BCLP. Client Intelligent

Insights

PRC LEGAL UPDATE: CHINA'S SCCS AND PERSONAL INFORMATION PROTECTION CERTIFICATION FOR OUTBOUND DATA TRANSFERS

Apr 03, 2023

After much anticipation by organisations both in and out of the PRC, the new standard contractual clauses have been issued by the Chinese regulatory authorities as a means to permission the cross-border transfer of personal information under the PRC Personal Information Protection Law. We have prepared this alert to help companies understand when they may utilize the SCC Approach (as defined below) as well as the underlying obligations contained in such standard contractual clauses. To help put this development in context, we also discuss the broader privacy framework in relation to the SCC Approach and the alternative PIP Certification Approach (as defined below).

Regulatory Framework

Under Article 38 of the PRC Personal Information Protection Law, a data processor[1] is required to meet one of the following conditions before transferring personal information to overseas recipients for the purpose of its business needs: (i) passing the security assessment on outbound data transfer organised by the Cyberspace Administration of China (the "**CAC**") (the "**Security Assessment Approach**"); (ii) obtaining the personal information protection certification from an authorised certification institution (the "**PIP Certification Approach**"); (iii) concluding a contract with the overseas recipient based on the standard contract announced by the CAC (the "**SCC Approach**"); ***or*** (iv) as otherwise permitted under the law or by the CAC. The specific approach that may be utilised by an organization depends on the type of organisation involved as well as the organisation's data flow activities (as further described below).

In order to implement such rules, various measures have been issued by the PRC government. Specifically, on 7 July 2022, the Measures for the Security Assessment of Outbound Data Transfer were announced and took effect on 1 September 2022, and on 4 November 2022, the Personal Information Protection Certification Implementation Rules (the "**PIP Certification Rules**") were announced and took effect on the same day. Finally, on 22 February 2023, the Measures on Standard Contract for Outbound Transfer of Personal Information (the "**SCC Measures**") as well as the corresponding standard contract clauses (the "**Standard Contract**") were announced. The SCC Measures will take effect on 1 June 2023.

We previously outlined the requirements and process with respect to the Security Assessment Approach in an earlier alert titled "China's Security Assessment Process of Outbound Data Transfers" (click *link* for details) (the "**Security Assessment Alert**"). In particular, the following outbound transfers of data are subject to a mandatory government led security assessment process:

- outbound transfers of "important data";
- outbound transfers of personal information by critical information infrastructure operators ;[2]
- outbound transfers of personal information by data processors that have processed personal information of over 1 million individuals; and
- outbound transfers of personal information by data processors that have transferred personal information of over 100,000 individuals or transferred sensitive personal information of over 10,000 individuals abroad since 1 January of the previous year.

In this instalment, we focus on key issues regarding the SCC Approach as well as the PIP Certification Approach.

Part 1: SCC Approach

Eligibility for the SCC Approach

As noted above, one way that companies can permission the outbound transfer of personal information to other countries is to implement the Standard Contract and comply with the broader SCC Approach. However, only certain organisations can utilise this approach. Specifically, a data processor may only carry out the outbound transfer of personal information[3] with the SCC Approach if the processor meets all of the following conditions:

- It is not a "Critical Information Infrastructure" operator;
- It has not processed personal information of more than 1 million individuals;
- It has not transferred out of China personal information of more than 100,000 individuals since 1 January of the previous year; and
- It has not transferred out of China sensitive personal information of more than 10,000 individuals since 1 January of the previous year.

Essentially, a data processor that is not subject to the government-led mandatory Security Assessment Approach may adopt either the SCC Approach or the PIP Certification Approach. It is important to note that the SCC Measures prohibit a data processor from taking steps to circumvent the Security Assessment Approach, such as splitting the processing of personal information across

different batches and concluding multiple Standard Contracts to transfer personal information that should have been subject to the Security Assessment Approach according to the law.

Content of the Standard Contract

The Standard Contract is currently only available in Chinese and must be governed by PRC law. The Standard Contract includes the following major elements:

- definitions of key terms;
- obligations of the data processor and the overseas recipient;
- obligations to assess the impact of the personal information protection policies and regulations of the country or region where the recipient is located on the performance of the contract;
- rights and remedies of the data subjects and related third party beneficiary rights that may be enforced against the data processor or overseas recipient by filing a complaint with regulatory authorities or through court proceedings in competent PRC courts;
- termination provisions;
- liabilities for breach of contract, governing law and a dispute resolution mechanism;
- an appendix addressing factual information on outbound transfer of personal data (such as purpose and means of processing the personal information, volume and type of personal information being transferred, type of sensitive personal information being transferred, etc.); and
- if needed, an appendix on additional clauses agreed to by the parties.

Concerning the last element, such additional clauses may not contradict the existing terms of the Standard Contract, and in the event of any inconsistency between the terms of the Standard Contract and additional terms agreed by the parties, the terms of the Standard Contract will prevail.

Filing of the Standard Contract and Personal Information Protection Impact Appraisal

The data processor must file the signed Standard Contract with the local CAC authority (provincial level) within 10 days of it becoming effective. This filing must include a copy of the Standard Contract itself as well as a personal information protection impact appraisal report.

Thus, the personal information protection impact appraisal should be prepared prior to the outbound transfer of personal information. It should address the following:

- the legality, appropriateness and necessity of the purpose, scope and method of the processing of personal information by the data processor and the overseas recipient;
- the scale, scope, type, and sensitivity of the outbound transfer of personal information, as well as the risks to personal rights and interests that may be caused by the outbound transfer of personal information;
- the obligations assumed by the overseas recipient, and whether the management and technical measures and capabilities for fulfilling obligations can guarantee the security of personal information being transferred abroad;
- the risk of personal information being tampered with, destroyed, leaked, lost, or illegally used after being transferred abroad, and whether a mechanism for protecting personal information rights is easily accessible;
- the impact of the personal information protection policies, laws and regulations of the country or region where the overseas recipient is located on the performance of the Standard Contract; and
- other matters that may have an impact on the security of personal information being transferred abroad.

During the term of the Standard Contract, upon the occurrence of certain events, the data processor is required to (i) conduct a new impact assessment, (ii) supplement the Standard Contract or conclude a new Standard Contract, and (iii) complete a new filing with the requisite authority. Such events include (a) a change of purpose, scope, type, sensitivity, method, storage location of outbound transfer of personal information, (b) a change of the purpose or method of processing personal information by the overseas recipient, (c) extension of the overseas storage period of personal information, or (d) a change in personal information protection policies, laws or regulations in the country or region where the overseas recipient is located that may have an impact on the personal rights and interests of data subjects.

Part 2: PIP Certification Approach

Eligibility for the PIP Certification Approach

PIP Certification Approach involves obtaining a personal information protection certification from an authorised certification institution. The institution certifies that the data processing activities (such as the collection, storage, use, processing, transmission, provision, publication, deletion and cross-border transfer of personal data) that a data processor conducts within the scope of certification are compliant with the standards pursuant to which the PIP Certification is carried out. As mentioned in Part 1 above, a data processor that is not subject to the government led Security

Assessment Approach may adopt either the SCC Approach or the PIP Certification Approach (at the data processor's election).

Certification Institutions

The Announcement on Implementing Personal Information Protection Certification jointly issued by the PRC State Administration of Market Supervision and the CAC on 4 November 2022 states that a certification institution shall only provide personal information certification upon obtaining the relevant approvals. So far, only the China Cybersecurity Review Technology and Certification Centre has been designated as an authorised certification institution for PIP Certification.

PIP Certification Process

The PIP Certification process includes technical verification, onsite inspection and post-certification supervision. Specifically, the following steps are involved:

- engagement of a certification institution by the data processor and confirmation of a certification plan by the certification institution;
- technical verification and issuance of a technical verification report by the certification institution;
- onsite inspection by the certification institution and issuance of onsite inspection report;
- certification, or a request for the correction of non-compliant aspects, or even potentially termination of the certification or the certification process if it is determined that the data processor is not able to comply with the relevant certification requirements; and
- if the certification certificate is issued, ongoing post-certification supervision.

The review is based on the requirements set out in the Information Security Technology - Personal Information Security Specification (GB/T 35273)[4] and the Personal Information Cross-border Processing Activities Security Certification Specification (TC260-PG-20222A)[5].

The data processor is also required to conduct a self-assessment on personal information protection impacts.

Compared to the SCC Approach, one advantage that the PIP Certification has is that a certification certificate can cover multiple recipients. However, it will likely take much longer for the PIP Certification to be completed compared to the time required for the signing and filing of the Standard Contract under the SCC Approach.

Validity Period of PIP Certification

The certificate of PIP Certification is valid for 3 years, subject to ongoing supervision by the certification institution. The data processor shall notify the certification institution no less than six months prior to the expiration of the validity period if it intends to renew the certification.

Conclusion

With the publication of the Standard Contract, all three options for legally transferring personal information out of China (Security Assessment Approach, PIP Certification Approach and SCC Approach) as contemplated under the PRC Personal Information Protection Law are now in place.

We anticipate that China will further strengthen the protection of personal information in cross-border data transfers by strictly enforcing these implementation measures. This will have a direct and immediate impact on many multinational companies having operations in China. Failing to comply with these implementation measures may result in fines and administrative penalties imposed by the PRC authorities, including orders of suspension or cessation of operations in China for serious violations.

The SCC Measures will come into effect on 1 June 2023 and companies will have until the end of 2023 to ensure compliance. To get started on this process, companies with operations in China should conduct the necessary self-assessment on their current cross-border data transfer practices and start to consider the approach for which it is eligible and that best fits its business needs.

---

[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. This term is distinguishable under the PRC law from the concept "processor" under the EU and UK GDPR, which is roughly analogous to the concept of service provider. "**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.

[2] The PRC Cybersecurity Law describes Critical Information Infrastructure as including 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 destroyed, 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.

[3] The following situations are considered to be outbound transfers: the actual transfer or storage outside of China of the personal information collected or generated during operations within China, or the storage in China of personal information collected or generated by the data processor but such information is accessible to organisations or individuals outside of China. In other words, access counts as a transfer. Transfers of personal information from mainland China to

Hong Kong SAR, Macau and Taiwan are considered to be outbound transfers of personal information.

[4] An English translation of this document can be viewed at https://www.tc260.org.cn/upload/2020-09-18/1600432872689070371.pdf

[5] Full text of this document (Chinese only) can be viewed at https://www.tc260.org.cn/upload/2022-12-16/1671179931039025340.pdf

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
