CLIENT ALERTS & INSIGHTS

China Officially Promulgates New Cross-Border Data Transfer Requirements

MARCH 29, 2024

Authors: Ryan T. Sulkin, Megan C. Parker

The newly promulgated measures increase the threshold of data triggering security assessments and contract requirements while leaving room for Chinese authorities to heavily restrict cross-border data transfers.

In accordance with China's Personal Information Protection Law ("PIPL"), the Cyberspace Administration of China ("CAC") finally promulgated the Regulations on Promoting and Regulating Cross-Border Data Flows (the "Rules") on March 22, 2024, altering the regulatory framework of the cross-border data transfer.

The Rules were promulgated with the intent to balance addressing critical national concerns on protecting personal information rights and promoting orderly and free flow of data for the continuation of international business operations in China. Specifically, the Rules create procedures required to export certain volumes and types of personal information ("**PI**") outside of China.

Background

PIPL represents China's most comprehensive and specific data protection law to date, largely mirroring specific requirements found in other omnibus data protection laws such as Europe's General Data Protection Regulation ("**GDPR**"). Like other omnibus privacy laws, PIPL **(1)** requires a lawful basis for collecting and processing personal data; **(2)** specifies notice and consent requirements; **(3)** creates specific requirements for processing information from children; **(4)** provides individual's certain rights over their data; and **(5)** requires certain minimum safeguards in an entity's security procedures and policies.

PIPL Data Protection Agreements

In almost all cases, PIPL requires entities to obtain consent from a data subject and have a data protection agreement ("**DPA**") in place prior to transferring data to a foreign jurisdiction. Specifically, any contract between the parties of a cross-border data transfer must include provisions that specify:

1. the purpose, method, and scope of the outbound transfer;
2. the purpose and method of the receiving party's handling and processing of the data;
3. the location and retention period of the foreign data storage and the subsequent controls to handle the data once the retention period is reached, the agreed purpose is completed, or the contract is terminated;

4. safeguards and security measures that must be adopted when changes occur in the control and scope of the transfer services contemplated in the contract or when local laws change;
5. distribution of liability for violating and breaching the data security provisions within the contract;
6. enforceable dispute resolution procedures that do not include actual restraining force; and
7. data breach requirements including, but not limited to, the launching of emergency measures and opening of avenues for individuals to enforce their privacy rights.

Cross-Border Data Transfer Compliance Procedures

Entities wishing to export certain volumes and types of PI outside of China must undergo one of three compliance procedures: **(1)** apply for a data export security assessment by the central-level CAC ("**CAC Security Assessment**"); **(2)** enter into a standard contractual clauses ("**SCC**") filing with the provincial-level CAC (the "**SCC Filing**"); or **(3)** obtain a PI protection certification by a professional third-party recognized by the CAC (the "**PI Protection Certification**").

Which compliance procedure is required depends on the amount of PI an entity handles, whether the data is considered "important", and whether the entity itself is considered a critical information infrastructure operator ("**CIIO**"). CIIO's are defined within other Chinese laws and regulations and include, among other things, service providers in the following industries or fields: communication, energy, transport, water, finance, public services, E-government services, and national defense.

One of the most important implications of the Rules is the increase in the data volume thresholds triggering one of the PIPL compliance procedures, meaning entities will be able to handle higher volumes of data that previously allowed before needing to do a CAC Security Assessment, SCC Filing, or PI Protection Certification.

CAC Security Assessment

An entity must conduct a CAC Security Assessment if, since January 1 of the current year, it **(1)** transfers important data collected or produced by a CIIO; **(2)** transfers important data; **(3)** transfers PI of more than 1 million individuals, **(4)** transfers sensitive PI of over 10,000 individuals; or **(5)** if other circumstances as stipulated by CAC apply. An entity must submit their self-assessment, an application letter, a copy of the contract between the parties, and any other materials required for a full review as the CAC determines.

PIPL defines sensitive PI as "personal information that, once leaked or illegally used, may easily lead to infringement of a natural person's personal dignity or endanger personal safety or the property of a person". Critically, "important data" is still undefined under the Rules.

The CAC Security Assessment will largely focus on topics covered in an entity's self-assessment (outlined below), specifically determining whether the contemplated cross-border data transfer complies with applicable Chinese law and whether the receiving foreign party's data protection standards and obligations reach the level required by applicable laws and regulations. The CAC will also look to ensure individual privacy rights are fully and effectively ensured and whether there are restrictions on re-transfer of the data.

If the CAC approves a CAC Security Assessment, it is valid for 3 years and can be further renewed every three years at least 60 days prior to the CAC Security Assessment's expiration. Entities are required to reapply for a new CAC Security Assessment if **(1)** the purpose, method, scope, retention period, or the type of data being transferred changes; **(2)** relevant foreign laws or regulations change; **(3)** control over the data being transferred changes; or **(4)** other circumstances that the CAC may stipulate.

Cross-Border Data Transfer Self-Assessment

Prior to the CAC Security Assessment, entities must conduct a self-assessment analyzing the risk of the contemplated cross-border data transfer. Specifically, the self-assessment must focus on:

1. the legality, necessity, purpose, scope, and method of the cross-border data transfer;
2. the quantity, scope, categories, and degree of sensitivity of the data involved;
3. risks the cross-border data transfer poses to China's national security;
4. any pertinent individual rights at issue;
5. whether there are proper safeguards in place to mitigate risks;
6. the obligations the receiving foreign party is under and whether there are processes to enforce such obligations;
7. the risks of data breach once the data has been transferred and whether individuals will be able to exercise their rights; and
8. whether the pertinent contract between the parties fully stipulates data security protection responsibilities and duties.

SCC Filing or PI Protection Certification

An entity must complete a SCC Filing or obtain a PI Protection Certification if, since January 1 of the current year, it **(1)** transfers PI of more than 100,000 but less than 1 million individuals or **(2)** transfers sensitive PI of less than 10,000 individuals. In practice, obtaining a PI Protection Certification can be a burdensome process, and few entities use this compliance procedure.

Exemptions from Cross-Border Data Transfer Compliance Procedures

Under the Rules, no CAC Security Assessment, SCC Filing, or PI Protection Certification is required under the following circumstances:

1. the cross-border data transfer of data arising from international trade, cross-border transportation, academic cooperation, transactional manufacturing, marketing, and other activities that do not involve PI or important data;
2. the cross-border data transfer of PI originally collected and generated outside of China and then transferred into China for processing, and subsequently transferred abroad-provided no PI or important data collected and generated within China is incorporated during processing;

3. the cross-border transfer of PI for purposes of entering into and performing a contract to which the individual concerned is a party;
4. the cross-border data transfer of employees' PI, provided that such transfer is necessary for the cross-border human resources management;
5. the necessary cross-border data transfer of PI in emergency situations to protect an individual's life, health, and property; and
6. the cross-border data transfer that does not meet the threshold of 100,000 individuals' non-sensitive PI since January 1 of the current year.

Further, the number of individuals under these circumstances can be excluded when calculating the thresholds triggering compliance procedures. There is also no need to apply for a CAC Security Assessment for the cross-border data transfer of data that have not been notified or publicly announced by the relevant departments or regions as important data.

Data Element-based Exemption in Free Trade Zone

The Rules authorize competent authorities in a Free Trade Zone-for example, China (Shanghai) Pilot Free Trade Zone or China (Beijing) Pilot Free Trade Zone-to formulate a list of data categories to be regulated through the CAC Security Assessment, SCC Filing and/or PI Protection Certification (the "Negative List"). The Negative List will be approved by the provincial-level CAC and filed with the central-level CAC.

As such, no compliance procedure will be required if an entity within a Free Trade Zone transfers data that is not listed on the Negative list to a location outside of China.

Now that the Regulations on Promoting and Regulating Cross-Border Data Flows have been promulgated, the Benesch Data Protection and Privacy team is committed to staying at the forefront of knowledge and experience to assist our clients in compliance efforts. We are available to assist you with any compliance needs.

Ryan T. Sulkin at rsulkin@beneschlaw.com or 312.624.6398.

Luke Schaetzel at lschaetzel@beneschlaw.com or 312.212.4977.

Megan C. Parker at mparker@beneschlaw.com or 216.363.4416