The Final Piece of China's Cross-Border Personal Information Transfer Regulations

A brief review of the Measures for Certification of Cross-Border Personal Information Transfer

By David Pan | Nigel Zhu | Susan Deng

On October 14, 2025, the Cyberspace Administration of China (CAC) and the State Administration for Market Regulation (SAMR) jointly issued the "Measures for Certification of Cross-Border Personal Information Transfer" (hereinafter referred to as the "Measures"), which will take effect on January 1, 2026. The issuance of the Measures marks the completion of the regulatory framework for the three legal pathways for cross-border personal information transfers established by the Personal Information Protection Law (PIPL): security assessment, standard contract, and certification. As a critical component in perfecting China's regulatory system for cross-border data transfers, the Measures provide a new compliance option for personal information export activities and hold profound significance for promoting the secure and orderly cross-border flow of data elements and for guiding corporate compliance practices. This article aims to provide a legal analysis of the core systems of the Measures and to predict to its future implementation.

1. Scope of Application

Article 5 of the Measures clearly defines the conditions under which certification is applicable as a pathway for cross-border transfers. A personal information exporter choosing this path must meet all of the following three conditions:

- **Type of data exporter:** The exporting entity must be a "non-critical information infrastructure operator" (non-CIIO). This provision continues the principle within China's data security legal framework of imposing the strictest supervision on operators of critical information infrastructure operators (CIIOs), whose transfers of any personal information and important data abroad are required to undergo a security assessment organized by the CAC.

For more Llinks publications, please contact:

Publication@llinkslaw.com

- **Threshold for Data Processing Volume:** A clear quantitative range has been set, namely "cumulatively providing the personal information (excluding sensitive personal information) of more than 100,000 but less than 1 million individuals to overseas recipients since January 1 of the current year" or "the sensitive personal information of less than 10,000 individuals." (It is worth noting that our understanding is that the "Provisions on Promoting and Regulating Cross-Border Data Flow" (hereinafter the "Cross-Border Flow Provisions") issued by the CAC in March 2024 also apply to certification for cross-border personal information transfers. Therefore, personal information exporters should assess whether the data export meets the exemption criteria listed in Article 5 of the Cross-Border Flow Provisions, such as being "necessary for the conclusion or performance of a contract" or "necessary for human resources management." If these conditions are met, a cross-border transfer certification is not required, even if the aforementioned volume thresholds are exceeded).
- **Restriction on Data Type:** It is explicitly stated that the exported personal information "does not include important data." The cross-border transfer of important data is strictly limited to the security assessment pathway to safeguard national security and the public interest.

2. Certification vs. Standard Contract

According to current regulations, provided that the cross-border transfer is not exempt and does not trigger a mandatory security assessment, a personal information exporter can, in theory, choose either the standard contract or personal information protection certification as the pathway for the transfer.

The main differences between the two lie in their compliance models and applicable scenarios. The standard contract mechanism is based on the contractual obligations of the two signing parties. It offers flexibility and is suitable for point-to-point, relatively simple transfer scenarios. In contrast, personal information protection certification involves an independent, third-party professional institution conducting a holistic assessment and endorsement of a personal information exporter's systematic and continuous data export activities. For scenarios such as intra-group data sharing within large multinational corporations or business models involving frequent data transfers to multiple overseas entities, obtaining a certification to cover a series of processing activities may offer advantages in data processing efficiency and management costs, compared to signing and managing standard contracts with each recipient individually.

A special consideration when choosing between a standard contract and certification is the practical dilemma that can arise with standard contracts. Since the standard contract must be signed by both the domestic exporter and the overseas recipient, situations often occur where the overseas recipient is unwilling or unable to sign (for example, where the foreign recipient is a government authority, or an important client), making it impossible to use the standard contract pathway. If the certification mechanism emphasizes the evaluation of the exporter, the overseas recipient, and the transfer activities themselves without requiring a signed agreement between the two parties, it could help resolve this predicament associated with the standard contract.

3. Pre-requisite Compliance Obligations

Article 6 of the Measures stipulates that the fundamental obligations under the PIPL must be fulfilled before applying for certification, including the obligation to inform, obtain separate consent from individuals, and conduct a Personal Information Protection Impact Assessment (PIA). This provision does not create new obligations but rather emphasizes the rigid application of these procedural requirements in the context of certification. The Measures further detail six key assessment areas for a PIA, covering core elements such as the legality of the basis for processing, risk assessment, the safeguarding capabilities of the overseas recipient, channels for individuals to protect their rights and interests, and the impact of the legal environment in the overseas jurisdiction.

Among the pre-requisite obligations, the PIA report is particularly important. The PIA report serves as the foundation for an exporter to demonstrate its compliance capabilities and is a key basis for the certification body's review; its quality directly impacts the outcome of the certification. The PIA must go beyond the perspective of a single data transfer and comprehensively assess the robustness of policies, procedures, and technical controls for all relevant transfer activities within the scope and validity period of the certification.

4. Effect of Certification

- **Scope of Certification:** Certification is not a blanket permission for all of a personal information exporter's cross-border data transfer activities. Articles 9 and 10 of the Measures clarify the legal status of the "scope of certification," requiring that the certificate must specify the business scenarios it covers, the types of personal information, the purposes of processing, the retention period after transfer, the overseas recipients involved, etc. Any cross-border transfer of personal information that falls outside the certified scope is not covered by the certification and constitutes a violation. If discovered, the professional certification body has the authority to suspend or even revoke the relevant certification.
- **Validity Period of Certification:** Article 8 of the Measures stipulates that the validity period of a certification certificate is 3 years. This provision is significant on two levels: on one hand, it provides a medium-term, stable legal expectation for corporate business activities and compliance planning; on the other hand, it ensures that the certification status is not permanent, requiring that the personal information processor's compliance level undergo periodic re-evaluation to adapt to business changes and updates in laws and regulations.
- **Renewal Mechanism:** Article 8 further provides that if the certificate needs to be used beyond its expiration, the personal information processor must submit a renewal application at least 6 months before the validity period ends.

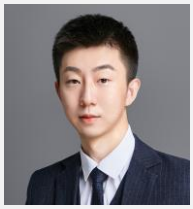
5. Implementation and Outlook: Unification and Refinement of Certification Rules

The introduction of the Measures completes the final piece of the puzzle for China's personal information export framework, but it also leaves some issues to be clarified in the future. The Measures do not specify

the certification rules, implementation details, or technical specifications for cross-border personal information transfers. The CAC and SAMR previously issued the "Announcement on the Implementation of Personal Information Protection Certification" (hereinafter the "Announcement") in 2022. The Announcement stated that certification for cross-border personal information transfers must follow the "Cybersecurity Standards Practice Guide—Security Certification Specification for Cross-Border Personal Information Processing Activities" (the "Certification Specification"). However, according to the Certification Specification, its scope is limited to (1) cross-border transfers of personal information within multinational corporations or between entities within the same group, and (2) the processing of personal information of individuals within China by entities outside of China. This scope is significantly narrower than that of the standard contract. Furthermore, the Certification Specification requires a "legally binding agreement" to be signed between the data exporter and the overseas recipient. If this remains the case, the materials required for certification and the standard contract would be nearly identical, which would greatly diminish the advantages of certification. Therefore, we hope regulatory authorities would introduce certification specifications and detailed rules that are aligned with the new Measures to resolve these issues and leverage the unique advantages of the certification pathway.

If you would like to know more information about the subjects covered in this publication, please contact:

David Pan
+86 21 3135 8701
david.pan@llinkslaw.com



Nigel Zhu
+86 21 3135 8683
nigel.zhu@llinkslaw.com

Susan Deng
+86 21 6043 3793
susan.deng@llinkslaw.com

SHANGHAI	BEIJING	SHENZHEN
19F, ONE LUJIAZUI 68 Yin Cheng Road Middle Shanghai 200120 P.R.China T: +86 21 3135 8666 F: +86 21 3135 8600	30F, Central Tower, China Overseas Plaza, 8 Guanghuadongli, Chaoyang District Beijing 100020 P.R.China T: +86 10 5081 3888 F: +86 10 5081 3866	18F, China Resources Tower 2666 Keyuan South Road, Nanshan District Shenzhen 518063 P.R.China T: +86 755 3391 7666 F: +86 755 3391 7668

HONG KONG	LONDON
Room 3201, 32/F, Alexandra House 18 Chater Road Central, Hong Kong T: +852 2592 1978 F: +852 2868 0883	1/F, 3 More London Riverside London SE1 2RE United Kingdom T: +44 (0)20 3283 4337 D: +44 (0)20 3283 4323

www.llinkslaw.com

Wechat: LlinksLaw

WE LINK LOCAL LEGAL INTELLIGENCE WITH THE WORLD