BCLP. Client Intelligent

Insights

PRC LEGAL UPDATE: CHINA'S SECURITY ASSESSMENT PROCESS OF OUTBOUND DATA TRANSFERS

Oct 31, 2022

Under the PRC Cybersecurity Law, PRC Personal Information Protection Law and PRC Data Security Law, certain organisations (as well as individuals) are now required to conduct a security assessment of outbound transfers of important data and personal information. In accordance with the rules of such laws, the PRC Measures for the Security Assessment of Outbound Data Transfer (the "Measures") were announced on 7 July 2022, and took effect on 1 September 2022.

On the same day, to provide guidance and assistance to "data processors" on the security assessment application process, the PRC Cyberspace Administration of China (the "CAC") issued the Application Guidelines for Security Assessment of Outbound Data Transfer (1st Edition) (the "Guidelines"). The Measures and the Guidelines set out the circumstances under which a security assessment is required for outbound data transfers and the procedure for applying for such security assessment. Data processors already engaging in outbound data transfers are required to conduct any required assessments by 1 March 2023.

To help organisations navigate this process, we set out in this brief alert the key issues that companies need to be aware of under the Measures and the Guidelines and a description of the steps in the application process.

WHO IS REQUIRED TO APPLY FOR SECURITY ASSESSMENT ON OUTBOUND DATA TRANSFER?

Data processors[1] engaging in certain outbound transfers of important data and/or personal information must complete a security assessment process prior to engaging in the relevant transfers. Specifically, the security assessment application process must be completed for the transfer of important data and/or personal information out of China under the following circumstances:

- Transfer of "Important data" out of China by data processors;
- Transfer of personal information out of China by "Critical Information Infrastructure" operators;

- Transfer of personal information out of China by data processors that have processed personal information of over 1 million individuals; or
- Transfer of personal information out of China by organisations that have processed personal information of over 100,000 individuals or sensitive personal information of over 10,000 individuals since January 1 of the previous year.

Important data is defined in the Measures as any data which, if tampered with, destructed, divulged, or illegally acquired or used, may endanger national security, economic operation, social stability or public health and security. This term is vague and could be interpreted broadly. The PRC Data Security Law requires that the relevant governmental authorities shall formulate specific catalogues of important data in the relevant regions, sectors and industries under their respective jurisdictions. Therefore, companies should pay attention to any such catalogues as announced by the PRC government from time to time to determine whether their outbound data transfers involve any important data.

The PRC Cybersecurity Law describes Critical Information Infrastructure to include important industries and sectors, such as public communication and information services, energy, transportation, water conservancy, finance, public services, e-government affairs, and other critical information infrastructure which, if destructed, dysfunctional, or subject to data leakage, may severely impair the national security, national economy, people's livelihood or public interest. A definitive list in this regard has not yet been provided such that it may not always be clear whether an organisation falls within this category or not.

WHAT ACTIVITIES ARE CONSIDERED AS OUTBOUND TRANSFER OF DATA?

As noted above, in order to trigger the security assessment requirement, a qualifying organisation also has to engage in outbound transfers of important data or personal information from China. The following situations are considered to be outbound transfers:

- The actual transfer or storage outside of China of the data collected or generated during operations within China;
- The storage in China of data collected or generated by the data processor but such information is accessible to organisations or individuals outside of China.

APPLICATION PROCEDURES

To the extent a data processor is required to submit the security assessment application, the procedures set out by the Guidelines include the following steps:

- The applicant conducts a self-assessment of the risks regarding out-bound data transfer and prepares a report of such self-assessment.

- The applicant submits the application documents (including the self-assessment report) to the local provincial branch of the CAC, which, upon reviewing and confirming the completeness of such documents within 5 working days, will forward the documents to the CAC.
- The CAC will confirm within 7 working days upon receipt of the documents whether it will accept the application and inform the applicant of its decision in writing. The CAC may request additional documents or request amendment of the existing application documents and the applicant must promptly submit additional or amended documents as requested. Failing to do so without any justified reason will result in the termination of the security assessment review. If needed, the CAC may extend the period for the security assessment review. The CAC may decline the application if it is of the view that the data transfer is not subject to the security assessment, in which case, the applicant may conduct outbound data transfer pursuant to other means as set out under the law, such as by entering into a data transfer contract with the data recipient.
- The CAC will complete the security assessment within 45 working days upon the issue of the notice of acceptance.
- The CAC will issue a notice about the result of the security assessment to the applicant. The applicant must then follow the requirements under the notice (as well as the general requirements under applicable law) to carry out or refrain from carrying out (as the case may be) its outbound data transfer activities.
- If the applicant is not satisfied with the result of the assessment, it can apply to the CAC for re-examination within 15 days of receipt of the notice of result. Any decision made by the CAC after such re-examination will be considered final.

According to the Measures, the focus of the security assessment of outbound data transfers is on assessing the risks that the outbound data transfers may endanger national security, public interest, or the lawful rights and interests of individuals or organisations, covering primarily the following aspects:

- the legality, legitimacy, and necessity of the purpose, scope, and method, among others, of the outbound data transfer;
- the impact of the data security protection policies and regulations and cybersecurity environment of the country or region where the overseas recipient is located on the security of the data to be transferred, and whether the extent of data protection of the overseas recipient satisfies the requirements under the PRC laws and regulations;
- the size, scope, type, and sensitivity of the data to be transferred abroad, and the risk that the data may be tampered with, destroyed, divulged, lost, transferred, illegally obtained, or illegally used, among others, during and after the outbound transfer;

- whether data security and personal information rights and interests are fully and effectively safeguarded;
- whether data security protection responsibilities and obligations are sufficiently included in the legal documents to be concluded between the data processor and the overseas data recipient; and
- general compliance with the PRC laws and regulations.

APPLICATION DOCUMENTS REQUIRED

The following application documents are required to be submitted to the CAC for the security assessment:

1. Copies of the business license of the data processor and the ID document of the legal representative of the data processor;
2. Copies of the relevant contracts or other legally binding documents to be entered into between the data processor and the overseas data recipient;
3. Power of attorney in respect of the person handling the application;
4. Application letter regarding the outbound data transfer; and
5. Self-assessment report on outbound data transfer risks. According to the template set out in the Guidelines, this report is expected to detail, among other things, the process, time, methods and result of self-assessment, the risks and issues discovered, the corrective measures taken and effect of corrective measures, relevant information regarding the data processor, its business, data processing system(s), data to be transferred and data protection capability, information on the overseas data recipient, and the terms of the relevant legal documents to be concluded between the data processor and the data recipient.

The Guidelines include templates for items (3)-(5) above. All documents must be submitted in Chinese or a Chinese translation must be provided.

VALIDITY PERIOD

The result of the security assessment for outbound data transfer issued by the CAC will be valid for two years, provided that, if certain designated changes have occurred, the data processor must apply for a new assessment.

Such designated changes include:

1. any change in the purpose, method, or scope of the outbound data transfer or the type of data, or the purpose or method of data processing by the overseas recipient, which affects the security of

the data transferred out of China, or the period for the storage of personal information outside of China is extended; and

2. any change in the data security protection policies or regulations or the cybersecurity environment or the occurrence of any other force majeure event in the country or region where the overseas data recipient is located, any change in the actual control of the data processor or the overseas data recipient, or any change in the legal documents entered into between the data processor and overseas recipient, and other changes which may affect the security of the data transferred out of China.

CONCLUSION

Based on the scope established by the Measures, the general, outbound transfers of most small and medium sized companies are unlikely to fall under the scope of the security assessment requirements. Companies that are likely to be impacted include: (i) those operating in regulated industries such as telecommunications, energy and resources, transportation, finance, banking, health care, military and government related services, or (ii) those involved in e-commerce platforms or that have large operations in China and process a large volume of personal data above the relevant thresholds set out under the Measures. Therefore, companies should as a first step evaluate their own cross-border data transfer practices to determine whether they are subject to the security assessment requirements, document this assessment and proceed accordingly. Although these rules are new and not clear in all circumstances, this is an important step as violations of the relevant rules under the Measures may lead to fines and administrative penalties imposed by the PRC authorities, including orders of suspension or cessation of operations in China for serious violations.

For cross-border transfers of data that do not trigger the security assessment obligations under the Measures, there are still steps that companies may need to take to comply with PRC law, including the requirement to obtain a personal information protection certification by a qualified professional institution, or to enter into a contract with the overseas data recipient in accordance with the standard form of contract announced by the CAC to agree on the parties' rights and obligations. Please stay tuned for our next alert on these obligations.

---

[1] "**Data processor**" is defined under the PRC Personal Information Protection Law as an organisation or individual that independently decides the purposes and methods of processing during information processing activities. "**Data processing**" is defined under the PRC Data Security Law to include, but not be limited to, the collection, storage, use, processing, transmission, provision and public disclosure of data.

RELATED CAPABILITIES

- Data Privacy & Security

MEET THE TEAM

Amy de La Lama

Boulder

amy.delalama@bclplaw.com
+1 303 417 8535

Christian M. Auty

Chicago

christian.auty@bclplaw.com
+1 312 602 5144
