JUNHE BULLETIN

JUNHE

July 14, 2022

Data Protection Law

China Releases New Requirements on Cross-Border Data Transfers

On August 20, 2021, China passed the Personal Information Protection Law (PIPL), which was the first national level personal information protection law in China. Specifically, Article 38 of the PIPL sets forth three legal ways to transfer personal information outside of China, which are: (1) pass the security assessment by the Cyberspace Administration of China ("CAC"); (2) obtain certification of data security by a professional agency recognized by CAC; or (3) enter into an agreement with the overseas recipient with provisions governing the rights and obligations of the parties based on a standard contract to be released by CAC.

The most recent developments concern security assessment by CAC and standard contract.

I. Measures for Security Assessment of Cross-border Data Transfers

On July 7, 2022, the final version of the *Measures for Security Assessment of Cross-border Data Transfers* (the "**Measures**") was released. They will take effect on September 1, 2022. We set out below some of the key points from the Measures.

1. **The conditions subject to security assessment by CAC**

Article 4 of the Measures specifies that before any cross-border transfer of data, personal information processors and critical information infrastructure (CII) operators must undergo security assessment conducted by CAC if ***any*** of the following conditions are met:

1) The transfer of personal information and important data[1]generated by CII operators;

2) The transfer of important data;

3) The transfer of personal information by a personal information processor that has processed more than one million persons' personal information; or

4) The transfer of the personal information of 100,000 persons or more, or the transfer of the sensitive personal information of 10,000 persons or more.

2. **The process and timeline of security assessment**

[1] *Information Security Technology - Guideline for Identification of Important Data* (draft for comments) promulgated by the State Administration for Market Regulation and the National Information Security Standardization Technical Committee on January 13, 2022, defines "*Important Data*" as *"Data that exists electronically, and once it is tampered with, destroyed, leaked, or illegally obtained or utilized, national security and public interests may be endangered.*

1) According to Article 5 of the Measures, the data processor should first conduct a risk self-assessment before they apply to a provincial CAC for security assessment. After the data processor completes the self-assessment, the data processing entity needs to apply to CAC at the provincial level for review.

2) The documents to be submitted to CAC contain, among others, an application form, a data transfer risk self-assessment report, and a contract signed by the foreign recipient. Once CAC receives the application, the provincial CAC must decide within five working days whether the application documents submitted are complete. If the documents are complete, the provincial CAC will forward the application to the central CAC.

3) Upon receipt of the application, CAC will decide within seven working days whether an application has been accepted and inform the applicant in writing once the application is accepted. CAC must conduct the evaluation within 45 working days and inform the applicant of the decision in due course. If the application is complex, CAC may extend the time period, provided that the applicant has been notified of the anticipated extension period.

4) During the review, CAC will mainly focus on the following aspects of the data transfer:

   a. The legality, legitimacy and necessity of the purpose, scope and method of the outbound data transfer and data processing by the overseas recipient;

   b. The scale, scope, type and sensitivity of the data to be transferred, and the risks to national security, public interests or the legitimate rights and interests of individuals or organizations caused by the outbound data transfer;

   c. The responsibilities and obligations that the overseas recipient promises to undertake, and whether the overseas recipient's management and technical measures and capabilities for performing its responsibilities and obligations can guarantee the security of the outbound data transfer;

   d. The risk of the data being tampered with, destroyed, divulged, lost, transferred, illegally obtained or illegally used during and after the outbound data transfer;

   e. Whether the channel for the maintenance of personal information rights and interests is smooth;

   f. Whether the contract signed by the cross-border recipient covers the responsibilities and obligations in relation to data security and protection; and

   g. Other matters required by CAC.

5) If the applicant is dissatisfied with the assessment results, it is entitled to apply to CAC for re-evaluation within 15 working days from receipt of the result. The re-evaluation result will be the final conclusion.

3. The validity period for a security assessment result and re-assessment

The security assessment result is valid for two years. The data processor may need to re-submit an application if any of the following circumstances occur during the two-year period:

1) The purpose, method, scope and type of the outbound data transfer, or the purpose and method of the data processing by the overseas recipient have changed or the cross-border storage period of personal

information and important data needs to be extended;

2) The security of the data transferred abroad is affected due to changes in the data security protection policies or regulations or the cybersecurity environment of the country or region where the overseas recipient is located, any other force majeure event, or any change in the actual control rights of the data processor or the cross-border recipient, or any change in the legal documents between the data processor and the overseas recipient; and

3) Any other circumstances affecting the security of the transferred data.

If a data processor wishes to continue the cross-border transfer of data after the original validity period expires, it needs to apply for a re-assessment within 60 working days of the expiration of the original validity period.

II. Draft Regulations on Standard Contract for Personal Information Export

On June 30, the Cyberspace Administration of China released the draft *Regulations on Standard Contract for Personal Information Export* (the "**Draft Regulations**"). As mentioned above, the standard contract is one of the legal mechanisms that data processors may undertake to transfer personal information overseas under Article 38 of the PIPL.

Under the Draft Regulations, data processors are eligible to transfer data overseas by signing a standard contract if the data processor can meet ***all*** of the following requirements:

1. It is not a critical information infrastructure operator (CIIO).
2. It processes the personal information of less than one million people.
3. It has transferred less than 100,000 people's personal information out of China since January 1 of the previous year.
4. It has transferred less than 10,000 people's "sensitive" personal information out of China since January 1 of the previous year.

The parties to the standard contract are limited to the data processor and the foreign recipient. In this regard, it is unclear whether authorized parties located in China are able to transfer information through such a mechanism. In addition, the standard contract shall specify certain contents, which is set out as a template standard contract attached to the Draft Regulations.

The signed standard contract and a personal information protection impact assessment report would need to be filed with the Chinese government within 10 working days of the standard contract taking into effect. The Draft Regulations do not set out whether anonymization could be applied to the contract submitted to CAC.

III. Implications.

1. Data processors that must pass security assessment by CAC are also required to sign a contract with the foreign recipients. These requirements are seen in the Measures and some guidelines issued by CAC. However, neither CAC nor other relevant authorities specify the template contract to be signed in such circumstances. It is recommended that the Standard Contract issued may be used for reference purposes.
2. The scope of self-assessment under the Draft Regulations includes assessment on the impact of foreign laws and policies on the performance of the Standard Contract. As such, companies may need to engage foreign law firms to provide legal advice to satisfy the self-assessment requirements.

3. Some multinational corporations in China may have signed a data transfer agreement within group entities to meet the requirements of GDPR. It is advisable that these companies attach the standard contract as an appendix to the existing cross-border data transfer agreement (if any) or specify in the agreement that the standard contract applies where a PRC data processor is involved.
4. Considering that these laws and rules imposed expansive compliance obligations on data processors, companies conducting business in China should reassess their information category systems and consult Chinese counsel before transmitting such information overseas.

Weining ZOU	Partner	Tel: 86 10 8519 1343	Email: zouwn@junhe.com
Jinwen YANG	Partner	Tel: 86 10 8553 7608	Email: yangjw@junhe.com
Yi Sun	Associate	Tel: 86 10 8553 7867	Email: suny_Stefanie@junhe.com
Yuanyuan LI	Associate	Tel: 86 10 8540 8665	Email: liyuanyuan@junhe.com