LATHAM&WATKINS

Client Alert Commentary

Latham & Watkins Privacy & Cyber Practice

February 28, 2023 | Number 3055

China Clarifies the Personal Information Protection Certification Regime

China's SAMR and CAC jointly released new rules on the Certification regime for cross-border data transfers, outlining the standards for PI Processors to comply with.

Key Points:

- **Expanded Scope of Application:** The Certification Specification V2.0 clarifies that the Certification process applies to all cross-border transfers of personal information out of the PRC. In the previous version, the Certification process seemed applicable only to intra-group data transfers and transfers of personal information by foreign PI Processors.

- **Framework of the Certification Process:** The Certification Rules outline three primary stages for the Certification Process, i.e., (i) the technical inspection, (ii) on-site review, and (iii) post-certification supervision. The certification agencies will likely issue further practical rules and guidelines.

- **CCRC Appointed as First Certification Agency:** China Cybersecurity Review Technology and Certification Center (CCRC) has announced on its webpage that it has been designated as a Certification agency under the PIPL and will be accepting Certification applications via its online portal. As at the time of writing of this Client Alert, the CCRC is the only designated agency to issue a Certification.

Background

Certification Rules

On November 18, 2022, the State Administration for Market Regulation (SAMR) and the Cyberspace Administration of China (CAC) jointly released the *Notice Regarding Personal Information Protection Certification* attached with the *Implementation Rules of Personal Information Protection Certification* (Certification Rules) (see Chinese version). The Certification Rules clarify the application scope and procedure for obtaining a personal information protection certification (Certification) for the purposes of facilitating cross-border data transfers under the Personal Information Protection Law (PIPL).

Recap: Three Ways to Transfer Data Out of the PRC

The PIPL provides three mechanisms for a personal information processor (PI Processor) to transfer personal information outside of the mainland of the People's Republic of China (PRC):

1. **Security Assessment:** passing a CAC security assessment prior to undertaking the cross-border data transfer (Security Assessment). The assessment is mandatory if the PI Processor meets any of the thresholds set out in the *Measures for Cross-Border Data Transfer Security Assessment* (Security Assessment Measures);

2. **Certification:** obtaining a Certification from a CAC-designated certification agency; or

3. **China Standard Contractual Clauses:** concluding a contract with the overseas data recipient in accordance with the CAC's published standard contractual clauses (China SCCs). The China SCCs are currently in draft form, as set out in the *Draft Provisions on Standard Contract for Cross-border Transfer of Personal Information,* which the CAC published on June 30, 2022.

For a summary of the three mechanisms described above, please read Latham's previous Client Alert.

Comparison with the EU GDPR

This Client Alert focuses on the Certification mechanism, which is similar to the Binding Corporate Rules (BCR) and the certification scheme under the EU's General Data Protection Regulation (EU GDPR). The certification scheme under the EU GDPR is similar to the Certification under the PIPL as both processes involve a certification issued by accredited third party certification bodies and are ways for an organization to demonstrate that its processing of personal data complies with data protection requirements (including cross-border data transfer requirements) under the EU GDPR and PIPL, respectively. Article 46(2) of the EU GDPR specifically states that the certification scheme is a means to support transfers of personal data to third countries outside the EEA. However, in practice, no data transfer certification mechanisms have been approved to date; the standard contractual clauses or the BCR are more commonly relied upon.

The BCR is similar to the Certification under the PIPL as both regimes are designed to enable intra-group data transfers between group companies and affiliates (although the CAC has clarified that the Certification mechanism applies more broadly than only intra-group data transfers and can apply to all forms of cross-border data transfers). Both regimes are also based on the certification of an organization's data protection policies and practices. The crucial difference between the BCR and the Certification is that the certifying body for the BCR is a supervisory authority whereas it is an accredited third party certification body for the Certification and not a regulatory authority.

Finally, the BCR, certification scheme under the EU GDPR and the Certification under the PIPL are all voluntary processes; if the PI Processor does not wish to obtain a Certification under the PIPL or rely on the EU GDPR certification scheme or BCR, the PI Processor can rely on alternative data transfer mechanisms (e.g. China SCCs under the PIPL or the EU standard contractual clauses under the EU GDPR). So the Certification, the BCR and (in theory though currently not in practice) the EU GDPR certification scheme are just one of the few mechanisms available to organizations (apart from standard contractual clauses) under the PIPL and EU GDPR, respectively, for facilitating cross-border data transfers.

Certification Scope and Requirements

Scope of Application

The Certification Rules apply to all types of PI Processors' processing activities, including: collection, storage, use, processing, transmission, provision, disclosure, deletion, and cross-border data transfer. In order to obtain a Certification for cross-border data transfers, PI Processors must comply with the following standards, notwithstanding that they are only a voluntary national standard and technical committee guidance, respectively:

- *Information Security Technology — Personal Information Security Specification (GB/T 35273-2020)*, a voluntary national standard issued by SAMR and the Standardization Administration of the PRC (see official English translation).

- *Security Certification Specification for Cross-border Processing of Personal Information (TC260-PG-20222A)*. On December 16, 2022, the National Information Security Standardization Technical Committee (TC 260) released the second version of the *Network Security Standards Practice Guide — Technical Specifications for the Security Certification of Personal Information Cross-Border Processing* (Certification Specification V2.0) (see Chinese version). It supersedes and replaces the first version which was released on June 24, 2022 (Certification Specification V1.0). If a Certification is required in circumstances other than cross-border data transfers, PI Processors do not need to comply with Certification Specification V2.0 or its later version.

Unlike the Certification Rules published by SAMR and CAC, which are legally binding, the specifications above do not have the force of law. However, the Certification Rules expressly refer to the latest version of *Information Security Technology — Personal Information Security Specification (GB/T 35273-2020)* and the latest version of *Certification Specification V2.0* as the basis of the Certification and require a PI Processor's compliance in order to transfer personal information outside of the PRC. This reference appears to indirectly elevate the legal status of *GB/T 35273-2020* and Certification Specification V2.0.

The Certification Specification V2.0 significantly expands the Certification's scope of application to cover any and all cross-border transfers of personal information. In comparison, the Certification Specification V1.0 states that the Certification mechanism may only apply in two scenarios, namely intra-group data transfers and cross-border data transfers by an overseas PI Processor.

Certification Applicant Requirements

The Certification Specification V2.0 also clarifies who may qualify as applicants for the Certification mechanism:

1. **Branches and representative offices are excluded:** The applicant for the Certification must be a PRC entity with a valid legal personality, normal operations, and good credit and reputation. While "normal operations" and "good credit and reputation" remain undefined, it is clear that branches and representative offices in the PRC do not qualify as applicants for obtaining a Certification.

2. **Local representative to apply for cross-border data transfers:** The Certification Specification V2.0 distinguishes between two scenarios and who may act as the applicant for each. For intra-group data transfers, the applicant must be the PRC entity (i.e., the domestic subsidiary), and for cross-border data transfers by overseas PI Processors, the applicant must be the local representative appointed by the overseas PI Processor in the PRC, in accordance with Article 53 of the PIPL.

Updated Requirements for Certification

The Certification Specification V2.0 updates the Certification requirements for PI Processors and overseas recipients (PI Processor and overseas recipient, together the Participants) when participating in the cross-border processing of personal information. For a comparison with the previous requirements set out under Certification Specification V1.0, please read Latham's previous Client Alert which sets out the requirements in Certification Specification V1.0.

1. **Legally Binding Document:** Compared to Certification Specification V1.0, the Certification Specification V2.0 further specifies what to include in the legally binding document between the Participants. A legally binding document between the Participants must specify the following at a minimum:

   - the relevant Participants involved in the cross-border data transfer, including their names, addresses, names of the contact persons, and their contact information, etc.;
   - the purpose, scope, type, sensitivity, quantity, means, retention period, storage location, etc. of the cross-border data transfer;
   - the responsibilities and obligations of the Participants to protect personal information, and the technical and management measures taken to prevent the possible security risks of the personal information to be exported;
   - the rights of data subjects, and the ways and means to protect such rights;
   - remedy, contract termination, liability for breach of contract, and dispute resolution;
   - the overseas recipient undertakes and shall comply with the data processing rules to ensure that the level of data protection meets the standards set out under the relevant PRC laws and administrative regulations on personal information protection;
   - the overseas recipient accepts the continuous supervision of the Certification agency and to be subject to the jurisdiction of relevant PRC laws and administrative regulations on personal information protection;
   - the Participants' entities in PRC must bear legal liability and perform personal information protection obligations;
   - the Participants both undertake to bear civil liability for any breach against personal information rights and interests, and make explicit agreement on the civil liabilities to be borne by the Participants; and
   - to comply with other obligations as stipulated by applicable laws and regulations.

The Certification Specification V2.0 bolsters the obligations required under the legally binding document and aligns such requirements with those under the self-assessment prior to the mandatory Security Assessment and the provisions in the draft China SCCs.

2. **Organization Management:** The Participants must each designate a data protection officer (DPO) and establish a data protection department responsible for ensuring compliance with personal information protection obligations. Similar to points discussed in Latham's previous Client Alert, this requirement goes beyond the requirements of Article 52 of the PIPL, which imposes this DPO obligation only on PI Processors that process above certain thresholds.

   The Certification Specification V2.0 imposes further duties on the DPO and the data protection department. The DPO must have expertise and the relevant management experience in personal information protection and must be a member of the organization's management, though the question remains what job positions would constitute the management. The data protection department must:

- perform personal information protection obligations,
- prevent personal information from unauthorized access, leak, tampering, loss, etc.,
- perform compliance audits on personal information processing periodically, and
- accept the continuous supervision of the certification agencies, e.g., to answer enquiries, and to facilitate inspections, which the Certification Rules designate the Certification agencies to conduct post-certification.

1. **Processing Rules:** The Certification Specification V2.0 emphasizes that both Participants should abide by the same processing rules. Such processing rules should at a minimum include the scope, purpose, method of processing information, retention period, countries through which personal data will transit during the transfer, measures to protect data subject rights, and the incident response policy for data breaches.

2. **Personal Information Impact Assessment (PIA):** the Certification Specification V2.0 adds further factors for PI Processors to consider in relation to PIA, consistent with the PIA requirements under the other two mechanisms — the Security Assessment and the China SCCs. The Certification Specification V2.0 emphasizes that the PIA report should be issued and retained for at least three years, which resembles the requirements under the PIPL.

3. **Individuals' Rights:** the Certification Specification V2.0 elaborates on the requirement that organizations must ensure the data subjects' rights and interests under the PIPL. Notably, the Certification Specification V2.0 further requires that, (i) the overseas data recipient shall not disclose the personal information it receives to any third party, unless the disclosure is in compliance with the relevant PRC laws; and (ii) in the event of any personal information breach, the data subject may send requests to the PI Processor or directly to the overseas data recipient.

The Certification Process

The Certification process includes three stages: (i) technical inspection; (ii) on-site review; and (iii) post-certification supervision. The three stages can be broken down to five steps that the applicant must go through in order to obtain a Certification:

1. **Preparation and Seeking Authorization:** The applicant submits "authorization documents" to the Certification agency, including the applicant's basic materials, a letter of authorization (authorizing the designated agent to certify the applicant PI Processor), and other relevant proofing documents (the Certification Specification V2.0 does not define "proofing" documents) as specified by the Certification agency. If the Certification agency accepts the application pack, it will develop a Certification plan for the applicant based on the type and quantity of personal information involved, the scope of personal information processing activities, and information the technical verification agency provides. The agency will then inform the applicant of the certification plan.

2. **Technical Verification:** A technical verification agency (presumably a different body to the Certification agency) carries out the technical verification in accordance with the Certification plan and issues a report to the Certification agency and the applicant.

3. **On-Site Review:** The Certification agency performs an on-site review and issues an on-site report to the applicant.

4. **Assessment and Approval of the Certification Result:** The Certification agency shall issue the Certification decision based on the application, the technical verification report, the on-site review report, and other relevant materials. If the applicant meets the Certification requirements, the agency issues a Certification to the applicant. The Certification agency may give applicants that fail to comply with the Certification requirements another chance to rectify the non-compliance within a designated timeline. If the certification requirements are still not met after rectification, the Certification agency shall inform the applicant in writing that it is terminating the Certification process.

5. **Post-Certification Supervision:** During the three-year validity period of the Certification, the Certification agency shall continuously supervise PI Processors that have obtained Certifications and "take appropriate measures" to ensure the PI Processors' continuous compliance with the requirements for Certification. The Certification agency shall determine the frequency for supervision and has the power to suspend or revoke the Certification if the PI Processor no longer meets the requirements. The certified PI Processor may also apply for a suspension or deregistration of its Certification during the term.

The Certification Rules do not provide a time limit for each stage or step, but delegate power to the Certification agencies to decide on a reasonable timeframe for the Certification process to follow. Until the Certification mechanism is fully operational for some time, the timeframe for the entire Certification process remains unclear.

Certification Agency: CCRC

CCRC is one of the most important government affiliated institutions in the area of cybersecurity and data security certification and inspection, which also carries out various other important government-led reviews, including cybersecurity review, Data Security Management certification, and application security certification. The CCRC is a director-level institution directly under the SAMR.

The CCRC appears to have been designated as a Certification agency to handle and review Certification applications and, as at the time of writing of this Client Alert, appears to be the only agency to be so designated. The CCRC's designation is revealed by the launch of a webpage by the name of "Personal Information Protection Certification", together with an online portal called "Personal Information Protection Certification Management System" for applicants to register accounts and submit the Certification application online. It remains unclear whether the CAC has designated / will designate any other agencies to carry out the Certification.

Notably, the CCRC published a blank application form revealing some of the factors to be considered during the Certification process. The application form sets forth a list of documents required for the application pack:

- The identity documents of the applicant (business license) and details of the PI Processor's office premises (including documentation showing the legal status of the premises, e.g. property lease contracts);
- A self-assessment form (no specific explanation or guidance yet) and the proofing documents;
- Business process and description, specifically for cross-border data transfer if any;
- Organizational chart and the relevant function of each department, both for the PI processor and other entities if involved in cross-border data transfer; and

- List of the personal information involved and their classifications, e.g. whether personal information is sensitive personal information. For cross-border data transfers, the applicant must specify the overseas recipient and the destination country.

- Other supplemental documents.

Apart from the above, the applicant must also declare that there has not been any material personal information breach in the past 12 months. This appears to be a specific requirement added by CCRC considering it is not reflected in the PIPL, Implementation Rules, national standards, or technical committee guidance.

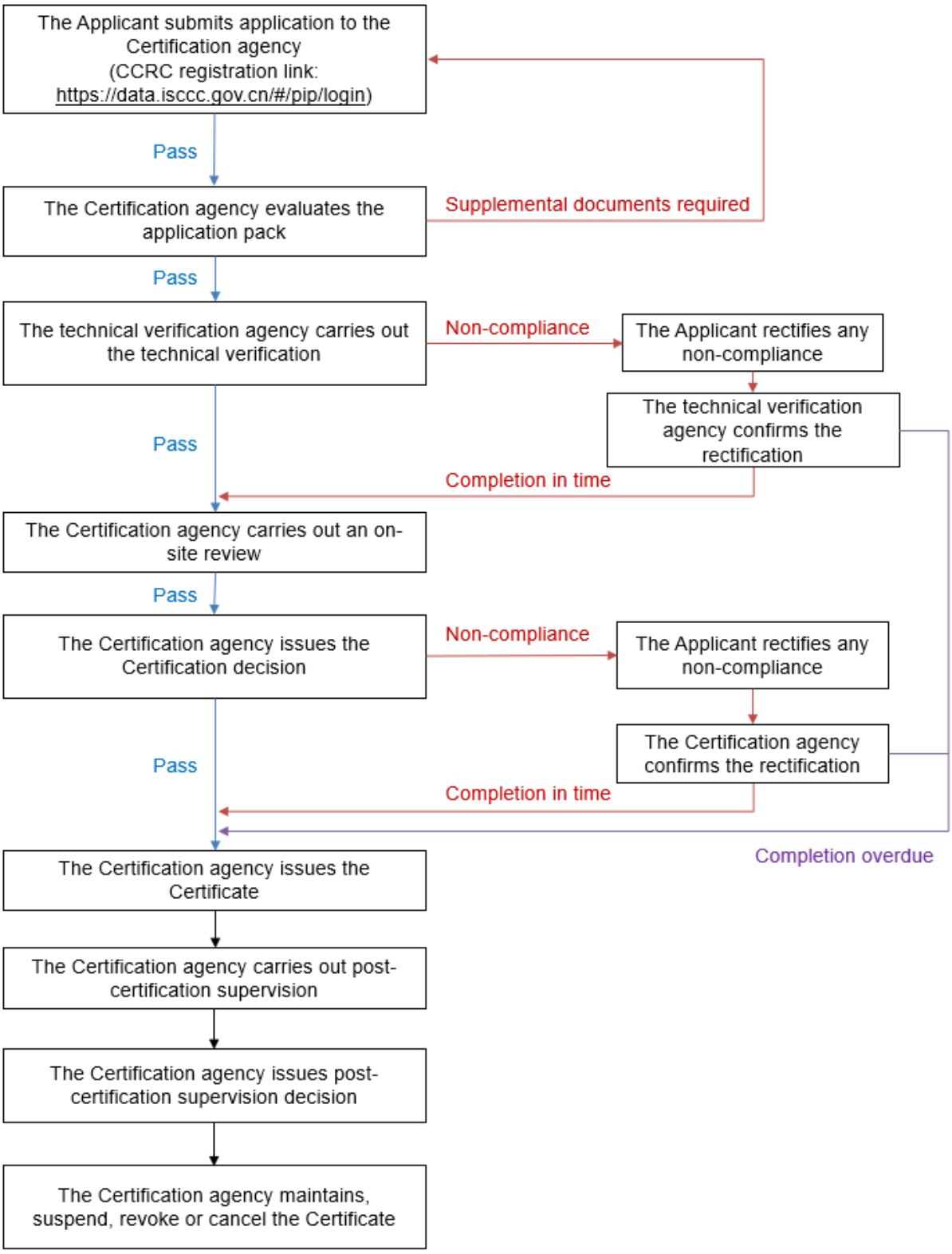
The applicant must also select the volume of the personal information involved, i.e., whether the number of personal information subjects reaches 1 million, 10 million, or 100 million. For cross-border data transfers, the applicant must select the number of personal information transferred outside of China cumulatively since January 1 of the previous year, whether it contains (i) personal information of 100,000 individuals, and / or (ii) sensitive personal information of 10,000 individuals.

Validity/Term of Certification

The Certification is valid for three years, and the applicant shall re-submit the application for renewal six months before the three-year validity of Certification expires. During the term of the Certification, the certified PI Processor will need to request a modification of its initial application for any change to its name, registered office address, compliance with the Certification requirements, or Certification scope. The Certification agency shall then consider whether it is necessary to re-perform the technical verification and/or the on-site review; and whether to approve the modification.

Certification agencies are required to disclose the issuance, modification, suspension, or revocation of Certification.

Below please find a flow chart which demonstrates the entire application process:


The Applicant submits application to the Certification agency (CCRC registration link: https://data.isccc.gov.cn/#/pip/login)
Pass
The Certification agency evaluates the application pack
Supplemental documents required
Pass
The technical verification agency carries out the technical verification
Non-compliance
The Applicant rectifies any non-compliance
The technical verification agency confirms the rectification
Pass
Completion in time
The Certification agency carries out an on-site review
Pass
The Certification agency issues the Certification decision
Non-compliance
The Applicant rectifies any non-compliance
The Certification agency confirms the rectification
Pass
Completion in time
Completion overdue
The Certification agency issues the Certificate
The Certification agency carries out post-certification supervision
The Certification agency issues post-certification supervision decision
The Certification agency maintains, suspend, revoke or cancel the Certificate

The Certificates and Marks

The Certification Rules provide for two different Certification marks: (i) Certification for the collection, use, and processing of personal information generally, but which **does not** involve cross-border data transfers; and (ii) Certification specifically for cross-border data transfer. Both the certificates and the marks can be used in advertisements or other promotional activities, provided that the certificates or marks are not displayed in a misleading manner. There is no official explanation as to why a PI Processor would apply for the first certification which does not include cross-border data transfers. Perhaps such certification can act as a "badge of approval" or a qualification for the PI Processor, since it has gone through the Certification process generally. In the sample marks below, ABCD refers to the name of the specific Certification agency (e.g., CCRC):

Certification mark excluding cross-border data transfer

Certification mark specifically for cross-border data transfer

Takeaways

For PI Processors that regularly transfer personal information outside of the PRC, but do not meet the thresholds in the Security Assessment Measures that trigger a mandatory Security Assessment, the Certification mechanism can be a suitable tool for enabling cross-border data transfers. As it has now been clarified that the Certification is suitable for all cross-border data transfers, uptake of the Certification mechanism will likely increase. Though whether the Certification of the China SCCs will be increasingly popular in practice for facilitating cross-border data transfers remains to be seen.

Though the further details on the Certification mechanism highlighted in the Certification Specification V2.0 are welcome, a number of uncertainties remain before PI Processors may successfully rely on this mechanism in practice. For example, the CAC has yet to address key questions about whether there are going to be any other designated Certification agencies apart from CCRC, how will post-Certification supervision be conducted in practice, and how can PI Processors switch to apply for a Security Assessment if the relevant thresholds in the Security Assessment Measures are met during the Certification's validity period. As the Certification mechanism is now fully operative with the designation of the CCRC, it is likely that more PI Processors will submit Certification applications and further practical guidance will be released by the CCRC on the Certification process.

Finally, as the PRC authorities begin to ramp up their enforcement activities under the Cybersecurity Law, Data Security Law, and PIPL, they likely will refer to the Certification Specification, the national standards, and technical committee guidance mentioned therein as recommended best practices for PI Processors to adopt in order to comply with the new laws' requirements.

If you have questions about this Client Alert, please contact one of the authors listed below or the Latham lawyer with whom you normally consult:

Hui Xu
hui.xu@lw.com
+86.10.5965.7006
Beijing

Kieran Donovan
kieran.donovan@lw.com
+852.2912.2701
Hong Kong

Bianca Lee
bianca.lee@lw.com
+852.2912.2500
Hong Kong

This Client Alert was prepared with the assistance of Zhiying Li in the Beijing office of Latham & Watkins.

You Might Also Be Interested In

China Unveils Draft Standard Contract And Provides Clarifications on Cross-Border Data Transfer Mechanisms

China Issues New Rules on Cybersecurity Review for Network Platform Operators Listing Abroad

China Introduces First Comprehensive Legislation on Personal Information Protection

China's New Data Security Law: What to Know

China Issues New Regulations to Protect the Critical Information Infrastructure