CLIENT ALERTS & INSIGHTS

China Data Transfer Mechanisms and Requirements Come into View as Security Assessment and Technical Certification Measures Finalized; Standard Contract Measures Proposed

JULY 18, 2022

The transfer mechanisms drive home China's focus on data localization, as the measures all set forth cumbersome procedures and requirements, including security assessments and required contractual considerations.

Despite going into effect last year on Nov. 1, 2021, China's sweeping data protection law, the Personal Information Protection Law ("**PIPL**"), did not clearly set forth specific cross-border data transfer requirements for entities transferring personal data from China, to a location outside of China.

PIPL heavily restricts cross-border data transfers. In almost all cases, entities are required to obtain consent from a data subject prior to transferring data to a foreign jurisdiction.

Additionally, an entity must ensure the data transferred is sufficiently protected. To meet this requirement, PIPL set forth three expressed options: **(1)** passing a Cyberspace Administration of China ("**CAC**") security assessment; **(2)** receiving certification from CAC-certified professional organizations; or **(3)** entering into standard contractual clauses. The foregoing options are finally coming into focus.

Pursuant to the first option, the CAC published the draft "Outbound Data Transfer and Security Assessment Measures" ("**Security Assessment Measures**") in Oct. 2021. The CAC finalized the Security Assessment Measures on July 7, 2022; effective in less than three months -September 1, 2022.

As for the second cross-border data transfer option, China's National Information Security Standardization Technical committee ("**TC260**") published the "Technical Specification for Certification of Personal Information Cross-Border Processing Activities" ("**Technical Certification Measures**"). The Technical Certification Measures are limited in applicability and requires a security assessment, among other requirements.

Finally, as to the third cross-border data transfer option, the CAC published "Regulations on Personal Information Export Standard Contractual Clauses" ("**Draft Contractual Measures**"). These measures are still out for comment. As drafted, the scope of the Draft Contractual Measures is limited to only provide a transfer mechanism to those entities that are not critical information operators and only process small amounts of information.

It is important to note that all three of data transfer mechanism require some level of interaction with the Chinese government, with the Draft Contractual Measures requiring the lowest amount of interaction (filing the applicable contract and a data protection impact assessment).

See below for further insight and analysis into the various cross-border data transfer mechanisms.

Standard Contractual Measures

The Draft Contractual Measures provide standard contractual clauses that can be copy and pasted into applicable agreements between parties, in a similar method as many entities use for the European Union Standard Contractual Clauses ("**EU SCCs**"). The same standard contractual clauses can be used for both controller-controller transfers and controller-processor transfers.

According to the Draft Contractual Measures, the transfer mechanism can only be relied on by entities that **(1)** are not considered critical information infrastructure operators (e.g., internet providers, financial service providers, transportation providers, utility providers, etc.); **(2)** process the personal data of less than one million individuals; **(3)** have only transferred the personal data of 100,000 individuals since Jan. 1 of the preceding year; and **(4)** have only transferred the sensitive personal data of 10,000 since Jan. 1 of the preceding year.

Entities whose business model is reliant on the collection, use, and transfer of personal data will likely not be able to use the Draft Contact Measures to transfer personal data to a location outside of China.

Under the Draft Contractual Measures, the applicable contract itself must include and address six main concepts, all of which are familiar under similar cross-border data transfer regimes (such as under the EU SCCs).

The applicable contract must contemplate: **(1)** identification of, and contact information for, the relevant controller and processor; **(2)** the purpose, scope, type, sensitivity, quantity, method, storage period, and storage location of the personal data; **(3)** the responsibilities and obligations that the non-China recipient is contracting to and whether proper technical and organizational measures are in place to ensure the personal data's protection; **(4)** the laws and regulations of the jurisdiction the personal data is being transferred to; **(5)** the rights of individual data subjects; and (6) contractual remedies, allocation of liability in the event of a breach, and dispute resolution provisions.

Even if an entity is relying on the Draft Contractual Measures, a data impact assessment must be conducted prior to the transfer of personal data.

The assessment must analyze (essentially the same topics as needed in the applicable contract: **(1)** the legitimacy and necessity of the processing; **(2)** the quantity, scope, type, and sensitivity of the personal data and the risks the cross-border transfer create with respect to a data subject's privacy interests and rights; **(3)** the responsibilities and obligations that the non-China recipient is contracting to and whether proper technical and organizational measures are in place to ensure the personal data's protection; **(4)** risk of personal data breach and the ability for a data subject to seek recourse or control over their personal data; **(5)** the laws and regulations of the jurisdiction the personal data is being transferred to; and **(6)** any other applicable matters.

Once agreed to by the contracting parties, the applicable processor must-within 10 business days from the effective date of the applicable contact-file the contract and the data impact assessment with the local cybersecurity government entity or agency.

Technical Specification Certification

The Technical Certification Measures only apply in *two* instances and require entities to jump through a multitude of hoops to transfer personal data to a location outside of China.

The first instance is where a multinational company conducting *internal data transfers* within the same company or business entity (i.e., "**Internal Company Transfers**"). The second instance is where there is a cross-border transfer conducted by a non-China-based entity who is subject to PIPL's extraterritorial jurisdiction (i.e., the entity **(1)** intends to provide products or services to individuals in China; **(2)** is analyzing activities of individual in China; or **(3)** other circumstances as determined by applicable law and regulation) (i.e., "**Extraterritorial Transfer**").

An entity falling within either category, as described above, can apply for certification under the Technical Certification Measures. If pursuant to an Internal Company Transfer, the China-based affiliate must apply for certification and bear the legal liability. If pursuant to an Extraterritorial Transfer, the non-China-based entity must appoint a designated representative in China to apply and bear legal liability.

1. Contractual Considerations

The main requirement under the Technical Certification Measures is for there to be a legally binding agreement between the involved parties. Such an agreement must contemplate the following: **(1)** the parties involved in the cross-border transfer and processing of the personal data; **(2)** the purpose of the transfer; **(3)** categories of personal data involved; **(4)** measures in place to protect the rights and interests of the data subjects; **(5)** specify the entity bearing legal liability in China; and **(6)** any other obligations required by law.

Further, all parties must agree to **(1)** implement and maintain those measures necessary to process and protect the personal data equivalent to those set forth in PIPL; **(2)** be subject to the supervision of the applicable certification body; and **(3)** comply with Chinese data protection laws and accept Chinese jurisdiction.

While not required in the specific contract, the Technical Measures also require the parties to agree to certain data processing rules: **(1)** the context of the transfer (i.e., categories of data, sensitivity, amount, etc.); **(2)** the purpose, method, and scope of the transfer and processing; **(3)** the duration of the processing; **(4)** the location the personal data is being transferred; **(5)** the measures taken to protect the rights of data subjects; and **(6)** the measures to be taken in the event of a personal data breach.

The most efficient way to address the data processing rules would be to include them in the contract as a number of the topics overlap with the contractual requirements discussed at the beginning of this section.

1. Organizational Management

The Technical Certification Measures also requires all parties involved in the cross-border data transfer to designate a data protection officer who would take on the function and role that is now familiar under similar data protection regimes.

However, the Technical Certification Measures are silent on whether or not an entity making a transfer pursuant to an Internal Company Transfer can rely on the same data protection officer. If separate data protection officers are necessary, entities may need to appoint a China-specific data protection officer to fulfill the Technical Certification Measure's requirements.

1. Data Protection Impact Assessment

Similar to the Draft Standard Contractual Measures, the Technical Certification requires a data protection impact assessment.

The data protection impact assessment required under the Technical Certification requires the parties to address **(1)** whether the cross-border data transfer complies with all applicable laws and regulations; **(2)** the impact the cross-border data transfer will have on data subjects; **(3)** the potential impact of the destination jurisdiction's applicable laws; and **(4)** other matters needed to safeguard the rights of data subjects.

1. Data Subject Rights and Protections

Data subjects have numerous rights under the Technical Certification Measures (similar to and in line with those set forth in the Standard Contractual Measures). Data subjects are made third-party beneficiaries of the personal data portions of the applicable agreement and has a right to request a copy of such agreement at any time.

Even further, the data subject has the right to restrict or refuse the transfer of their personal data, even if all requirements are met by the applicable parties under the Technical Certification Measures.

Security Assessment Measures

The Security Assessment Measures require both assessments *and* contractual considerations. Except in this case, the Security Assessment Measures require both a self-assessment and a CAC assessment.

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, the finalized Security Assessment Measures provided a definition for "important data", which includes 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.

1. Security Assessment

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 business days, the CAC will complete the security assessment (unless extended by the agency due to the complexity of the transfer).

If the CAC denies the security assessment and does not allow the cross-border data transfer, the applicable controller can request re-assessment so long as such a request is made within 15 days of receiving the initial result.

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.

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.

1. 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.

Practical Takeaways

The data transfer mechanisms set forth by Chinese authorities under PIPL have thus far driven home their focus on data localization-heavily favoring and incentivizing businesses to store Chinese personal data in China.

At a minimum, all three transfer mechanisms require **(1)** some form of a security or data impact assessment; **(2)** filing with a Chinese government authority or agency; and **(3)** necessary topics and provisions for the applicable contract between the relevant parties.

Entities who collect, use, or otherwise process Chinese personal data will now face the choice of investing time and resources into creating separate systems in China to locally store the personal data, or undergo cumbersome processes and security assessments.

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.

Luke Schaetzel at lschaetzel@beneschlaw.com or 312.212.4977.