LATHAM&WATKINS

Client Alert Commentary

Latham & Watkins Privacy & Cyber Practice

9 July 2024 | Number 3249

China Finalises Exemptions to Cross-Border Data Transfer Rules and Eases Restrictions

Personal Information processors should revisit their policies and agreements to assess whether they can benefit from the relaxed requirements that could ease their compliance burden.

Key Points:

- **Exemptions to Data Transfer Mechanisms:** The Provisions on Promoting and Regulating Cross-Border Data Flows (Provisions) significantly reduce compliance burdens for companies by introducing exemptions to the cross-border data transfer requirements under the Personal Information Protection Law (PIPL). For example, if the transfer is necessary for performance of a contract or cross-border HR management, or the volume of personal information (PI) transferred is below 100,000 individuals, the transfer is exempt from the requirements for a Data Transfer Mechanism.
- **Relaxing the volume thresholds for requiring a Data Transfer Mechanism:** The requirement to implement a Data Transfer Mechanism is only triggered if the volume of PI exported exceeds certain thresholds *and* there is no applicable exemption. The Provisions increase the existing volume thresholds below which a Data Transfer Mechanism is not needed.
- **Important Data:** Export of "Important Data" also requires a Data Transfer Mechanism to be implemented (specifically, passing a security assessment) and cannot benefit from the newly introduced exemptions. The Cyberspace Administration of China (CAC) and its local departments will publish catalogues of what they consider to be "Important Data. Practically, this means that unless a regulator has notified a personal information processor (PI Processor) that it handles Important Data or a PI Processor believes that the data it processes likely falls within one of the published Important Data catalogues, a PI Processor may assume that it does not handle Important Data.
- **Security Assessment:** Notwithstanding the exemptions introduced (e.g., contractual necessity, HR management, and transfers of PI belonging to less than 100,000 individuals), PI transfers by a critical information infrastructure operator (CIIO) and transfers of Important Data outside of the PRC will always require a Security Assessment — consistent with the requirements under previous guidance.

Background

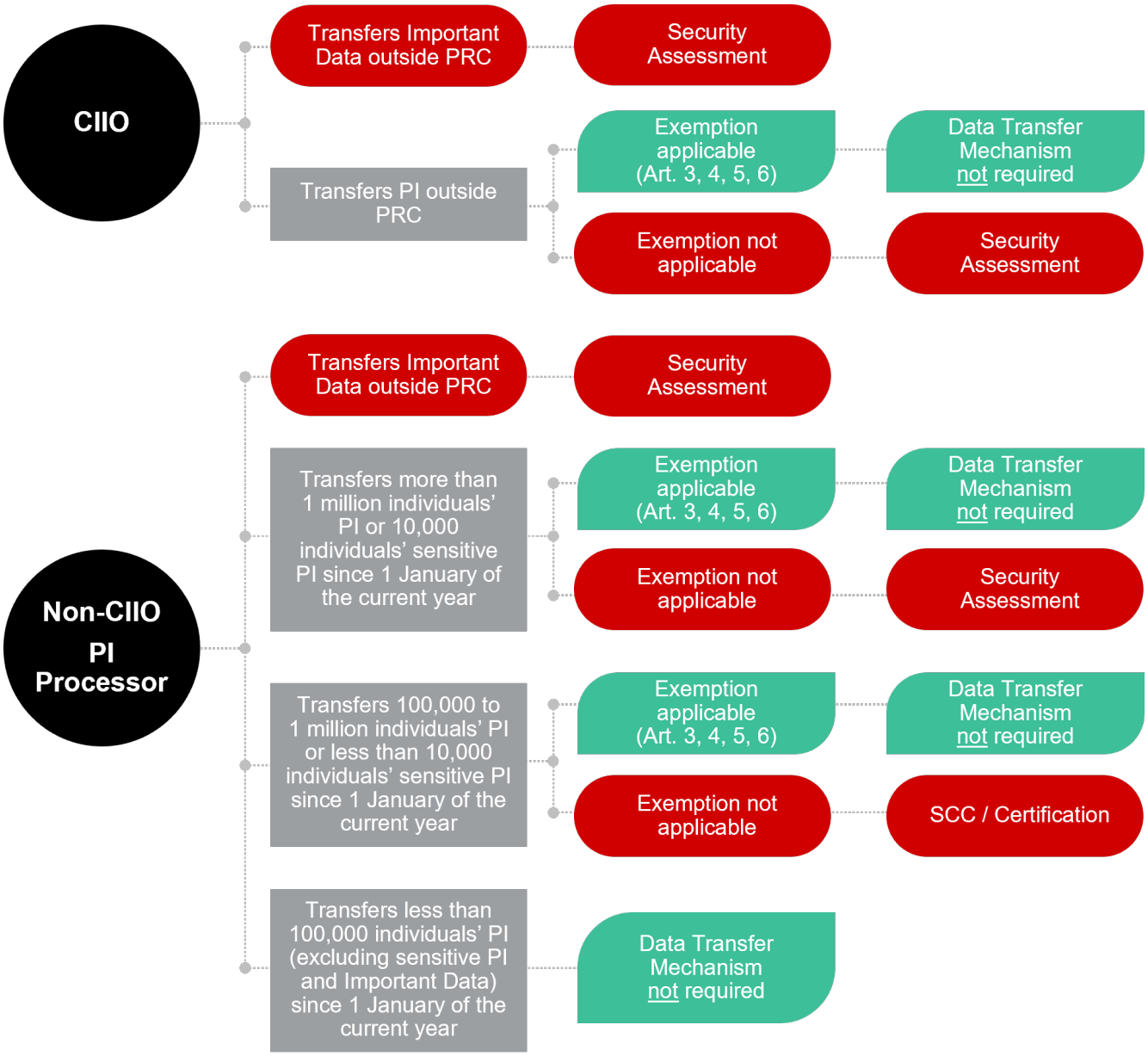
On 22 March 2024, the CAC published the final version of the Provisions on Promoting and Regulating Cross-Border Data Flows (see Chinese version) which took effect immediately and follows the draft published for consultation in September 2023. On the same day, the CAC also held a press conference (FAQ) (see Chinese version) on the Provisions and published the second edition of the Security Assessment Filing Guidelines and Filing Guidelines for the SCCs (see Chinese version).

Under the PIPL, in order to transfer PI out of the PRC, a PI Processor must, depending on the volume thresholds met, either:

- conduct and pass a security assessment;
- enter into standard contractual clauses published by the CAC with the overseas recipient (SCCs); *or*
- obtain a PI protection certification from an agency designated by the CAC (Certification, and together with the Security Assessment and SCCs, the Data Transfer Mechanisms).

The Provisions introduce exemptions to the Data Transfer Mechanisms and relax the existing volume thresholds which trigger the need for a Data Transfer Mechanism.

The Provisions



Exemptions for a Security Assessment, SCCs, or Certification

Data Transfer Mechanisms are *not* required if a data transfer falls within any one of the below circumstances:

Exemption	Commentary
Main Exemptions	
PI Generated Outside the PRC (Article 4)	Cross-border transfer of PI (including sensitive PI), which is collected and generated outside of the PRC, transferred to the PRC for processing, and then transferred back out, provided that no new PI or Important Data is introduced during the processing in the PRC.
Contractual Necessity (Article 5(1))	Cross-border transfer of PI (including sensitive PI) which is necessary for entering into and performing a contract to which the individual is a party, *such as* cross-border shopping, cross-border delivery and express, cross-border remittances, cross-border payment, cross-border bank account opening, air ticket and hotel reservations, visa processing, or exam services.
Necessary for Cross-Border HR Management (Article 5(2))	Cross-border transfer of employee's PI (including sensitive PI) which is necessary for implementing cross-border HR management in accordance with lawfully formulated labour rules and signed collective contracts. • While this is positive news for PRC companies that rely on centralised global HR systems, this exemption remains to be tested in practice and it is unclear how the CAC may interpret "necessary"; e.g., whether centralised HR systems are to be interpreted as "necessary" and what types of PI would be considered as *necessary* to export.
Vital Interests (Article 5(3))	Cross-border transfers of PI (including sensitive PI) necessary for protecting the life, health, and safety of persons in emergencies.
Low-Volume Transfers (Article 5(4))	A transfer in which a PI Processor that is not a CIIO transfers PI belonging to less than 100,000 individuals (excluding sensitive PI) since 1 January of the current year. • This exemption does *not* include the transfer of *sensitive PI,* i.e., in order for a transfer of sensitive PI to be exempt from a Data Transfer Mechanism, one of the other exemptions above must be relied on instead. • This exemption also does not apply to the export of Important Data as there is no volume-based exemption from Security Assessment for such export.
Other Exemptions / Clarifications	
Non-PI /Non-Important Data (Article 3)	Cross-border transfer of data collected and generated in activities such as international trade, cross-border transportation, academic cooperation, transnational manufacturing, and marketing and such data does *not* contain PI or Important Data.

	This aligns with existing laws and regulations, as non-PI and data not classified as Important Data has always been outside the scope of the PIPL.
FTZ Special Rules (Article 6)	Pilot free trade zones (FTZs) in the PRC can formulate their own negative list of data which would require a Data Transfer Mechanism. Such lists would need to be submitted to and approved by provincial offices of the CAC and filed with the CAC and State Data Bureau of China. Transfer of data which is not on the negative list would *not* be subject to a Data Transfer Mechanism.

For the exemptions tied to a legal basis under the PIPL (i.e., contract, HR administration, and vital interests), separate consent for cross-border data transfer is not required as it is required only if consent is the legal basis relied on. This was confirmed in the second version of the Security Assessment Filing Guidelines, which states that separate consent is not required for cross-border data transfers relying on a legal basis under Art. 13(2) - (7) of the PIPL.

Practically, in order to rely on an exemption under Article 5(1) – (3), a PI Processor must be able to demonstrate that the data export is necessary for one or more of the exempted purposes and it has sufficient documents in place to support such exemption. Examples include an employee contract / handbook explaining the use and necessity of a centralised HR system, and customer agreements with individuals for cross-border services.

Updated Thresholds for the Security Assessment, SCCs, or Certification

The Provisions introduce new thresholds for triggering a Data Transfer Mechanism, thereby relaxing the previous thresholds under the Security Assessment Measures and the Measures for the SCCs. The table below highlights the *changes* to the thresholds for triggering a Data Transfer Mechanism.

	Security Assessment Measures / Measures for the SCCs (thresholds superseded and no longer applicable)	**Provisions (effective from 22 March 2024 and the current legal position)**
Thresholds Triggering a Security Assessment		
Transfers of PI	Any PI transfers by PI Processors processing PI of over 1 million individuals	Deleted and replaced with the cumulative threshold requirements below
	More than 100,000 individuals' PI transferred since 1 January of the previous year	More than 1 million individuals' PI transferred since 1 January of the current year
Transfers of Sensitive PI	More than 10,000 individuals' sensitive PI transferred since 1 January of the previous year	More than 10,000 individuals' sensitive PI transferred since 1 January of the current year
Thresholds Triggering the SCCs/Certification		
Transfers of PI	Less than 100,000 individuals' PI transferred since 1 January of the previous year	Less than 1 million individuals' PI transferred since 1 January of the current year
Transfers of Sensitive PI	Less than 10,000 individuals' sensitive PI transferred since 1 January of the previous year	Less than 10,000 individuals' sensitive PI transferred since 1 January of the current year

Volume-Based Exemption From Any Data Transfer Mechanism		
Transfers of PI	No exemption from any Data Transfer Mechanism based purely on volume	Less than 100,000 individuals' PI (excluding sensitive PI) transferred since 1 January of the current year (see Article 5(4) of the Provisions), i.e., no Data Transfer Mechanism is needed
Transfers of Sensitive PI		No exemption from any Data Transfer Mechanism based purely on volume (see Article 5(4) of the Provisions)

Notably:

- What remains unchanged from the Security Assessment Measures and the Measures for the SCCs is that a Security Assessment is required if a CIIO transfers PI (if none of the exemptions under Article 3-6 apply) or if Important Data is transferred outside of the PRC.
- According to the CAC's FAQ, data transfers which rely on an exemption (except for the low-volume transfer exemption in Art. 5(4)) shall not be included when calculating the above thresholds.

Other Clarifications

Cross-Border Data Transfer Requirements Apply to Overseas PI Processors

The second version of the Security Assessment Filing Guidelines and Filing Guidelines for the SCCs clarify that if an overseas PI Processor who is subject to the extra-territorial application of the PIPL under Art. 3(2) processes the PI of individuals from the PRC, it would qualify as a cross-border data transfer. This was not previously included in the first edition of the guidelines. However, it still remains unclear how overseas PI Processors would, in practice, file for a Security Assessment or execute / file the SCCs, e.g., whether the filing or signing entity should be the overseas PI Processors' PRC local representatives appointed according to the PIPL, which are usually their subsidiaries, affiliates, or representative office in the PRC.

Important Data

According to Article 2 of the Provisions, PI Processors must identify and report Important Data as required by laws and regulations. Data only qualifies as Important Data if the CAC has notified the PI Processor of such qualification or has publicly identified such data as Important Data, e.g., via publication of Important Data catalogues. No industry-specific Important Data catalogues or reporting regulations have been released to date, but guidance is available in the recently released suggestive national standard GB/T 43697-2024 *Data security technology — Rules for data classification and grading* (see Chinese version).

PIPL Compliance Obligations Are Still Relevant

Although the Data Transfer Mechanisms may no longer apply to certain data transfers, PI Processors must continue to comply with other compliance obligations under the PIPL, e.g., obtaining separate consent to transfer data (if consent is relied on as the legal basis), conducting privacy impact assessments as required by laws and regulations when transferring PI outside of the PRC, providing individuals with a privacy notice containing the required disclosure, or maintaining a record of processing.

Centralised Online Filing System

The CAC launched a centralised online platform for the submission of Security Assessment and SCC filings. PI Processors that qualify as CIIOs, as well as "other cases that are not appropriate for online submission" (which still remains unclear in practice), are still required to submit their filings in written form to the provincial-level CACs.

Next Steps

PI Processors that have been taking steps to comply with the previous PRC cross-border data transfer regulations (e.g., adopting one of the Data Transfer Mechanisms) should revisit their internal and external policies and agreements to assess whether they can take advantage of the relaxed requirements under the Provisions to ease their compliance burden.

The CAC also provided guidance for PI Processors that have previously submitted filings:

- Companies that previously did not pass the Security Assessment but are now exempt from the Security Assessment under the Provisions can proceed with PI transfers outside the PRC by utilising SCCs or obtaining certifications.

- Companies which are still undergoing the Security Assessment / SCC filing process but can now rely on an exemption can either choose to continue with the filings (in which case their self-assessment and applications will likely need to be updated) or withdraw their applications.

However, PI Processors should continue to take a number of compliance steps, including:

- monitoring existing and new data transfer activities to determine whether they can rely on an exemption. They can do so by continually assessing whether the data transfer is below the prescribed volume thresholds, or fulfils the condition for the exemption (e.g., it is indeed "necessary" for the performance of a contract or HR management); and

- identifying whether Important Data is collected, and monitoring any Important Data catalogues published by the CAC.

Regulated PI Processors should also consider whether they are subject to additional industry-specific obligations under other PRC regulations and measures.

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

Bianca H. 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 and Hong Kong Publish Standard Contract for Transferring Personal Information Within GBA Area

China's New AI Regulations

China Clarifies the Personal Information Protection Certification Regime