CLIENT ALERTS & INSIGHTS

China Publishes Draft Data Transfer Requirements That Heavily Favor Data Localization

DECEMBER 2, 2021

Authors: Ryan T. Sulkin

As drafted the new measures specify security assessment and contract requirements but leave ample room for Chinese authorities to heavily restrict cross-border data transfers. At the end of October, China's top privacy and data protection agency, the Cyberspace Administration of China ("**CAC**"), released the draft measures on "Outbound Data Transfer and Security Assessment Measures" (the "**Draft Measures**") for public comment.

This marks CAC's third iteration of draft-specific regulations related to cross-border data transfers. The first two drafts were also released for public comment but were never adopted into law.

Importantly, the Draft Measures finally provide insight into how the CAC will conduct security assessments, what the CAC will review in determining whether to allow a cross-border data transfer, and the types of contractual provisions that will need to be in contracts that contemplate cross-border data transfers.

The release of the Draft Measures coincides with the effective date of China's Personal Information Protection Law ("**PIPL**"). 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 collected 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 took effect on Nov. 1, 2021. For Data Meets World's coverage of PIPL and more in-depth analysis of the law's requirements, click here. While PIPL did not give entities details related to cross-border data transfers, the law provided a general framework that the Draft Measures now expand on.

PIPL Data Localization and Cross-border Transfer

PIPL restricts cross-border data transfer. In almost all cases, entities are required to obtain consent from a data subject and have a data protection agreement ("**DPA**") in place prior to transferring data to a foreign jurisdiction.

The Draft Measures go even further for entities that meet certain criteria and require additional compliance steps before an entity can transfer data to a foreign jurisdiction. In addition to obtaining consent and entering into DPAs, entities that meet the criteria specified in the Draft Measures will

need to conduct security assessments in order to transfer data outside of China. Additionally, the Draft Measures describe the provisions that must be in a DPA in order to be compliant.

The Draft Measures, while potentially restrictive and cumbersome, hope to clear up the ambiguities left by PIPL related cross-border data transfers.

Scope

The Draft Measures outline which entities must conduct security assessments, in addition to obtaining consent and entering into DPAs, in order to transfer data outside of China.

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.

Critically, "important data" is still undefined within the Draft Measures or in other applicable law. 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.

Security Assessment

The main cross-border data transfer requirement imposed by the Draft Measures is the security assessment. Prior to the CAC security assessment, entities must conduct a self-assessment analyzing the risk of the contemplated cross-border data transfer.

The self-assessment must focus on **(1)** the legality, necessity, purpose, scope, and method of the cross-border transfer; **(2)** the quantity, scope, categories, and degree of sensitivity of the data involved; **(3)** risks the cross-border 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 of breach during the transfer; **(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.

Under the Draft Measures, an entity that meets the Draft Measure's criteria 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 determined by the CAC.

Within 7 days of submitting the self-assessment and the above documents to the CAC, the entity will receive notice that the CAC is conducting a security assessment. Within 45 to 60 business days, the CAC will complete the security assessment.

The security assessment will largely focus on the topics covered in an entity's self-assessment (as outlined above), 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.

The CAC's determinations will likely be less transparent and clear than the European Union's adequacy determinations under the GDPR, leaving little in the way of guidance. Further, the security assessment gives the CAC broad and vague discretion to deny cross-border data transfers and require data localization by default.

If the CAC approves a security assessment and the cross-border data transfer, it is valid for 2 years. Entities must reapply for a new security assessment if **(1)** the purpose, method, scope, retention period, or 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.

If the cross-border data transfer contemplated under a valid security assessment is required to go beyond 2 years, an entity must reapply for a security assessment at least 60 days prior to expiration of the security assessment. Further, entities have a continuing duty to assess whether a valid security assessment properly covers ongoing data transfers and must cease transfers that are no longer covered.

Contractual Provisions

Beyond laying out the scope of the CAC security assessments, the Draft Measures describe what a DPA must address to be valid.

Under PIPL, entities must have an agreement in place with the receiving, foreign party. The Draft Measures specify certain privacy and data protection provisions that must be in that agreement.

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.

Implications

Where PIPL was meant to address both the Chinese Government's and the public's concern over the privacy of their personal information, the Draft Measures and China's tendency to heavily favor data localization is seen as a national security move.

The still vague terms, and lack of clear definitions for specific terms such as "important data," allow the Chinese government to yield a lot of discretion in allowing cross-border data transfers. The

Chinese government, in theory, could require data localization by default depending on how they yield the discretion the Draft Measures grant it.

For example, because “important data” is still undefined, the CAC may decide on a case-by-case basis whether data contemplated in a cross-border transfer is important or not; leaving little to no guidance for entities to base decisions business on.

If adopted into law, entities falling within the scope of the Draft Measures, of which there will likely be many, will face the choice of investing time and resources into creating separate systems in China, or undergo the cumbersome CAC security assessment and contractual process.

Regardless, any entity contemplating cross border transfer of data will need to (1) obtain consent from the data subject; (2) put a DPA in place between it and the party receiving the data; and (3) *possibly* go through the CAC security assessment process if they meet the criteria set forth in the Draft Measures.

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.

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

Lucas Schaetzel at lschaetzel@beneschlaw.com or 312.212.4977.