legal advice predominantly to SMEs from Austria, Germany, and Switzerland on their investments in China.

Ondrej Zapletal is a legal advisor at Burkardt & Partner in Shanghai. He studied PRC Civil and Commercial Law at the Shanghai East China University of Political Science and Law and advises foreign companies on their investments and business in the PRC. His focus lies mainly on Chinese commercial law and data protection law.