CLIENT ALERTS & INSIGHTS

As China Cross-Border Data Transfer Security Assessment Requirement Comes Into Effect, New Guidelines Posted for Security Assessment Application

OCTOBER 18, 2022

The new guidelines provide insight into how businesses can submit applications to the CAC in order to obtain approval via the CAC security assessment cross-border data transfer requirement.

As of September 2022, all businesses falling within the scope of China's Cyberspace Administration ("**CAC**") of China security assessment (one of three mechanisms that allow a business to conduct cross-border data transfers) must be complying with the applicable self-assessment and government assessment requirements. To help businesses comply, the CAC recently released guidelines on the applicable requirements.

Last year, China's sweeping data protection law, the Personal Information Protection Law ("**PIPL**"), went into effect on November 1, 2021. The law specifically addresses entities that engage in transferring personal data from China to a location outside of China, but it left many wondering what exactly the new cross-border data transfer requirements are and how they can be satisfied.

As noted in previous posts, entities that are transferring Chinese personal data to another jurisdiction are required (1) to obtain consent from a data subject prior to transferring data to a foreign jurisdiction, and (2) to ensure the data transferred is sufficiently protected.

To meet this second requirement, PIPL sets forth three expressed options: (1) passing a CAC security assessment; (2) receiving certification from CAC-certified professional organizations; or (3) entering into standard contractual clauses. It is likely that the standard contractual clauses will become the standard mechanism as the professional certifications are limited in applicability. It is important to note, however, that if a business falls within the CAC security assessment scope that it must use the CAC security assessment as the transfer mechanism.

The second option-professional CAC certifications-are limited in that businesses are only able to utilize them to satisfy PIPL requirements in the following instances: (1) internal transfers between entities under the same business organization (e.g., intra-group data transfer agreements); and (2) data processing conducted wholly outside of China, by a non-China entity, related to the personal information of individuals located in China (e.g., businesses subject to PIPL's extraterritorial jurisdiction). Additionally, the CAC has yet to actually specify which sub-agencies are allowed to grant the professional certifications.

Related to the CAC security assessment, the CAC published the draft "Outbound Data Transfer and Security Assessment Measures" ("**CAC Measures**") in Oct. 2021, which recently took effect September 1, 2022. For more information on the CAC Measures, please see our previous alert

. Only twenty-four hours before the Security Assessment Measures took effect, however, the CAC announced the publication of the Guidelines for Data Export Security Assessment Declaration (First Edition) ("**CAC Guidelines**"). The CAC Guidelines provide businesses with more specific details as to the Chinese government's role in the assessment process and are intended to help businesses comply and to make data export security assessments standardized and orderly.

Importantly, the Security Assessment Measures require both a self-assessment and a government-led assessment. For entities that must conduct a CAC assessment to continue transferring "important data" or personal information, the CAC Guidelines provide directives on how to conduct the self-assessment, the contents of the application, and what supporting documents need to be filed with the CAC for approval. Only certain entities must comply with the CAC assessment depending on the type and volume of information transferred - see our previous alert for more information about all three of the cross-border data transfer mechanisms.

Scope of CAC Security Assessment Requirement

An entity must conduct a CAC security assessment if it (1) transfers important data collected or produced by critical infrastructure operators; (2) transfers "important data;" (3) collects personal information of over 1 million individuals; (4) transfers personal information of over 100,000 individuals; (5) transfers sensitive information of over 10,000 individuals; or (6) if other circumstances as stipulated by CAC apply.

Under the CAC Measures, "important data", is defined to include any data that could endanger national security, economic operation, social stability, or public health and safety" if breached. In contrast, critical infrastructure is defined within other Chinese laws and regulations and includes, among other things service providers in the following industries or fields: communication, energy, transport, water, finance, public services, E-government services, and national defense.

Application & Supporting Documents

While the previously passed CAC Measures set forth specifics related to timing and the self-assessment requirement under the CAC security assessment, the newly published CAC Guidelines provide details on the second requirement-the government-led assessment.

Specifically, the CAC Guidelines set forth the documents and information that businesses need to include in their application to the CAC prior to the CAC conducting their assessment.

Applications must include a general description of the data transfers at issue, the self-assessment required under the CAC Measures, and copies of the applicable cross-border data transfer agreements that the in-scope business has entered into with the data processor(s).

The application also requires multiple documents, on top of the above information.

The application requires the data controller to prepare a certified copy of its (1) unified social credit code certificate, (2) legal representative's ID card, (3) appointed agent's ID card, and (4) agreements or other legal documents with the overseas data recipients-these must be in Chinese or bilingual. The data controller must also provide a Power of Attorney document appointing an agent handling the application and related matters, meaning in-scope businesses will likely need to engage local counsel in China. Additionally, a completed Application Form for Security Assessment of

Cross-border Data Transfers-the templates for these requirements are included in the CAC Guidelines.

The foregoing is not an exhaustive list of what an entity may be required to submit for CAC assessment. Other relevant contractual and legally binding documents intended to conclude the data export risk self-assessment report may also be required.

Key Takeaways

The CAC assessment and application process are now in effect and remains a significant task. The deadline to prepare and submit the application is March 2023, and as it requires a substantial amount of information about the data recipient (who, in many cases, may likely be reluctant to provide the necessary information (e.g., registered capital amount, ID of security officer, number of employees), we recommend effected entities take action as soon as possible.

To assist entities in meeting the application deadline, the CAC Guidelines provide copies of the relevant forms required to be submitted (described above) and additional clarifications concerning questions presented in each form.

As compliance with PIPL comes into effect and as Data Transfer requirements in China are adopted or amended, 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.

Megan Kern at mkern@beneschlaw.com or 216.363.4615.

Lucas Schaetzel at lschaetzel@beneschlaw.com or 312.212.4977.