China Issues Security Assessment Measures of Data Cross-border Transfer

Article By

Ruiqi Guo
Yuanmei Lu

Sheppard, Mullin, Richter & Hampton LLP
China Law Update Blog

Related Practices & Jurisdictions

- Communications, Media & Internet
- Consumer Protection
- Global
- Administrative & Regulatory
- China

Wednesday, August 10, 2022

On July 7, 2022, the Cyberspace Administration of China (“CAC”) released the *Security Assessment Measures of Cross-border Data Transfer* (the “Measures”) which will be effective from September 1, 2022. Previously on October 29, 2021, CAC has published a draft version of such Measures for public comments (which we covered in this blog post: [here](#)). In this blog post, we will present the major differences between this final version of the Measures and the prior draft version.

1. Triggering Scenarios

Article 4 of the Measures, which describes the scenarios under which data cross-border transfer will trigger governmental security assessment, has been updated. The final version provides the following four scenarios (we have underlined herein...
the provisions where updates have been made):

- transfer of important data;
- any critical information infrastructure operator or data processor which processes the personal information ("PI") of more than 1 million individuals;
- any data processor which has transferred the PI of 100,000 individuals or sensitive PI of 10,000 individuals abroad since January 1st of the previous year;
- other situations as stipulated by the CAC.

Regarding the definition of “important data”, the National Information Security Standardization Technical Committee published a draft version of “Information Security Technology – Guideline for Identification of Critical Data” on January 13, 2022, which specifies the general principles and factors for important data identification. We will discuss this later in a separate post.

Section (iii) listed above specifies the time frame for calculating the cumulative amount of PI transferred during a cross-border transfer. Accumulated since January 1 of the previous year means that the calculation period is limited to a maximum of 2 years. This adjustment will certainly mitigate compliance costs for companies with smaller amount of PI needing to be transferred.

In addition, it is worth mentioning that for the other PI processors who do not fall within the definition of the data processors as specified in Article 4 (i.e. those that handle less than 1 million PI, or those that have cumulatively transferred PI of less than 100,000 individuals since January 1 of the previous year)(“General PI Processors”), their cross-border transfer of PI may still be required to be filed with the CAC. To be compliant with Article 38 of the Personal Information Protection Law, if a General PI Processor choose to transfer PI abroad by entering into a standard contract, according to the draft of “Provisions on Standard Contract for Cross-Border Transfer of Personal Information” published for public comment by the CAC on June 30, 2022, the General PI Processor would need to file the standard contract and self-assessment report with the provincial branch of CAC within 10 business days after the effective date of such standard contract.

2. Self-Assessment and Governmental Assessment

According to Article 5 of the Measures, the following matters shall be included in the self-assessment report:

- the legality, reasonability, necessity of the purpose, scope, and manner of data cross-border transfer;
- the scale, scope, type, and sensitivity of the data to be transferred and the risks that the cross-border transfer of data may pose to the national security, public interests, rights and interests of any individuals or organizations;
- the obligations of foreign recipients, and whether the management, technical level and capabilities of foreign recipients can guarantee the security of the
data to be transferred;

- the risk of data being tampered, destructed, leaked, lost, transferred, illegal accessed or illegal used during and after the cross-border transfer, and whether there are mechanisms for individuals to exercise their rights etc.;

- whether the security protection responsibility and obligations are fully and comprehensively agreed to in the legal documents between the transferors and recipients;

- other matters that may affect the security of data cross-border transfer.

The specific matters to be considered during the governmental assessment process (provided in the Article 8 of the Measures) are substantially similar to those of the self-assessment process as described above, although the government would additionally review the legal environment of the recipients’ countries and the historical compliance records of the data processors.

3. Procedures and Timeline

The final version provides a more detailed description of the procedures and timeline of the governmental assessment process. First, a data processor should submit application to the local provincial branch of the CAC, and the provincial branch of the CAC shall confirm the submitted documents within 5 business days and then send them to the CAC. Then, the CAC should determine whether to accept such application and notify the data processor its decision in writing within 7 business days from the date of receipt of such documents from its local branch. Next, the CAC shall complete the governmental assessment within 45 business days from the date of issuance of the aforesaid written notice of acceptance. The timeline can be reasonably extended if the CAC considers the case is complicated or additional documents are needed. Once a governmental assessment is completed and approval is granted, such approval is valid for two years.

The Measures will be effective from September 1, 2022, and it provides 6-month transition period starting from September 1, 2022 for the data processors who have been transferring their data overseas before the effective date of the Measures to be compliant with the Measures. The applicable multinational companies should carefully consider the companies’ business modes, the cost of security assessment, the cost of relocating database, and prepare practical plans during this transition period.

Copyright © 2022, Sheppard Mullin Richter & Hampton LLP.

National Law Review, Volume XII, Number 222