Transferring Employee or Customer Data Out of China Without Proper Reporting May Have Criminal Consequences: A 4-Step Compliance Plan

Insights
4.21.23

The compliance grace period for China's cross-border data security assessment measures has expired — but many international companies with operations or employees in China are still not compliant. In light of the diminishing political relationship between China and the U.S. in recent months, China has stepped up its enforcement efforts against Western companies — especially those in the U.S. — for violation of the Measures for Data Export Security Assessment and other data protection regulations. Consequences could include restrictions on the transfer of data out of China, forced closure of a company's business in China, steep fines, as well as criminal penalties for the companies and their executives. Therefore, it is critical for companies with employees or business operations in China to understand the relevant rules and take action. Here's what you need to know about the requirements, as well as a four-step compliance plan.

Data Privacy Regulations Governing International Transfers

Under China's Personal Information Protection Law, in order to transfer personal information to another country, the individual or entity controlling such information must satisfy one of the following conditions:

- Pass the security assessment conducted by the Chinese Cyberspace Administration;
- Be certified by a designated institution in accordance with the regulations of the Cyberspace Administration;
- Sign a contract with the overseas recipient of the information in accordance with the standard contract formulated by the Cyberspace Administration to stipulate the rights and obligations of both parties; or
- Otherwise be permitted to do so by other laws, administrative regulations, or the Cyberspace Administration.

Even if any one of the above conditions is met, the data controller must provide proper notice to the individuals whose information is to be transferred *and* obtain their individual consent. If the amount of information collected reaches a certain threshold (as described below), it must be stored in

China, or if transfer abroad is absolutely necessary, such transfer must first be assessed and approved by the Cyberspace Administration.

The Measures for Data Export Security Assessment further clarify that data controllers in the following situations must have the international transfer assessed by the Cyberspace Administration:

- If "important data" is transferred ("important data" is defined as data that may endanger national security, economic operation, social stability, public health, and safety — this essentially reserves unlimited discretion for the Chinese government to deem any data "important"); or
- If the controller has transferred personal information of more than 100,000 individuals or sensitive personal information of more than 10,000 individuals from China to another jurisdiction since January 1 of the previous year.

Consequences of Noncompliance

Failure to comply with these requirements has serious consequences for the companies controlling or processing personal data, as well as their executives. Fines can range between RMB 50 million ($7.8 million USD) or up to 5% of a company's previous year's business revenue. The violating company and its executives may be subject to public shame and point reduction on China's social credit system. The company may be prohibited from doing business in China, and the executives may face imprisonment in serious cases.

4-Step Compliance Plan

International companies with employees or customers in China should take the following four steps to stay compliant:

1. Execute an international data transfer agreement in accordance with the standard contract formulated by the Cyberspace Administration;
2. Prepare or update local law compliant data privacy notifications for employees and customers in China;
3. Review your international data transfer policy and practices to ensure compliance with Chinese law (note that it may be different and in certain areas more stringent than the GDPR, so GDPR compliance does not guarantee Chinese Personal Information Protection Law compliance); and
4. Conduct a separate and thorough data inventory analysis for China, and if the total amount has exceeded the threshold discussed above, work with counsel to report the proposed transfer to the Cyberspace Administration for assessment and approval.

Conclusion

If your organization does business or has employees in China — or processes personal data from China — please contact your Fisher Phillips attorney, the author of this Insight, or any attorney in our International Practice Group or Consumer Data Privacy Team to learn more about the implications of this new law. We will monitor these developments and provide updates as warranted, so make sure that you are subscribed to Fisher Phillips' Insight System to get the most up-to-date information direct to your inbox.

Related People

Nan Sato, CIPP/E, CIPP/C
Partner
610.230.2148
Email

Service Focus

Counseling and Advice

Privacy and Cyber

International