WINSTON & STRAWN LLP

BLOG

China's Regulations on Cross-Border Transfers of Personal Information Now in Effect

JULY 6, 2023

In February 2023, the Cybersecurity Administration of China (CAC) issued the *Measures for the Standard Contract for Outbound Cross-Border Transfer of Personal Information* (the "Measures") which became effective on June 1, 2023. It will be important for global companies to comply with these Measures. Currently, the CAC is one of the most active enforcement agencies in China. Furthermore, the penalties can be substantial, including serious business disruption and fines of the greater of RMB 50 million (~USD 7 million) or 5% of the prior year's revenue.

The Measures provide guidance and procedures for the adoption of Standard Contractual Clauses (SCC) to allow for cross-border transfers of personal information and provide a six-month grace period to execute the SCCs and file for recording with the provincial-level CAC. Companies that obtain personal information from China should take advantage of this window to bring their practices into compliance.

As background, the PRC Personal Information Protection Law (PIPL) requires personal information processors to implement one of the following three data transfer mechanisms before conducting cross-border transfers of personal information outside of China:

1. Complete a Security Assessment by the CAC;
2. Complete a Security Certification by a certification institution designated by the CAC; or
3. Adopt SCCs.

A Security Assessment is required in the following four enumerated circumstances:

1. The company is a critical information infrastructure operator (CIIO);
2. The company has processed the personal information of more than one million individuals;
3. Since January 1 of the previous year, the company has transferred the personal information of more than 100,000 individuals; or
4. Since January 1 of the previous year, the company has transferred the sensitive personal information of more than 10,000 individuals.

If a Security Assessment is not required, then companies will typically decide to adopt SCCs for their cross-border transfers of personal information. The SCC procedure has its own complexities. First, it is necessary for the company to first complete a Personal Information Protection Impact Assessment (PIPIA), which will include an audit and reporting.

In addition, the SCC needs to be filed with the provincial-level CAC for recordation along with other documents, including the PIPIA. While the procedure is described as a filing for recording, it should be understood to be a review or approval. For example, the Measures suggest that the CAC may request modifications and a new PIPIA to be conducted and an SCC to be executed. Thus, it is critical to have experience with the CAC and understand its particular interpretation or preferences for the documentation.

Tip: Companies should take advantage of the grace period to come into compliance to reduce the risk of severe penalties.

Dora You, associate at Winston & Strawn's China-based strategic alliance partner, YuandaWinston, co-authored this blog post.

2 Min Read

Author

Jacob Harding

Related Topics

Privacy | Cybersecurity Administration of China (CAC) | Compliance | PRC Personal Information Protection Law (PIPL) | Data Security

Related Capabilities

Privacy & Data Security | Government Investigations, Enforcement & Compliance

Related Professionals

Jacob Harding

This entry has been created for information and planning purposes. It is not intended to be, nor should it be substituted for, legal advice, which turns on specific facts.