CHINA COMPLIANCE | JULY 2022

CHINA RELEASES LONG-AWAITED DATA TRANSFER RULES

Review your data practices now – China's Cyberspace Administration ("CAC") releases long-awaited rules updates

During the last two weeks, China's Cyberspace Administration (CAC) released two significant updates to its data protection and compliance framework: the final language of the Measures for the Security Assessment of Outbound Data Transfers ("Measures") and the draft Regulations of Standard Contracts for Cross-border Transfer of Personal Information ("SCCRs"). The Measures become effective on 1 September 2022, while the SCCs are still open for public comment until 29 July 2022.

The Measures and the SCCRs are in line with China's years-long push towards creating a coherent, workable compliance framework for companies that need to engage in cross-border data transfers, but have been waiting for regulators to provide guidance on how they can do so in a legally compliant manner. Below are brief primers on both.

The Measures

While the Measures do not cover every business, companies need to familiarise themselves with the triggers. In addition to generally required personal information impact assessments ("PIIAs"), companies must perform internal security assessments and then apply for formal, regulator-driven assessments prior to cross-border data transfer if:

- They export "important data".

  The Measures define important data as "any data that, once tampered with, damaged, leaked, or illegally obtained or used, may endanger national security, economic operation, social stability, and public health and safety." This remains a vague definition, but in our experience, officials do not appear to apply it broadly to restrict ordinary business activities. That said, we note that a number of regulatory bodies are currently working on further guiding language to clarify factors they will use to identify important data on an industry by industry basis, and we are closely tracking those developments.

- They are a Critical Information Infrastructure Operator ("CIIO").

  Whether a company is a CIIO can be difficult to determine, because language in other parts of China's data compliance framework provides only loosely defined considerations, and similarly leave it to specific industry regulators to create their own definitions. "Critical" is the key word here – a CIIO engages in business that significantly, directly impacts the overall functioning of a given industry. As above, we have not yet seen regulators applying the CIIO designation broadly to restrict ordinary business activities. This will likely continue to be true, especially outside of sensitive industries which include, for example, telecom, energy, transport, healthcare, finance, and defence. Companies should continue monitoring this space closely, as more precise industry and sector-based definitions are forthcoming.

- They *process* personal information of more than 1 million individuals.

- They cumulatively transfer personal information of more than 100,000 individuals, or the *sensitive* personal information of more than 10,000 individuals, calculated from 1 January of the previous year.

  The above two categories are where the Measures will begin to ensnare more ordinary but data-heavy companies. For instance, any company that relies on or maintains a large, rich CRM system likely needs to begin preparing for a mandatory security assessment. Companies should also keep a close eye on the threshold limits for data transfers.

While some uncertainty remains about the definitions of various terms in the Measures, as well as how they will be implemented and enforced starting on 1 September, companies should spend the intervening time re-examining their data practices to see if they potentially fall under any of the above categories. If there is a chance they do, it is time to prepare for both internal and formal security assessments.

The SCCRs

If a company finds itself outside the bounds of required security assessments under the Measures discussed above, the SCCRs provide another avenue towards complaint cross-border transfers of personal information. Released along with the SCCRs is an annex containing model standard contract language which companies can use, and to which they can add language that does not conflict with the model clauses. Note that we base the below discussion on draft language – after the public comment period ending 29 July, the CAC might make changes.

In contrast to the Measures, the SCCRs serve as a compliance mechanism only for companies that:

- *Are not* CIIOs;
- Process personal information of *less than* 1 million individuals; *and*
- *Have not* cumulatively exported the personal information of 100,000 individuals, or the sensitive personal information of more than 10,000 individuals, calculated from 1 January of the previous year.

The SCCRs indicate that standard contracts must contain clauses covering:

- Identities of sender and recipient
- The purpose, scope, type, sensitivity, quantity, method, retention period, and storage location abroad
- The responsibilities and obligations of the parties, including the technical security measures to be taken
- Impact of personal information protection regulations of the jurisdiction of the recipient is located on performance of the transfer contract
- Data subjects' rights and how they are protected
- General contractual terms covering remedies, termination, breach, liability, and dispute resolution

In addition to the above, companies intending to use standard contracts must also perform and document personal information impact assessments ("PIIAs") and then file both the signed standard contract and related PIIAs with the CAC within 10 days of the contract becoming effective.

What does this mean for you?

The data compliance framework in China just got clearer. Companies, especially foreign companies, need to immediately assess whether they might fall under any of the categories requiring a security assessment. If they do, it is crucial to begin preparing before the Measures come into effect on 1 September.

If security assessment isn't triggered, standard contracts provide another compliance mechanism for necessary cross-border data transfers. Many companies doing business in or with China already have standard contracts in place that comply with other data protection frameworks, the GDPR for example, and we think standard contracts will be widely used in China – they offer a familiar, lower cost, and less cumbersome cross-border data transfer compliance process. However, companies need to keep in mind that what works in other jurisdictions might not work in China, even if the fundamentals of the contracts seem to align. As mentioned above, the SCCRs are still in draft form, and we suggest that companies take this time to do a thorough review of existing contracts to determine if and how they might use standard data transfer contracts to their advantage.

For more information, contact:

BRINTON SCOTT
Partner, Shanghai
T +86 (21) 2080 1068
E brinton.scott@hfw.com

NATHANIEL RUSHFORTH
Senior Associate, Shanghai
T +86 (21) 2080 1186
E nathaniel.rushforth@hfw.com

hfw.com