



7 Steps to Success: China Releases New Guidelines on Standard Contracts for Exporting Personal Information

Insights

7.06.23

Chinese government data privacy officials recently implemented Guidelines for Filing of Standard Contracts for Export of Personal Information that carry significant consequences for non-compliance – which means organizations that do business in China need to get up to speed right away. The Cyberspace Administration of China (CAC) implemented the new guidelines on June 1, following up on the Measures on Standard Contracts for the Export of Personal Information released in February. Together, they define the scope of application of contracts and prevent data controllers from separating data exports into different batches to avoid the security assessment mechanism. What do Personal Information Handlers need to know about the steps outlined in the Guidelines in order to comply with the new law? The seven steps are outlined below.

Step 1: Determine the Applicability of the Guidelines

The Measures and the Guidelines only apply if at least one of the following conditions is satisfied:

- the Personal Information Handler (PIH) transfers and stores personal information collected in domestic operations overseas;
- the personal information can be inquired, retrieved, downloaded, or exported by an organization outside China even though the information itself is generated, collected, and stored inside of China; or
- other export behaviors of personal information stipulated by the CAC.

Step 2: Judge Whether the Standard Contract Filing for Export of Personal Information Abroad Mechanism is Applicable

The PIH then must determine if it:

- is a non-critical information processor;
- is handling personal information of less than 1 million people;
- provided personal information to less than 100,000 people overseas since January 1 of the previous year; and

- provided overseas sensitive personal information of less than 10,000 people since January 1 or the previous year.

If the four criteria apply, the data controller should move on to Step 3 of the analysis.

Step 3: Assess the Impact on Personal Information Protection and Create Contract According to Standard Contract Template

The timing between step 3 and Step 4 is critical. You need to submit the filing materials within three months from the date of the completion of the assessment and within 10 working days from the effective date of the contract.

Step 4: Submit Filing Materials to the CAC at the Provincial Level

You then must submit the necessary materials to the CAC at the provincial level. The required materials include:

- a photocopy of the unified social credit code certificate;
- a photocopy of legal representative's ID card;
- a photocopy of the ID card of the person in charge;
- a letter of entrustment from the person in charge;
- a letter of commitment;
- the standard contract executed in Step 3; and
- the personal information protection impact assessment report generated in Step 3.

Step 5: Wait for the Provincial CAC to Inspect the Filed Materials

Within 15 business days, the data controller should hear back from the provincial CAC regarding whether the filing has been approved.

- If the filing is denied, the data controller will receive a notification regarding the unsuccessful record filing and the reasons for the denial. At this point, the data controller will have 10 days to correct the defect, which may require submitting additional materials.
- Depending on the circumstances during the validity period of the standard contract, it may be necessary to re-evaluate the impact of personal information protection, supplement or re-conclude standard contracts, and perform corresponding filing procedures.

Step 7: When the Filing Passes, the CAC Will Issue a Filing Number

After the filing passes, you may need to submit a supplementary re-filing of materials. Circumstances that would lead to such an event may include:

- Changes in the purpose, scope, category, sensitivity, method, and storage location of personal information provided overseas, or changes in the purpose and method of processing personal information by overseas recipients, or extension of the overseas storage period of personal information;
- Changes in personal information protection policies and regulations in the country or region where the overseas recipient is located may affect the rights and interests of personal information; or
- Other circumstances that may affect the rights and interests of personal information.

Consequences of Non-Compliance

Noncompliance with the filing requirements could expose data controllers to legal liability and penalties under the Personal Information Protection Law (PIPL). This law came into force in 2021 and regulates use of personal data by all companies operating in China, including international businesses. Liability under the PIPL could lead to penalties of up to RMB 50 million or 5% of the data controller's annual revenue.

What Should You Do?

If you have questions about the process or need assistance during any step along the way, contact your Fisher Phillips, the authors of this Insight, or any attorney in our [International Practice Group](#) or [Consumer Data Privacy Team](#). We will monitor these developments and provide updates as warranted, so make sure that you are subscribed to [Fisher Phillips' Insight System](#) to get the most up-to-date information directly to your inbox.

Related People



Nan Sato, CIPP/E, CIPP/C

Partner

610.230.2148

Email

Service Focus

Privacy and Cyber

International