Updates
September 12, 2022

China Increases Security Measures on Cross-Border Data Transfers

In order to regulate cross-border data transfers in accordance with the Cybersecurity Law, the Data Security Law, and the Personal Information Protection Law, the Cyberspace Administration of China (CAC) released the *Measures for the Security Assessment of Cross-border Data Transfer* (Measures) on July 7, 2022, effective on September 1, 2022. The Measures provide a six-month grace period from September 1, 2022, to March 1, 2023, for companies with prior and existing cross-border data transfer activities to comply with the new standards.

Scope of Application

The Measures apply to cross-border data transfers that fit the definition of "important data" and "personal information" with a minimum threshold for common processors and no threshold for critical information infrastructure operators (CIIO). According to Article 19 of the Measures, important data refers to "any data, the tampering, damage, leakage, or illegal acquisition or use of which, if it happens, may endanger national security, the operation of the economy, social stability, public health and security."

According to the guidance provided by the CAC at a Q&A session with media at the time of issuance, cross-border transfers occur when: (1) a company directly provides important data or personal information collected and generated in the course of its operations within the territory of China to overseas recipients and (2) when a company does not directly provide such data to an overseas recipient, but the overseas party can access transferred information from the company in China.

Assessment Types and Their Scopes of Applications

According to the Measures, the assessment for cross-border transfer of important data and personal information includes two sets of risk assessments, one self assessment to be completed by the transferer and another (the CAC security assessment) by CAC local offices at the provincial level (local CAC).

Risk self-assessments are required for all transferors who engage in cross-border transfers of important and personal data. In addition, the CAC security assessment is mandatory in the following scenarios:

- The data processor transfers important data outside of China.
- CIIO and the data processor handle the personal information of over one million individuals and transfer that personal information outside of China.
- The data processor has transferred the personal information of 100,000 individuals or the sensitive personal information of 10,000 individuals since January 1, 2021, on a cumulative basis.

The above circumstances for the CAC security assessment remain the same as in the version drafted for public comment and released in October 2021. The official version clarified the period for calculating the cumulative volume of personal information transferred abroad, which was unclear in the 2021 draft version.

Application Procedure for the CAC Security Assessment

The CAC security assessment application procedure includes the following steps:

1. Submission of completed risk self-assessment by the data processor.
2. Submission of the application to the local CAC.
3. Completion of review of the application documents by the local CAC within five business days of their receipt and the submission of completed documents to the national CAC by the local CAC.
4. Determination of acceptance or rejection by the national CAC within seven business days of document receipt.
5. Administration of a security assessment after a determination of acceptance. (Depending on individual application circumstances, relevant departments of the State Council, the local CAC, and other professional agencies may be involved in the assessment.)
6. Completion of the assessment within 45 business days of sending the acceptance notice to the data processor.
7. Granting of appropriate extension is allowed if the circumstances are complicated or application documents are incomplete.

Notably, the official version of the Measures omits the capped extension period of 60 business days. Also, the Measures provide a channel for applicants unhappy with the assessment results to apply for reassessment within 15 business days of notice. The reassessment results of the administrative appeal are final and binding.

Application Timing for the CAC Security Assessment

The CAC clarified during the media Q&A session that the application should be made before executing a cross-border transfer contract between the transferor and an overseas recipient. If the application is created after the execution of the contract, the contract should specify that it will go into effect only after the security assessment is passed to avoid potential interruptions to the business.

Focus of Assessments

The Measures provide the focus points for both the self-assessment and CAC security assessment, including the following relevant points:

- Legality, justification, and necessity related to the cross-border transfer.
- Data subject to the transfer and risk associated with the transfer.
- Data protection capabilities of the overseas recipient.
- Individual data privacy rights.
- Cross-border transfer contract between the data processor and the recipient.

In addition to the above assessment criteria, the CAC security assessment also includes an evaluation of the effects of changes in the data security laws, policies, and the cybersecurity environment of the countries or regions where the overseas recipient is located.

Reassessment

The Measures require data transferors to apply for reassessment in the following circumstances:

- Within 60 business days of the expiration of the previous assessment results, which occurs two years from the initial issuance date.
- If one of the following events occurs during the valid period of the assessment result:
    - Any change to the purpose, method, or scope of the outbound data transfer or the type of data; any change to the purpose or method of data processing by the overseas recipient that would affect the security of the outbound data; or if the period for retaining personal information or important data overseas is to be extended.
    - Any change in the data security protection policies, legislation, cybersecurity environment, or any other force majeure event that has occurred in the country or region where the overseas recipient is located; any change in the actual control of the data processor or overseas recipient; or any change to the legal document executed between the data processor and the overseas recipient that would affect the security of the outbound data.
    - Other circumstances that may affect the security of the outbound data.
- The CAC discovers that data transfer activities that previously passed the assessment no longer comply with data transfer requirements.

In order to ensure compliance, companies with outbound data transfers should seek knowledgeable counsel to monitor the implementation and enforcement of the Measures by the CAC.

Explore more in

Privacy & Security Corporate Law

Related insights

Update

Employers and Immigration Under Trump: What You Need To Know

Update

‘Tis the Season… for Cybercriminals: A Holiday Reminder for Retailers