中倫律師事務所
ZHONG LUN LAW FIRM

A Practical Guide: How to make China's SCC work for your business

Peng Cai, Pulingling Xiao, Yunlang Hu

Article 38 of the *Personal Information Protection Law* stipulates four compliance paths for cross-border transfer of personal information, namely: (1) passing the security assessment organized by the Cyberspace Administration of China (the "**CAC**"); (2) obtaining the protection certification by a specialized agency; (3) entering into a standard contract formulated by the CAC; and (4) meeting other conditions set forth by laws and administrative regulations and by the CAC.

On 24 February 2023, the CAC issued the *Measures for Standard Contract for Cross-border Transfer of Personal Information* (the "**Measures**"), which officially announced the implementation of the third path of the "four paths" for cross-border transfer of personal information. In light of our practical experience, this article analyses the key elements of the *Standard Contract for Cross-border Transfer of Personal Information* (the "**Standard Contract"**), with the aim of assisting relevant enterprises in carrying out compliance work on cross-border data transfer.

1. CHARACTERISTICS OF THE STANDARD CONTRACT

(1) Standard Terms Recognized by the Chinese Government

As the cornerstone of contract law in modern society, the principle of "autonomy" is well recognized in legislation and case laws of most countries and in international treaties. In general, the parties have the liberty to determine the majority of the commercial arrangements in a contract, unless such determination is invalidated by mandatory rules. In contrast to freely negotiated contract terms, there are take-or-leave contracts with non-negotiable standard terms. Standard contracts were originally created by one of the parties with the aim of improving transaction efficiency and providing standardized services. Later, in order to balance the position of each party during the transaction and to protect the interests of parties with less bargaining power, standard contracts were

formulated and issued by the Chinese government. Previously, China also issued the *Guidelines on the Content and Form of Specific Asset Management Contracts* and the *Guidelines on the Specification of Standard Clauses in Online Trading Platform Contracts*, which require standard terms to be included or specified in contracts in certain areas.

By far, the Standard Contract has undoubtedly the most stringent standard terms and conditions under the current legal system of China. With complete and comprehensive content, the Standard Contract requires the domestic personal information processor and the overseas recipient to strictly comply with the standard terms and conditions provided by the CAC in the execution and performance of the Standard Contract. When entering into a Standard Contract or a supplemental agreement, companies should be aware of two prongs of the "no conflict" requirements:

- First prong: If the parties enter into any supplemental agreements, the additional terms and conditions shall not contradict the standard terms and conditions of the Standard Contract. According to Article 6 of the Measures and the Official Q&A, only the CAC has the right to revise the standard terms and conditions of the Standard Contract. Therefore, enterprises may execute other terms and conditions when signing a Standard Contract, but such additional terms and conditions are invalid if they conflict with the standard terms and conditions of the Standard Contract. In other words, the standard terms take precedence over any other terms agreed by the parties.

- Second prong: Other "legal documents" binding on the parties must not conflict with the Standard Contract. According to Article 9(1) of the Standard Contract, the Standard Contract takes precedence over any other "legal documents" signed by the parties. In other words, if the Standard Contract comes into force with the signatures of both parties, the Standard Contract takes precedence over any other agreement or policy between the parties.

In view of the two prongs of the "no conflict" requirements, the Standard Contract, although it takes the form of a "contract", does not particularly carry with the concept of "statutory empowerment". On the contrary, the Standard Contract leaves rather limited room for the parties to negotiate freely.

(2) Administrative Record-filing

In addition to the requirements on the standard terms of the Standard Contract, the personal information processors is also obliged to file the executed Standard Contract with the provincial-level CAC office at the place where the personal information processor resides. Such filing must be made within 10 working days after the Standard Contract comes into effect.

The Standard Contract is not the only contract subject to record-filing. In the areas of patent and trademark licensing and construction projects, record-filing is often an effective means of protecting the rights of the contracting parties against any third parties. However, the Standard Contract differs from these contracts due to the administrative nature of its record-filing requirement. Pursuant to the relevant provisions of the Measures and the Personal Information Protection Law, failure to comply with the record-filing obligation of the Standard Contract may result in penalties including, but not limited to, warning, fine, revocation of business license, and publication of credit file records; if a crime is committed during such failure, criminal liability shall be investigated in accordance with law.

In addition, it should be noted that the record-filing of a Standard Contract is not completed once and for all. The personal information processor must initiate the record-filing for the Standard Contract when one or more of the following conditions occur.

- The purpose, scope, category, sensitivity, method, and storage location of personal information transferred abroad, or the purpose and method of personal information processing by the overseas recipient has changed, or the retention period of personal information located abroad is extended;

- The personal information rights and interests will be affected by the changes in the policies and regulations on personal information protection in the country or region where the overseas recipient is located;
- Other circumstances that may affect the rights and interests of personal information subjects.

Considering the above conditions triggering another round of mandatory recordkeeping, it is recommended that the contracting parties allow for some leeway in the implementation of the Standard Contract by foreseeing or anticipating possible changes that are likely to occur after the personal information is transferred abroad. In addition, when the Standard Contract comes into force, companies should also establish internal and external procedures to closely monitor the personal information processing and changes in the legal environment where the overseas recipient is located, so as to prevent illegal consequences caused by failure to conduct another round of mandatory record-filing in a timely manner.

(3) Contract for the Third-party Beneficiary

The Standard Contract sets out rights and obligations among three parties, namely: the obligations of the domestic personal information processor, the obligations of the overseas recipient, and the rights of and remedies available for a personal information subject. The domestic personal information processor and the overseas recipient enter into and perform the Standard Contract as the contractual parties, while any of the personal information subjects, as a third-party beneficiary, is also granted the corresponding rights through the agreement reached between the contracting parties.

In principle, based on the doctrine of privity, contractual rights, and obligations are usually negotiated between the contractual parties. A contractual party may only make a claim or file a lawsuit against the other party, and may not, at its discretion, claim against or create obligations for a third party who is not in privity to the contractual party. However, for the protection of the personal information subjects, the Standard Contract directly incorporates the spirit of Article 522 of the *Civil Code* concerning the third-party beneficiary, granting a personal information subject the right to sue

the personal information processor and the overseas recipient in an individual capacity. In addition, the Standard Contract recognizes the joint and several liabilities, which expand the choices for a personal information subject to exercise his/her rights when litigating against the personal information processor or the overseas recipient. In particular, it should be noted that rights and obligations created by contracts are highly recognized in mainstream countries. Therefore, during extraterritorial litigations, it is undoubtedly a better choice for a personal information subject to establish claims based on the Standard Contract, so that he/she can exercise remedial actions to protect his or her rights against the overseas recipient directly.

2. SCENARIOS FOR THE APPLICATION OF THE STANDARD CONTRACT

When the *Security Assessment Measures for Outbound Data Transfer* was introduced in 2022, we published an interpretation article entitled "Planning before Moving, Gaining after Knowing When to Stop - How to Effectively Choose Data Cross-border Solutions for Enterprises under all Three Laws" to analyze and explain typical scenarios of the three paths of cross-border data transfer applicable to enterprises with the purpose of helping them choose the appropriate path of cross-border data transfer. Considering the provisions of the Measures, the Standard Contract is likely to be applicable in the following two scenarios:

(1) Cross-border Transfer of Personal Information for Small and Medium-size Enterprises

According to the Measures, the application of the Standard Contract is premised on satisfying all four conditions: (1) the personal information processor is not a critical information infrastructure operator; (2) in the aggregate, the personal information processor processes personal information of fewer than one million people; (3) the personal information processor provides personal information to foreign countries of less than 100,000 people in total within two years; and (4) the personal information processor provides sensitive personal information to foreign countries of less than 10,000 people in total within two years. In other words, the application scope of the Standard

Contract is supplemental to the application scope of *Security Assessment Measures for Outbound Data Transfer*, and enterprises can choose to apply the Standard Contract for outbound data transfer only if they are not under mandatory obligation to declare a security assessment.

Considering the business realities and the wide varieties of personal information processors, the number of users hosted by domestic internet enterprises or TO-C-type large and medium-size enterprises generally exceeds one million; secondly, enterprises that value intellectual property rights and have high R&D investment ratio often control important data (e.g. automobile data) or a large amount of sensitive personal information (e.g. facial recognition data), which is highly likely to fall into the regulation scope of the *Security Assessment Measures for Outbound Data Transfer*s; moreover, there is a greater possibility of large-scale defense enterprises, telecommunication companies, financial institutions, and medical institutions constituting critical information infrastructure operators due to their industrial nature and status, and such entities are therefore excluded from the application scope of the Standard Contract.

Therefore, the majority of eligible subjects for the Standard Contract will be small and medium-size enterprises, and its application scope will be limited to the transfer of a small amount of personal information or sensitive personal information.

(2) Cross-border Investment and M&A Transactions

During cross-border investment and M&A transactions, when the target company is a foreign enterprise, the majority of the personal information will be transferred inbound from overseas to the Chinese mainland. Therefore, only a limited amount of personal information needs to be transferred abroad and such transfer can often be completed through a one-off transaction. In this scenario, we recommend that domestic enterprises choose the Standard Contract as the compliance path for cross-border transfer of personal information.

Undoubtedly, for cross-border transactions involving the two-way transfer of personal information, the buyer and the seller should follow the data privacy laws of the countries where they are incorporated or operate. Considering that negotiation and execution of a Standard Contract will

create an additional hurdle to the transaction, how to negotiate a valid and agreeable contract will also be the key issue under the cross-border investment and M&A transactions scenario.

(3) Inapplicable Scenarios

In particular, the Measures states that the personal information processor may not circumvent the mandatory security assessment and utilize the Standard Contract instead for outbound data transfer by means of volume splitting, among others. As such, it is safe to conclude that it is illegal under the laws for group companies to reduce the amount of personal information to be transferred abroad by means of splitting and categorizing a certain volume of personal information to its subsidiaries to circumvent the security assessment. Instead of praying for escaping punishment, enterprises shall genuinely and strictly assess the amount of personal information to be transferred abroad.

3. COMPLIANCE ADVICE ON THE APPLICATION OF THE STANDARD CONTRACT

The Standard Contract, encompassing extensive topics, is way more than a regular contract. From the perspective of the full-scale performance of the contract, we believe that the Standard Contract sets a very high bar of obligations for contractual parties to fulfill. From the perspective of a domestic personal information processor, we would like to suggest enterprises take three "early" steps to timely and effectively utilize the Standard Contract for cross-border data transfer.

(1) Clarifying Data Assets and the Number of Personal Information Subjects as Early as Possible

The Measures will come into effect on June 1, 2023 (the "**Implementation Date**"). Enterprises that have already conducted cross-border personal information transfer activities before the Implementation Date but have not fulfilled the obligation of signing a Standard Contract should complete the rectification within six months from the Implementation Date. In other words, the grace period for rectification under the Standard Contract will last until December 1, 2023.

Per our abundant experience in security assessment of cross-border data transfer, the supervisory authorities will generally require eligible enterprises to complete the rectification as early as possible, so that such enterprises can declare and receive the acceptance notice before the deadline. Therefore, in terms of the record-filing process of the Standard Contract, it is reasonable to assume that enterprises should allow for sufficient time to confirm the appropriate path and prepare relevant material. We strongly advise against the practice of submitting the report on or shortly before December 1, 2023.

We recommend that enterprises shall, as soon as possible, conduct a clear and comprehensive review of their data assets and the scenarios of cross-border transfer, and then determine a compliance path for cross-border transfer of personal information.

(2) Pushing the Negotiation and Execution of the Standard Contract Forward as Early as Possible

The implementation of the Standard Contract does not proceed easily.

First, the overseas recipients are usually foreign organizations working in their native language. At present, the Chinese government has not yet issued an official English translation of the Standard Contract. Considering the stringent restrictions imposed by the CAC on the Standard Contract's formative terms, it may take some time for the contractual parties to clarify the contract's content term by term in order to reach a consensus.

Second, the compulsory nature of the Standard Contract may affect the ongoing or planned commercial arrangements of the enterprises involved, and the contractual parties should properly negotiate while factoring in a foreseeable change to the commercial arrangements.

Third, in scenarios involving the two-way cross-border transfer of personal information, the domestic personal information processor may be confronted with the requirement to sign an "overseas" version of the SCC or to cooperate with the overseas recipient to fulfill compliance obligations under foreign laws. The domestic personal information processor should carefully assess whether other documents it signs or compliance obligations it performs are contrary to the compulsory requirements of PRC laws, including the Measures.

Finally, under the Measures, the personal information processor is required to submit an assessment report on the impacts on personal information protection when the Standard Contract is filed for record-keeping. The domestic personal information processor will consider matters concerning the assessment of the impacts on personal information protection when moving forward the signing of the Standard Contract.

To sum up, enterprises that choose to apply the "Standard Contract" path for cross-border data transfer should advance the negotiation and execution of the contract as soon as possible, reserving sufficient time to prepare for the execution of the Standard Contract.

(3) Deploying the Enterprises' Internal Control Measures Required for the Standard Contract as Soon as Possible

The Standard Contract is both a product of autonomy and legal requirement from compliance supervision. Before signing a Standard Contract, enterprises should ensure that they can fulfill the obligations prescribed by the standard terms and bear the burden of proof to evidence their compliant performance of contractual obligations. We have summarized six compliance measures that shall be taken by the domestic personal information processor:

a) fulfilling the obligation to inform

The domestic personal information processor is obligated to fulfill its obligations to inform. Except for cases where the obligation to inform is not required by laws and administrative regulations, the domestic personal information processor shall inform the personal information subjects of the following items:

- The name of the overseas recipient, contact information, the purpose of processing personal information transferred abroad, the method of processing, the type of personal information, the retention period, and the method and procedure for exercising the rights of a personal information subject, and other matters;
- A personal information subject is a third-party beneficiary of the Standard Contract and may enjoy the rights of a third-party beneficiary pursuant to the Standard Contract;
- If a domestic personal information processor plans to provide sensitive personal information abroad, it shall also inform the personal information subject of the necessity of providing sensitive personal information and the impact on personal rights and interests.

b) having a legal basis

Article 13 of the *Personal Information Protection Law* stipulates seven categories of legal bases for the processing of personal information. A domestic personal information processor may carry out personal information processing activities of, including cross-border transfer of personal information, if and only if it has a legal basis.

In the case of "consent" as the legal basis, the domestic personal information processor is required to obtain the separate consent from the personal information subject. The so-called "separate consent" excludes overall consent, general consent, and one-click-

tick consent. Therefore, in situations where the processing activities are subject to more stringent supervision, such as cross-border transfer of personal information, we recommend that enterprises obtain explicit separate consent from the personal information subjects in writing. In the case of cross-border transfer of personal information involving minors under the age of 14, the domestic personal information processor shall obtain separate consent from the parents or other guardians of each minor.

Additionally, written consent shall be obtained if laws and administrative regulations stipulate as such. For example, the *Administrative Regulations on Credit Investigation Industry* stipulates that credit institutions shall obtain the written consent from individuals when collecting information concerning income, deposit, securities, commercial insurance and real estate and information on tax payment amount; the *Administrative Regulations on Human Genetic Resources of the People's Republic of China* stipulates that the written consent from the provider of human genetic resources shall also be obtained when human genetic resources are collected within the PRC. For the scenario of cross-border transfer of the personal information mentioned before, the written consent of the personal information subject should also be obtained per our understanding.

c) prudently selecting the overseas recipient and making proper assessment records

According to the Standard Contract, the overseas recipient should have an adequate security management system, technical measures, and safeguarding capabilities, and must meet the personal information protection standards stipulated in relevant laws and regulations of China. Therefore, the selection of a competent overseas recipient is crucial to the implementation of the Standard Contract.

In the scenario of a "passive" cross-border transfer of personal information due to the international third-party supply chains, the domestic personal information processor is usually granted more power in the selection of qualified hardware or software suppliers, and we recommend that the processor should assess in detail the relevant qualifications of the overseas recipient (hardware or software supplier); in the scenario where the data processor "actively" transfers personal information abroad, the processor should negotiate with the overseas recipient properly, and guide and help the overseas recipient to establish a security management system and improve its technical security capabilities to meet the requirements of the Standard Contract.

Specifically, the domestic processor can assess the overseas recipient from the following aspects:

- Whether technical measures such as encryption, anonymization, de-identification, etc. are adopted;
- Whether any mechanisms are designed to carry out regular checks to ensure the security of personal information to be transferred abroad;
- Whether the obligation to keep confidentiality is imposed in any form on the personnel of the overseas recipient who is authorized to process personal information;
- Whether the minimum authorization of the rights of access is required;
- Whether there is any relevant prior experience in cross-border transfer and processing of personal information;
- Whether there have been incidents relating to the security of personal information and whether they have been handled promptly and effectively;

- Whether it has received a request to provide personal information from the public authority of the country or region where it is located, and how the overseas recipient has responded to the request.

d) assessing the impact of the legal environment of the country/region where the overseas recipient is located on the performance of the contract

An assessment of the legal environment where the overseas recipient is located constitutes an inextricably important term of the Standard Contract as indicated in the following aspects:

- The personal data processor has the right to immediately terminate the contract if the overseas recipient's compliance with the Standard Contract violates the laws and regulations of the country or region where it is located;
- The personal information processor has the right to suspend cross-border transfer until the breach is rectified or the Standard Contract is rescinded if a change in the legal environment where the overseas recipient is located makes it impossible for it to perform the contract.

Therefore, a comprehensive and proactive assessment of the legal environment where the overseas recipient is located prior to the signing of the Standard Contract is essential for the full and continuous performance of the Standard Contract. The domestic personal information processor should consider the following elements in the assessment:

- Present laws, regulations, and generally applicable standards with respect to personal information protection in the country/region where the overseas recipient is located, including any requirements to provide personal information or regulation authorizing access to personal information by public authorities;

- Regional or global organizations of which the overseas recipient's country or region is a member with respect to the protection of personal information, and binding international commitments that the overseas recipient's country or region has made;
- The mechanism for promoting the protection of personal information in the country or region where the overseas recipient is located, such as the existence of supervisory and enforcement bodies and relevant judicial bodies for the protection of personal information, etc.

In addition to the above three elements, we recommend that the domestic personal information processor further refers to previous cases or enforcement records to determine whether there is a greater likelihood that an overseas judicial or regulatory body will find a contract governed by Chinese law to be at risk of being invalid.

e) establishing a mechanism for the personal information subject to exercise his/her rights

Prior to signing the Standard Contract, the domestic personal information processor should establish effective mechanisms for a personal information subject to enforce his or her rights in the following aspects:

- Ensuring the personal information subject's rights to be informed, make decisions, restrict or refuse the processing of his or her personal information by others, and rights to access, copy, correct, supplement and delete his or her personal information;
- Explaining to the personal information subject regarding the rules for processing personal information by both contractual parties;

- Establishing effective communication channels with the overseas recipient regarding the personal information subject's exercise of his or her rights. When the personal information subject directly exercises his or her rights against the overseas recipient, or when the domestic personal information processor is unable to comply with the request of the personal information subject to exercise his or her rights, it can inform the overseas recipient and request its assistance to do so.

f) completing the impact assessment of personal information protection

According to the provisions of the Measures, the record-filing materials of a Standard Contract include the assessment report on the impacts on personal information protection, and the personal information processor is responsible for the authenticity of the filed materials.

By summarizing the key requirements of the Measures on the impact assessment of personal information protection, it is not difficult to find that the nature of the requirements is similar to the obligations imposed by the parties in the Standard Contract. Therefore, the process for the domestic personal processor to negotiate and facilitate the signing of contracts and deploy the internal control measures of compliance is in essence about conducting the impact assessment of personal information protection with respect to its cross-border processing activities of personal information.

To promptly provide a true, complete, and accurate assessment report on the impacts on personal information protection, enterprises that have businesses related to cross-border transfer of personal information should promptly conduct due diligence and compliance analysis of the entire process of cross-border processing of personal information and complete relevant rectification work.

Conclusion:

With the promulgation of the *Provisions on the Procedures for Administrative Law Enforcement by the Cyberspace Administration Authority of Various Levels* and other regulations, 2023 marks the "commencement of law enforcement" in this particular area. With the administrative enforcement procedures on which the CAC is acting as the main body of law enforcement to be implemented,

the CAC will reinforce administrative enforcement against illegal data activities. In the official version of the Measures and the Standard Contract, the penalties against non-compliant activities have been amended by replacing the term "prohibiting cross-border activities" originally provided in the draft for public comments with "summoned by authorities for talks or rectification". Nevertheless, we believe that this amendment is only made to comply with the legislative rules stipulated in the *Administrative Penalty Law*, rather than a "mitigation measure" for relevant violations.

The official promulgation of the Measures and the Standard Contract means that the last piece of regulations is in place to govern cross-border transfer of personal information. Enterprises should follow the compliance path applicable to their own cross-border volumes to fulfill their declaration or record-filing obligation. Enterprises with the needs for or find themselves in the scenarios of cross-border data transfer shall not suffer from an "Achilles' heel" in data compliance caused by their failure or delay in rectifications.