LATHAM&WATKINS

Client Alert Commentary

Latham & Watkins Privacy & Cyber Practice

August 9, 2022 | Number 2984

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

China's CAC publishes guidance on cross-border data transfers, including draft standard contractual clauses and regulatory guidance on certification and security assessment.

Key Points:

- **Security Assessment:** Effective September 1, 2022, personal information processors (PI Processors) under the Personal Information Protection Law (PIPL) must file for a Security Assessment with the Cyberspace Administration of China (CAC) if any of the following circumstances apply: (i) important data will be transferred; (ii) personal information will be transferred by a critical information infrastructure operator (CIIO) or a PI Processor who processes personal information of more than 1 million individuals; or (iii) in each case, the personal information of more than 100,000 individuals or sensitive personal information of more than 10,000 individuals will be cumulatively transferred since January 1 of the previous year.

- **Certification:** A PI Processor may obtain a personal information security certification from agencies designated by the CAC. According to the certification specification, the certification is suitable for (i) intra-group data transfers, similar to the Binding Corporate Rules under the General Data Protection Regulation (GDPR); and (ii) cross-border data transfers by foreign PI Processors subject to the PIPL's extraterritorial reach.

- **Draft China SCCs:** A draft of the China standard contractual clauses (China SCCs), a template contract for cross-border data transfers (similar to the EU standard contractual clauses under the GDPR), were released for public consultation. The China SCCs are intended for adoption for cross-border transfers of personal information, except those transfers subject to the Security Assessment.

Authorities in the People's Republic of China (the PRC, which is limited to mainland China only for the purposes of the PIPL) have published guidance on the three mechanisms for enabling cross-border data transfers under the PIPL:

- On June 24, 2022, the National Information Security Standardization Technical Committee (TC 260) released the final version of the *Network Security Standards Practice Guide - Technical Specifications for the Security Certification of Personal Information Cross-Border Processing* (the Certification Specification). (See Chinese version.)

- On June 30, 2022, the CAC released the draft *China Standard Contractual Clauses for Cross-border Transfer of Personal Information*, as well as the *Draft Provisions on Standard Contract for Cross-border Transfer of Personal Information* (the Draft Provisions) for a one-month public consultation ending on July 29, 2022. (See Chinese version.)

- On July 7, 2022, the CAC released the final version of the *Measures on Cross-Border Data Transfer Security Assessment* (the Assessment Measures), which supersedes three previous drafts and will take effect on September 1, 2022. (See Chinese version.)

Though a number of practical issues are yet to be addressed, the guidance provides PI Processors with clarity on Chinese authorities' expectations on how cross-border data transfers can comply with the PIPL. This Client Alert examines each of the data transfer mechanisms and how they may be applied by PI Processors.

Background

Data Transfer Mechanisms

Article 38 of the PIPL sets out three key ways (Data Transfer Mechanisms) for PI Processors to transfer data outside the PRC:

1. Passing a security assessment (Security Assessment) organized by the CAC prior to undertaking the cross-border data transfer;

2. Obtaining a personal information protection certification (Certification) from a certification agent designated by the CAC; or

3. Concluding a contract with the overseas recipient, in accordance with China SCCs, prior to the cross-border data transfer.

Other Cross-Border Data Transfer Requirements

In addition to satisfying one of the Data Transfer Mechanisms, the PI Processor must also fulfill the below requirements prior to transferring personal information outside of China, as discussed in this Client Alert on the PIPL. These include:

- **Necessary Security Measures:** Adopting necessary measures to ensure the overseas data recipient's personal information processing activities meet the standard provided in the PIPL;

- **Notice and Separate Consent:** Notifying the data subjects of the overseas data recipient's contact information, processing purpose and methods, categories of personal information, and procedures to exercise their personal information rights over the overseas data recipient and obtaining their separate consent; and

- **PIA:** Conducting a personal information protection impact assessment (PIA) prior to the transfer, which must be kept for at least three years.

Cybersecurity Review for Overseas Listing

An additional consideration is the Cybersecurity Review Measures 2021, promulgated on December 28, 2021. These measures further require network platform operators that hold personal information of more

than 1 million individuals and that seek an overseas listing to file for a cybersecurity review from the CAC, regardless of whether any data (or personal information) would be transferred overseas. See this Latham Client Alert on cybersecurity review for more information.

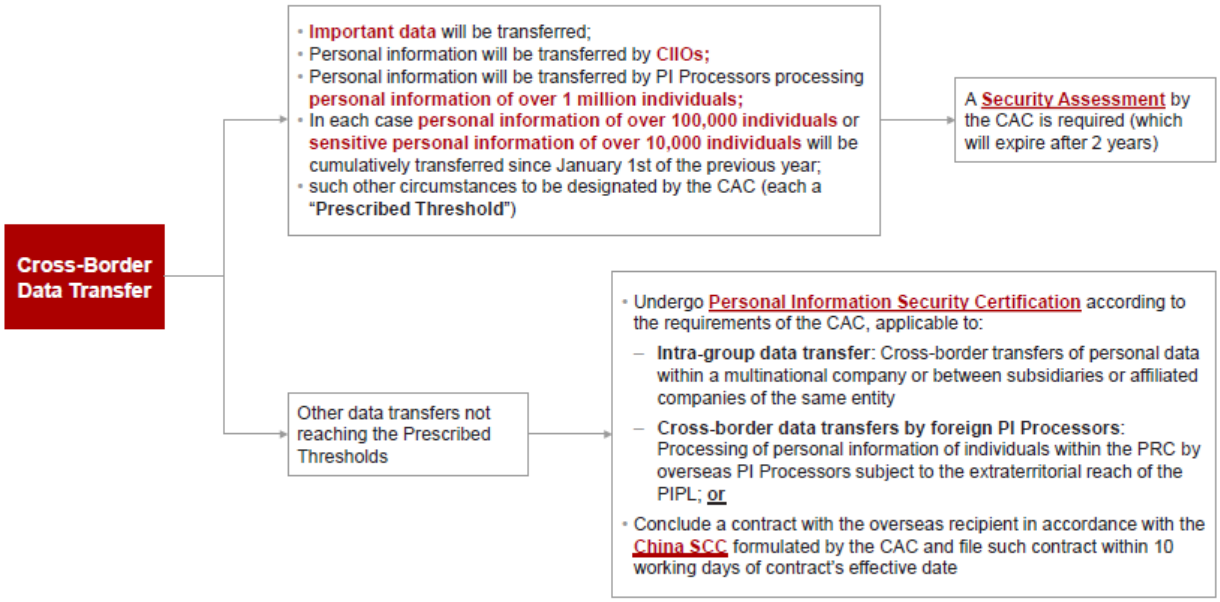
The three Data Transfer Mechanisms are discussed in detail below.

Mechanism I: Security Assessment

Scope of Application

The Assessment Measures aim to clarify the application and procedure of the Security Assessment stipulated under the PIPL. They state that if a cross-border data transfer falls under any of the circumstances below (Prescribed Thresholds), the PI Processor must apply for a Security Assessment prior to the transfer and may not rely on the other Data Transfer Mechanisms:

- **Important data** will be transferred ("important data" is defined under the Assessment Measures as "data that, once tampered with, destroyed, leaked, illegally obtained or illegally used, may endanger national security, economic operation, social stability, public health and safety, and so forth");
- Personal information will be transferred by a CIIO[1];
- Personal information will be transferred by a PI Processor who processes the personal information of more than **1 million individuals**;
- In each case, the **personal information** of more than **100,000 individuals** or **sensitive personal information** of more than **10,000 individuals** will be cumulatively transferred since January 1 of the previous year; or
- Such other circumstances to be designated by the CAC (this gives the CAC discretion to further expand the scope of data transfers subject to a mandatory Security Assessment in the future).



(Prerequisites for cross-border data transfers under Article 38 of the PIPL)

As explained above, the Assessment Measures make it mandatory for PI Processors to apply for a Security Assessment with the CAC prior to a cross-border data transfer if any one of the Prescribed Thresholds are met.

Security Assessment Procedure and Timeline

Self-Assessment

Before applying for a Security Assessment, PI Processors are required to carry out a self-assessment of data export risks associated with the data transfer. The self-assessment must address the following factors:

- The **legality, legitimacy, and necessity** of the purpose, scope and means of the cross-border data transfer and the data processing by the overseas data recipient;
- The **quantity, scope, categories, and sensitivity** of the data to be transferred, and the risks that such data transfer may bring to national security, the public interest, or the lawful rights and interests of individuals or organizations;
- The **responsibilities and obligations undertaken by the overseas recipient**, as well as whether the management and **technical measures** adopted by the overseas recipient are adequate to ensure the security of the outbound data;
- The **risks of data being tampered with**, damaged, leaked, lost, transferred, illegally obtained, or used during or after the transfer, and whether data subjects are able to exercise their rights in the overseas jurisdiction;
- Whether the **legal documents** to be concluded with the overseas data recipient impose sufficient obligations to ensure data security; and

- Other matters that may affect the security of the data export.

Following the self-assessment, the CAC will also consider the following as part of the formal Security Assessment:

- The impact of the local policies and regulations on the protection of personal information in the overseas jurisdiction where the data recipient is located and whether the data protection level of the overseas data recipient meets the requirement of the laws and administrative regulations of the PRC and mandatory national standards;

- Whether data security and personal information rights and interests can be fully and effectively ensured; and

- The PI Processor's compliance with the PRC laws, administrative regulations, and department rules.

(all of the factors above, the Data Transfer Assessment Factors)

These factors are substantially similar to those that must be considered by a PI Processor when conducting a PIA as a prerequisite for relying on the China SCCs. The requirement to undertake a self-assessment on data export risks is not novel and, in fact, resembles the requirement under the GDPR to perform a transfer impact assessment before transferring personal data to a third country.

Declaration and Submission

Provincial-level review: Once the self-assessment is completed, the PI Processor may submit to the provincial CAC the Security Assessment filing application pack that consists of a declaration form, the self-assessment report, the legal documents to be concluded with the overseas recipient, and any other materials if required. The provincial CAC shall conduct a review to ensure the application materials are complete within five working days from receipt of the application pack. Notably, the Assessment Measures do not specify whether the "legal documents to be concluded with the overseas data recipient" must be in the form of the China SCCs, so the PI Processor may be free to conclude a contract with the overseas recipient and may not have to adopt the China SCCs in their exact form.

State-level review: If the provincial CAC deems the application materials to be complete, it shall submit the application pack to the CAC, which shall determine whether to accept the Security Assessment application within seven working days after receipt of the application. If the CAC accepts the application, it will formally launch the Security Assessment, with input from other authorities, such as the relevant departments of the State Council, provincial CACs, and specialized agencies to perform a substantive review and to issue a decision in writing within 45 working days. If the CAC finds that the application submitted does not meet the Security Assessment requirements or involves complicated circumstances and, as a result, needs further supplementary materials or rectification, it may extend the timeframe to reach a determination, in which case it shall inform the PI Processor of such extension in writing. The timeline of the security assessment is generally around three months, subject to the CAC's discretion for extension, i.e., the Security Assessment should take 5 + 7 + 45 + n working days, from the date of application to receipt of the final result.

Security Assessment Result

The result of the Security Assessment will be notified to the PI Processor in writing and will be valid for two years from the date of issuance, which means PI Processors must go through the same exercise

every two years. For data transfers in which it is necessary to continue the data export after the expiry of the first Security Assessment, the PI Processor may re-apply for the Security Assessment 60 working days before the two-year validity duration of the assessment expires.

If the PI Processor has any objection to the evaluation results, it may apply to the CAC for re-evaluation within 15 working days of receiving the results, and the re-evaluation result is the final conclusion.

The PI Processor will need to re-apply for the Security Assessment if there are any changes that may impact the Data Transfer Assessment Factors and the overall data export risks. Such factors may include changes in the purpose and scope of data to be exported, the local data protection policies in the overseas jurisdiction and the legal documents entered into between the PI Processor and overseas recipient, and any other circumstances affecting the security of the data to be exported.

If data export activities that had passed the Security Assessment are found to no longer meet the requirements of the Security Assessment at any point during the two year validity period, the CAC will notify the PI Processor in writing to terminate data export activities. If the PI Processor needs to continue the data export, it may re-apply for the Security Assessment once it rectifies the non-compliance.

Transition Period

PI Processors have a transition period of six months (until March 1, 2023) to comply and to bring data exports prior to September 1, 2022, in line with the requirements of the Assessment Measures.

Remaining Uncertainties

While many of the requirements of the Security Assessment procedure seem straightforward (although very burdensome and time consuming), there still remain significant uncertainties. For example, how should the Prescribed Thresholds, particularly the volume of personal data processed, be calculated? And how should the changes that necessitate a refiling of the Security Assessment be quantified? The same questions apply for the China SCCs, as explained below.

Mechanism II: Personal Information Security Certification

On June 24, 2022, TC 260 published the Certification Specification, which provides guidance on the implementation of the Certification and clarify its scope of application.

Notably, the Certification Specification is not a regulation, administrative rule, or national standard but is only a technical committee guidance and, as a result, does not have the force of law. However, it could evolve into a mandatory, legally binding national standard in the future.

Scope of Application

The Certification mechanism resembles the GDPR's Binding Corporate Rules, which is one of the mechanisms available to data controllers and processors for the cross-border transfer of personal data between a group of undertakings or enterprises.

The Certification Specification clarifies that the Certification mechanism may be used in two scenarios:

- **Intra-group data transfer:** Cross-border transfers of personal data within a multinational company or between subsidiaries or affiliated companies of the same entity; and

- **Cross-border data transfers by foreign PI Processors:** Processing of personal information of individuals within the PRC by overseas PI Processors subject to the extraterritorial reach of the PIPL.

The second scenario means that the Certification may be used by overseas PI Processors that directly collect personal data from individuals in the PRC. The Certification Specification also provides that "the certification of cross-border personal information processing activities is a voluntary certification recommended by the state, and parties involved in qualified cross-border personal information activities are encouraged to voluntarily apply for certification of cross-border personal information processing activities." That statement seems to suggest that the Certification mechanism is not the only option available to PI Processors that wish to transfer personal data overseas; the China SCCs may be a second option for cross-border data transfers, although this has not been confirmed in the Certification Specification or the Draft Provisions.

To avoid doubt, if a PI Processor falls within the Prescribed Thresholds for Security Assessment, then it must apply for a Security Assessment and may not use the Certification as a means to facilitate the cross-border data transfer.

The Certification Specification states that in respect of intra-group data transfers, the PRC entity (i.e., domestic affiliate) shall be responsible for obtaining the Certification and shall bear legal liability, presumably only over the data transfers which rely on the Certification, though this is not explicitly stated in the Certification Specification. It also states that for cross-border data transfers by overseas PI Processors, their local representative shall be responsible for obtaining the Certification and shall bear legal liability, presumably only over the data transfers which rely on the Certification, though this has not been explicitly stated in the Certification Specification. This requirement goes beyond the PIPL, which is silent on the liability of local representatives, as the Certification Specification explicitly states that the local representative shall be liable for the overseas PI Processor's actions when adopting the Certification mechanism.

Requirements for Certification

The Certification Specification introduces five requirements for PI Processors and overseas recipients (Participants) when participating in the cross-border processing of personal information.

1. **Legally binding agreement:** Participants must enter into a legally binding agreement, which must specify the following at a minimum:

   - The relevant Participants involved in the cross-border data transfer
   - The purpose, categories, and scope of the cross-border data transfer
   - The measures to protect the rights and interests of data subjects
   - Obligation on the overseas recipient to comply with PRC data processing rules, ensure that the level of data protection is not lower than the standards under the PIPL, and accept the supervision of certification bodies and the jurisdiction of relevant PRC laws
   - The entities in PRC that shall bear legal liability
   - Other obligations stipulated by applicable laws and regulations

   Compared to the obligations set out in the draft China SCCs, the minimum requirements above appear to be much less onerous and prescriptive (i.e., more principles-based), which a PI Processor may wish to consider when deciding whether to rely on the Certification mechanism or the China SCCs.

2. **Organization management:** Participants must designate a data protection officer (DPO) and establish a data protection department responsible for ensuring personal information protection obligations are complied with. This requirement goes further than the requirements of Article 52 of the PIPL as the Certification Specification imposes this obligation on both the PI Processor and the overseas recipient, whilst the PIPL imposes this obligation only on PI Processors that process above certain thresholds.

3. **Processing rules:** The Participants must abide by the rules on cross-border transfers of personal data, including 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.

4. **PIA:** The Participants must carry out a PIA and assess the following: (i) whether the export is in compliance with applicable laws and regulations; (ii) the impact of the transfer on individual rights, especially the potential impact of foreign legal and network security environment on individual rights; and (iii) other matters on protecting personal information rights and interests, if necessary. This requirement is consistent with the one under the PIPL that PI Processors must carry out a PIA prior to any cross-border data transfers. The PIPL does not go into detail on the factors a PIA must cover, and neither does the Certification Specification except very briefly. The Assessment Measures and the Draft Provisions (which mirror the factors set out in the former's self-assessment) elaborate in more detail the factors that should be focused on in a self-assessment and a PIA, respectively. Therefore, if PI Processors rely on the Certification mechanism, they would be advised to undertake a PIA that covers the more comprehensive factors set out in the Assessment Measures as a best practice.

5. **Individuals' rights:** The Certification Specification requires that data subjects be designated as third-party beneficiaries of the legally binding agreement between the PI Processor and the overseas recipient. Data subjects are also given the right to require the PI Processor and overseas recipient to provide a copy of extracts of the legally binding agreement pertaining to the data subject's individual rights. This requirement resembles the one under the draft China SCCs, which also gives data subjects the right to request a copy of the China SCCs from the PI Processor and overseas recipient.

Remaining Uncertainties

The Certification Specification still leaves many practical uncertainties although it provides some detail on the Certification mechanism. It is unclear what the relevant certification agencies/bodies are, and unclear what the procedure is for obtaining a Certification or for switching to a mandatory Security Assessment if the Prescribed Thresholds are met during the Certification's validity period and the duration of the validity period.

Mechanism III: China SCCs

On June 30, 2022, the CAC finally published the long-awaited draft of the China SCCs, as part of the Draft Provisions, for public consultation until July 29, 2022. A number of provisions in the draft China SCCs are similar to the GDPR's standard contractual clauses (EU SCCs), particularly the controller-to-processor clauses. However, the draft China SCCs take a radically different approach from the EU SCCs, which address different processing arrangements under a four-modular approach. Instead, the draft China SCCs adopt a one-size-fits-all approach and do not distinguish between controller-to-controller and

controller-to-processor transfers. Therefore, the draft China SCCs are expected to apply to all cross-border data transfers irrespective of the particular transfer arrangement, except those that meet a Prescribed Threshold, in which case the PI Processor must undertake a Security Assessment. How this will play out in practice is unclear as data processing obligations typically differ from data controller obligations.

Scope of Application

The China SCCs may only be adopted if all of the conditions below (SCC Thresholds) are met, i.e., the data transfer does not reach any of the Prescribed Thresholds, in which case the mandatory Security Assessment would be applicable instead:

- A PI Processor is not a CIIO;
- A PI Processor does not process the personal information of more than 1 million individuals
- A PI Processor has not cumulatively transferred the personal information of more than 100,000 individuals since January 1 of the previous year; and
- A PI Processor has not cumulatively transferred the sensitive personal information of more than 10,000 individuals since January 1 of the previous year.

Since the SCC Thresholds play such an important role in determining whether a PI Processor can rely on the China SCCs, one would expect sufficient guidance on the calculation of such thresholds. Unfortunately, such guidance is lacking and, similar to the Assessment Measures, it remains unclear how the personal information volume is calculated (e.g., is it a per-entity or group calculation?) The Draft Provisions also lack a mechanism for a situation in which, during the term of the China SCCs, the PI Processor no longer meets the SCC Thresholds and instead one of the Prescribed Thresholds for the Security Assessment is triggered.

Obligations Under the China SCCs

According to the Draft Provisions, the China SCCs must cover the following:

- Basic information of the PI Processor and the overseas data recipient, including but not limited to their names, addresses, contact names and contact information;
- The purpose, scope, type, sensitivity, quantity, means, retention period, storage location, etc. of the personal information to be exported;
- The responsibilities and obligations of the PI Processor and the overseas data recipient 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 impact that the local personal information protection policies and regulations of the country or region where the overseas data recipient is located may have on compliance with the China SCCs;
- The rights of data subjects, and the ways and means to protect such rights; and
- Remedy, contract termination, liability for breach of contract and dispute resolution.

The Draft Provisions (like the PIPL for any cross-border data transfer) state that as a prerequisite for adopting the China SCCs, a PI Processor must carry out a PIA that should focus on certain factors relating to the risks of data export. These requirements are substantially similar to those required for the self-assessment prior to the mandatory Security Assessment. This approach is similar to that of a transfer impact assessment under the GDPR. A point of uncertainty is whether a local counsel's legal opinion will be required as part of the PIA and the filing in order to confirm that there are no data export risks. In accordance with the PIPL, the PIA must be retained for at least three years.

Filing Requirement and Procedure

Within 10 working days from entering into the China SCCs with the overseas recipient (i.e., effective date of the contract), a PI Processor must file both the China SCCs and the completed PIA report with the provincial CAC. The PI Processor may export personal information as soon as the filing is completed, because the filing requirement appears to be a formality / procedural requirement rather than a substantive review (though the CAC has not confirmed this).

This 10-day filing requirement will likely impose a burdensome obligation on PI Processors, especially those whose daily business needs require ongoing cross-border data transfers. This is exacerbated by the fact that, according to the Draft Provisions, failure to comply with the filing requirement would amount to a breach of the PIPL, which seems to be inconsistent with and goes beyond the provisions of the PIPL, which does not have such a filing requirement in Article 38.

If any of the following changes that may impact the data export occur during the term of the executed China SCCs, the PI Processor must re-sign the China SCCs and repeat the filing process:

- Changes in the purpose, scope, type, sensitivity, quantity, provision manner, retention period, storage location of the personal information transferred and the purpose and manner of processing by the overseas recipient, or extension of the retention period of the personal information transferred;

- Changes in the personal information protection policies and regulations of the country or region where the overseas recipient is located that may affect the rights and interests of the data subjects; or

- Any other circumstances that might affect the rights and interests of the data subjects.

The Draft Provisions do not state whether the PIA needs to also be repeated and refiled, and the threshold or range of changes that would necessitate the refiling is unclear. For example, when it is deemed that there is change in the quantity of the personal information transferred, is the quantity determined by the number of people involved or the amount of information transferred?

Remaining Uncertainties

Some of the key unresolved questions in the draft China SCCs include the following:

- **Application scope**: While many stakeholders may make the assumption that Article 38 of the PIPL and the China SCCs apply to overseas PI Processors due to the PIPL's extraterritorial reach, the Draft Provisions only state that the China SCCs should be executed when a PI Processor transfers personal information outside China to the overseas recipient. The Draft Provisions do not explicitly confirm whether the China SCCs are applicable if an overseas PI Processor directly collects personal information from individuals in China and transfers such data

to another offshore recipient. Since the Draft Provisions state that the China SCCs are applicable only to a PI Processor and an overseas recipient, it is also unclear whether an "entrusted party" that processes personal information on behalf of a PI Processor may also utilize the China SCCs to enable cross-border data transfers, e.g., where the PI Processor is located overseas. Furthermore, as the China SCCs do not distinguish between controller-to-controller and controller-to-processor clauses, it is unclear how the China SCCs may be adopted in the former scenario given the nature of the transfer arrangement and obligations on the parties would be fundamentally different.

- **Content, format, and language**: The Draft Provisions state that the PI Processor and overseas recipient must execute the China SCCs (which also includes an Appendix II that is left intentionally blank for any additional terms that the parties may wish to agree on). However, the Draft Provisions do not clarify further whether the parties, in order to comply with Article 38(3) of the PIPL, may modify the China SCCs and if so, to what extent the standard terms can be changed. For example, can the parties simply extract the obligations in the China SCCs and incorporate them within their own form of agreement, or should the China SCCs be executed exactly in their current form? Can the parties incorporate the China SCCs as a schedule to a master agreement? If an overseas recipient is involved, a contract between the PI Processor and overseas recipient will likely be in English and there will be an English prevailing language clause in the case of conflicts. However, the China SCCs are only available in Chinese, and whether the CAC will publish an English version to facilitate international data transfers is unclear. In this case, can the English version of the contract prevail?

- **Governing law**: The Draft Provisions state that the governing law of the China SCCs must be PRC law. In addition, the only available options for dispute resolution is litigation in Chinese courts and arbitrations administered by Chinese arbitration institutions. To the extent a foreign PI Processor can execute the China SCCs with an overseas recipient, the question remains as to whether foreign laws (e.g., laws of a PI Processor's home jurisdiction) can prevail. For example, the EU SCCs permit parties to choose, in certain circumstances, laws other than those of an EU Member State as the governing law of the EU SCCs.

- **Conflict of laws**: According to the Draft Provisions, other contracts signed between the PI Processor and overseas recipient must not conflict with the China SCCs. The question then arises as to how potential conflicts between the China SCCs and applicable laws in other jurisdictions, e.g., the GDPR and EU SCCs, which many multinational companies are subject to and adopt, may be resolved.

- **Implementation timeline**: The implementation timeline for entering into the China SCCs for new cross-border data transfers is unclear. The CAC also has not specified whether the requirement to enter into the China SCCs would apply retrospectively to existing cross-border data transfers and, if so, what the grace period is for amending existing contracts with overseas recipients. For example, the Assessment Measures provide a six-month transition period to comply with the Security Assessment.

Sanctions

A PI Processor and its relevant responsible persons may be subject to sanctions under relevant data laws, i.e., the Cybersecurity Law (CSL), the Data Security Law (DSL), and/or the PIPL if an appropriate Data Transfer Mechanism is not adopted for cross-border data transfers. According to the Assessment Measures, the sanctions provided under these different laws may be simultaneously applied. As the

Assessment Measures will soon come into effect on September 1, 2022, PI Processors that fall within scope face imminent risk of sanctions based on failure to file for a Security Assessment. Below is a recap of the potential sanctions under each of China's data laws.

Legal Authority	Sanctions (for Companies)	Sanctions (for Relevant Officers)
CSL (Article 66)	• **CIIOs** that fail to perform the Security Assessment as requested would be required to rectify the non-compliance, receive administrative warnings, forfeit any illegal proceeds, and/or face fines of **CNY 50,000 (US$7,400) to CNY 500,000 (US$74,000)**; as well as potential suspension of the business and revocation of the business license	• Responsible personnel could face fines of CNY 10,000 (US$1,480) to CNY 100,000 (US$14,800)
DSL (Article 45, 46)	• If a PI Processor fails to file an export of **important data** for the mandatory Security Assessment, it would be required to rectify its non-compliance and/or receive administrative warnings, and **may** also face fines from **CNY 100,000 (US$14,800) to CNY 1 million (US$148,000)** • Under severe circumstances of non-compliance, the PI Processor could face fines of **CNY 1 million (US$148,000) to CNY 10 million (US$1.48 million)**, and potential suspension of the business, revocation of the business license, and/or termination of business operations • If **state core data** is concerned, PI Processors found to be mishandling such data would be subject to fines of **CNY 2 million (US$296,000) to CNY 10 million (US$1.4 million)**, suspension or termination of operations, and/or revocation of business licenses, as well as criminal liability if applicable	• Responsible personnel could face fines of CNY 10,000 (US$1,480) to CNY 100,000 (US$14,800) • Under severe circumstances, responsible personnel could face fines of CNY 100,000 (US$14,800) to CNY 1 million (US$148,000)
PIPL (Article 66)	• A PI Processor mishandling **personal information** would first be required to rectify the non-compliance and receive administrative warnings. Any illegal proceeds would be confiscated and the PI Processor's services would be suspended or terminated • PI Processors refusing to rectify non-compliance would face fines of up to **CNY 1 million (US$148,000)**	• Responsible personnel who refuse to rectify non-compliance could face fines of CNY 10,000 (US$1,480) to CNY 100,000 (US$14,800) • Under severe circumstances, responsible personnel could face fines of CNY 100,000

Legal Authority	Sanctions (for Companies)	Sanctions (for Relevant Officers)
	• If the non-compliance leads to serious consequences, the PI Processors could face fines of up to **CNY 50 million (US$7.4 million),** or **5% of their annual turnover** of the preceding year — whichever is higher, as well as rectification of non-compliance, suspension or termination of operations, and/or revocation of business licenses	(US$14,800) to CNY 1 million (US$1.48 million)

Takeaways

As the Assessment Measures will soon come into force, PI Processors subject to the PIPL should assess whether their cross-border data transfers will be — or will soon fall under — any one of the Prescribed Thresholds. If so, PI Processors would need to file a Security Assessment. The Assessment Measures offer a six-month transition period for PI Processors to align their data transfers with the Assessment Measures.

Despite the general picture of the three Data Transfer Mechanisms available to PI Processors, the CAC still needs to provide further clarifications, such as the applicable scope of each mechanism and the practical steps that need to be taken in order to comply. A number of rules are also expected to be released on a sector-specific basis later this year (i.e., from the Ministry of Industry and Information Technology of China, and the Securities Regulatory Commission of China), which may impose further obligations on cross-border data transfers for PI Processors operating in specific industries.

The flurry of regulatory guidance published by the CAC, nearly all of which focuses on cross-border data transfers, indicates that such transfers are a key focus in the PRC. While further rules and guidance will likely follow, the latest guidance helpfully enables businesses to continue refining their compliance program to account for the PIPL and related laws.

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.

Endnote

1 The concept of CIIO has been further elaborated in the Security Protection Regulations on the Critical Information Infrastructure effective September 1, 2021 (Read this Latham Client Alert for more information). The regulations stipulate that the competent industry regulators would have the authority to designate companies as CIIOs via notifications, based on the nature and scale of their business, e.g., whether their facilities and information systems are critical to important industries and sectors, including public communication and information services, energy, transportation, water conservancy, finance, public service and e-government; or other industries and sectors that may pose severe threat to national security, people's livelihood, and public interests if their data is damaged, disabled, or leaked. CIIO determination is ultimately subject to the discretion of the industry regulator. Such authorities will arrange the critical information infrastructure (CII) identification in the sectors or fields governed by them respectively in accordance with the identification rules, and promptly inform the operators of the identification result. That means if any network facility or information system of a company is identified as a CII, the company will receive a clear notification of the identification result from the regulator, and on that basis, the company will be able to confirm whether it is a CIIO.