

Legal Commentary

June 1, 2023

CAC Releases Guidelines for China SCC Filings

Authors: Kevin DUAN | Kemeng CAI | Lian XU

On May 30, 2023, the Cyberspace Administration of China (the “**CAC**”) released the *Guidelines for Filing Standard Contract for the Outbound Transfer of Personal Information (First Edition)* (the “**Filing Guidelines**”). The Filing Guidelines provide operational guidance for enterprises planning to transfer personal information from China to overseas recipients by relying on the Standard Contract for the Outbound Transfer of Personal Information (the “**China SCC**” or “**Standard Contract**”) safeguard and marks the formal adoption of the Standard Contract for personal information exports.

The Standard Contract has attracted widespread interest due to its broader applicability and flexibility compared to the two other data export compliance safeguards, the CAC data export security assessment (“**CAC Security Assessment**”) and personal information protection certification. The previously introduced *Measures for the Standard Contract for Outbound Transfer of Personal Information* (the “**Measures**”) only provide principled provisions on the filing and personal information protection impact assessment (“**PIA**”) report that needs to be submitted together with the filing. The Filing Guidelines offer clarity on these two steps for the first time.

The Filing Guidelines contain two unexpected developments—submitted filings are subject to review and may be rejected under some circumstances; and the content required in the PIA has not been substantially simplified relative to that for the CAC Security Assessment. Both of these developments have raised concerns among practitioners and relevant enterprises about failing to complete the filing in a timely manner, which increases the uncertainty of adopting the Standard Contract safeguard. The Measures, which came into effect on June 1, stipulate a rectification period of six months which ends on November 30, 2023. Therefore, for enterprises intending to adopt the Standard Contract safeguard, it is advisable to begin preparing the Standard Contract filing materials soon to ensure both timely filing and the continuity of personal information exports.

In [our previous articles](#), we analyzed the Measures and the key points of the China SCC. In this article, we analyze the specific requirements outlined in the Filing Guidelines with our experience with CAC Security Assessment to offer our observations and views on issues that have not yet been addressed in the Standard Contract filing process.

Filing requirements

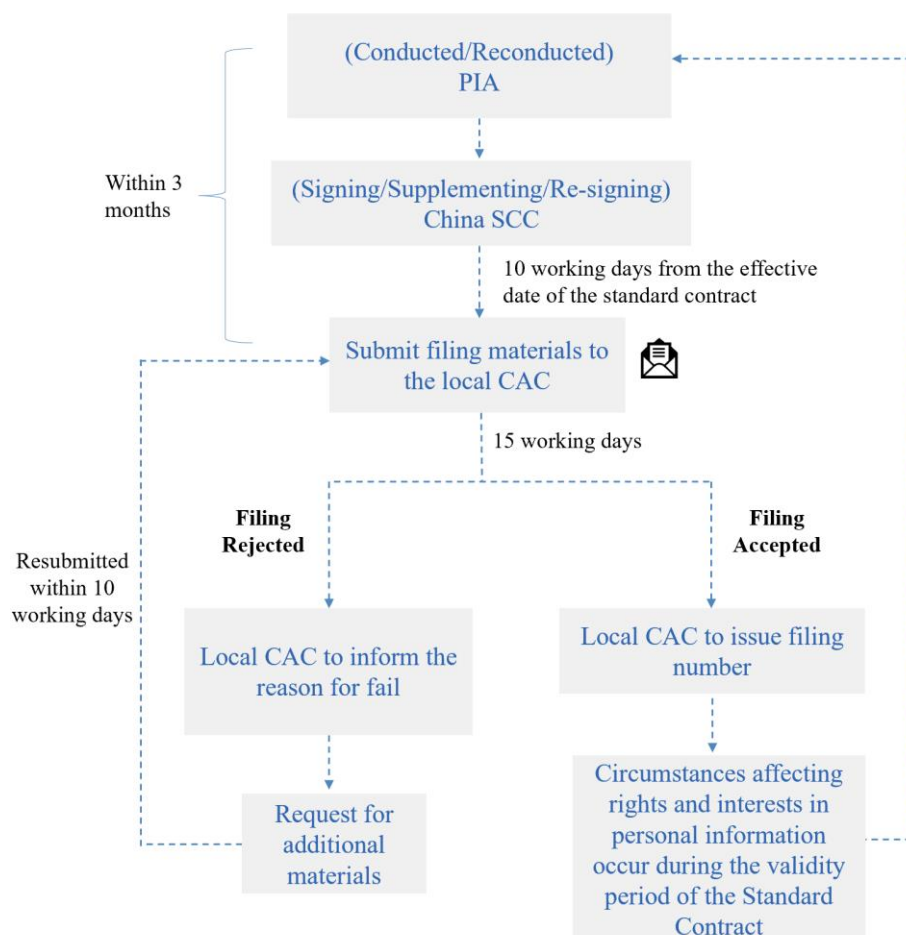
Regarding the filing requirements for Standard Contracts, the Filing Guidelines further specify the following points based on Article 7 of the Measures:

- Filing Time: Within 10 business days from the effective date of the Standard Contract.
- Filing Format: Submit written materials and electronic versions of the materials.
- Filing Authority: Provincial-level Cyberspace Administration (“**local CAC**”) where the personal information handler is located.

Based on current CAC Security Assessment practices, the authority to receive the Standard Contract filing materials is generally the local CAC where the filing applicant is registered. The electronic version of the materials usually refers to editable document files on a compact disc.

Filing process

Regarding the filing process for Standard Contracts, the Filing Guidelines divide the filing process into steps including applicant material submission, CAC material verification, CAC feedback of filing results, and applicant supplementation or re-filing. The key points of this process are presented in the flowchart below.



I. PIA must be completed within three months of filing

The Filing Guidelines contain a template “Letter of Undertaking” which explicitly requires the PIA to have been completed within three months of successfully submitting the filing materials with the local CAC. No significant changes to matters addressed in the PIA should occur before or during the filing process.

Based on current CAC Security Assessment practices, when initially submitting filing materials, filing applicants are usually able to ensure that the PIA has been completed within this three-month period. **However, this three-month period may be exceeded if the filing applicant is required to supplement its filing materials, especially for multiple rounds. In such cases, the filing applicant may need to conduct additional PIA work.**

II. Time limit for filing review

According to the Filing Guidelines, the local CAC will verify the filing materials within 15 working days of receipt and notify the filing applicant of the result. If the filing applicant is requested to supplement the materials, it should do so within ten working days. Thereafter, the local CAC will have an additional 15 working days to verify the materials.

According to the above provisions, a filing applicant can obtain a filing approval within 15 working days if it is not required to supplement its filing materials. However, if supplementation is required, it may take at least 40 working days to obtain the filing result. Based on current CAC Security Assessment practices, assessment applicants have often been required to supplement their security assessment materials. Given this, filing applicants may need to consider reasonably extending the authorization period of their agents tasked with handling the filing materials.

III. Circumstances for supplementing or re-filing

The Filing Guidelines reaffirm the provisions of the Measures and state that if the following circumstances occur during the validity period of the Standard Contract, the personal information handler should conduct a new PIA, supplement or re-execute the standard contract, and fulfill the corresponding filing procedures:

- There are changes in the purpose, scope, type, sensitivity, method, storage location of personal information transferred to overseas recipients, or in the purposes and methods of personal information processing by the overseas recipients, or an extension of the period for retaining personal information overseas;
- Changes occur in the personal information protection policies and regulations of the country or region where the overseas recipients are located, which may affect the rights and interests of personal information subjects;
- Other circumstances that may affect the rights and interests of personal information subjects.

The Filing Guidelines further specify that if supplementary materials need to be provided, the filing applicant should submit the supplementary materials to the local CAC. If a new standard contract

needs to be executed, it should be re-filed. However, there is no clear boundary between circumstances requiring supplementary materials and those requiring the re-filing of a Standard Contract. It is also unclear whether filing applicants have the discretion to make the judgment by themselves. Further clarification may be needed in this regard.

Materials to be submitted for filing

Compared to Article 6 of the Measures, the Filing Guidelines further detail the materials to be submitted for the Standard Contract filing, which include the following.

I. Photocopies of:

- The filing applicant's Unified Social Credit Code certificate;
- The legal representative's government-issued identification;
- The agent's government-issued identification;

II. Documents (templates provided):

- Authorized power of attorney for the agent;
- Letter of undertaking;
- Standard contract;
- PIA report.

We note the following key points with respect to these materials.

1. Simplification of required materials

Compared to the *Guidelines for the Security Assessment of Outbound Data Transfer (First Edition)* issued by the CAC on August 31, 2022, filing the Standard Contract does not require an application form and other related supporting documents. However, since the Filing Guidelines still give the local CAC the discretion to conduct supplementary inspections, it is possible that filing applicants may need to submit such supporting documents in practice.

2. Third-party institutions involved in PIA work required to stamp the PIA report

In the filing material templates provided in the Filing Guidelines, the PIA Report Template explicitly requires third-party institutions involved in preparing the PIA work to provide their basic information and participation in the PIA process. Such institutions should affix their official seals on the relevant pages.

3. PIA report focuses on the impact on personal information rights and interests

The PIA Report Template provided in the Filing Guidelines is similar in content to the Data Export Risk Self-Assessment Report Template provided in the *Guidelines for the Security Assessment of Outbound Data Transfer (First Edition)* issued by the CAC on August 31, 2022. **The core difference lies in the**

fact that the self-assessment for data exports focuses more on the impact of data exports on national security and public interests, while the PIA focuses on the impact on personal information subject rights and interests. Specifically, it includes:

- Explanations regarding the processing of sensitive personal information and the use of personal information for automated decision-making;
- Explanations regarding whether personal information is to be transferred to third parties; and
- Explanations regarding how both parties ensure the implementation of Standard Contract clauses.

Considering that the assessment points and granularity of the PIA Report Template are similar to the Data Export Risk Self-Assessment Report Template, and no substantial simplification has been made, we recommend that enterprises that intend to submit filings to conduct comprehensive mapping and review of their data processing activities and to begin arranging for rectification in order to complete the filing by the end of the rectification period, which is November 30, 2023.

Our observations and perspectives

The release of the Filing Guidelines provides guidance and assistance for personal information handlers to carry out Standard Contract filing work in a standardized and orderly manner. However, in light of current CAC Security Assessment practices, the following issues still require clarification from the CAC in the subsequent filing process.

I. Can affiliated entities file jointly?

The Filing Guidelines and the Measures do not specify whether joint filings are permitted, e.g., whether affiliated entities within a group may designate one entity, such as the Chinese holding company, to submit a filing on their behalf. Based on current practices, whether joint filings may be made will likely depend on the specific facts and circumstances, taking into consideration factors such as equity relationships, information system relationships, business relationships, data sharing, and data flows between the entities.

II. What is the relationship between the Standard Contract and IGDTAs?

Multinationals often already have intra-group data transfer agreements (“**IGDTAs**”) to facilitate cross-border data transfers within the group. These multinationals usually want to utilize existing IGDTAs as much as possible or include the scenarios of providing personal information from China to overseas recipients into their existing IGDTAs. However, according to the Measures, the Standard Contract must be executed strictly in accordance with its terms. Therefore, an IGDTA cannot replace the China SCC for personal information cross-border transfers from China. As long as the content of the IGDTA and the provisions of the China SCC do not conflict, personal information handlers and overseas recipients can include the IGDTA as an appendix to the China SCC or explicitly specify the scope and effectiveness of the China SCC for personal information cross-border transfers from China by referencing it in the IGDTA.

III. Can entrusted parties sign Standard Contracts?

Unlike the EU Standard Contractual Clauses, the current China SCC template does not provide different terms based on the legal status of the contracting parties, e.g., whether they are personal information handlers or entrusted processors. In this respect, it appears that the eligible contracting parties are limited to a domestic transferor that is a personal information handler (i.e., a “data controller” under GDPR) and an overseas recipient that is either a personal information handler or an entrusted processor (i.e., a “data processor” under GDPR). However, based on our CAC Security Assessment experience, the CAC has not sought to distinguish whether the domestic transferor is a personal information handler or an entrusted party. Moreover, in practice, there are often circumstances where a domestic entrusted party transfers personal information to an overseas personal information handler (entrusting party) or the domestic entrusted party transfers personal information to an overseas entrusted party. Non-compliant cross-border transfers may result if these parties are not eligible to act as parties to the Standard Contract. Therefore, we believe that a domestic transferor that acts as an entrusted party may still be able to rely on the Standard Contract safeguard when transferring personal information to an overseas recipient.

IV. Is the review of the filing materials a formality or can it be more substantive? Will a rejected filing affect the transfer of personal information to overseas recipients?

The Filing Guidelines state that a submitted filing can result in either a “pass” or a “fail”, which suggests that the regulatory authorities may substantively review the filing materials. However, neither the Filing Guidelines nor the Measures specify any form of penalty for filing applicants whose filings are rejected. Furthermore, according to Articles 6 and 7 of the Measures, completion of the filing process is not a prerequisite for the effectiveness of the Standard Contract, and a personal information handler is entitled to transfer personal information overseas upon the effectiveness of the Standard Contract.

While it remains unclear, we take the view that a rejected filing could result in an order to halt personal information export activities or other administrative penalties. This is because a rejected filing may indicate the filing applicant has non-compliance issues with respect to the PIA or its executed Standard Contract does not conform to the requirements of the Measures, either of which may constitute a violation of the *Personal Information Protection Law*.

With the Measures coming into effect on June 1, 2023, the countdown to the close of the six-month rectification period has officially begun. From a CAC Security Assessment perspective, it takes substantial time to carry out PIA work, conduct research and sort out data export information, prepare PIA reports, and negotiate with overseas recipients to sign China SCC. Therefore, enterprises that intend to rely on the Standard Contract safeguard for their personal information exports are recommended to begin undertaking this work soon to ensure the legal compliance of their personal information export activities.

Important Announcement

This Legal Commentary has been prepared for clients and professional associates of Han Kun Law Offices. Whilst every effort has been made to ensure accuracy, no responsibility can be accepted for errors and omissions, however caused. The information contained in this publication should not be relied on as legal advice and should not be regarded as a substitute for detailed advice in individual cases.

If you have any questions regarding this publication, please contact:

Kevin DUAN

Tel: +86 10 8516 4123

Email: kevin.duan@hankunlaw.com