China's New Cyber Security Law Goes into Effect June 1, 2017

Insights
3.13.17

China's new cyber security law (Law) could have far-reaching impacts for companies that do business there. The Law goes into effect on June 1, 2017. As is typical of legislation passed by the Standing Committee of the National People's Congress, China's highest legislative authority, the law has been criticized for its vagueness. Its provisions cover a wide range of issues. It regulates technology that can be used in China's cyber space and requires network operators to cooperate in national security and criminal investigations. The Law also requires "critical information infrastructure operators" to store personal data and important business data within China.

The Law's requirements for critical information infrastructure operators are stringent and could apply broadly – to any information infrastructure that, if destroyed, could "endanger national security, national welfare and the people's livelihood, or the public interest." Critical information infrastructure operators are required to (1) have specific management bodies responsible for security management, (2) conduct network security education and training, (3) conduct backups of important systems and databases, (4) formulate emergency response plans and conduct periodic drills to deal with network security incidents, and (5) comply with other (unspecified) obligations provided by law. Similar requirements apply to "network operators" (owners or managers of any cyber network). Additionally, "personal information and other important data gathered or produced by critical information infrastructure operators during operations within" mainland China must be stored in mainland China.

These provisions could apply to any personnel information or any confidential or proprietary business information. There is an exception to the data localization requirement "where due to business requirements it is truly necessary to provide [data] outside the mainland." But to take advantage of this provision, critical information infrastructure operators must follow unspecified "measures" and the State Council will conduct a security assessment. The vague and ambiguous nature of the critical information infrastructure provisions are representative of the rest of the Law and make it difficult to formulate compliance programs.

The enforcement provisions of the Law are equally unclear. Penalties for violations could include warnings, rectification orders, fines, confiscation of illegal gains, suspension of business operations or the revocation of the entity's business license. The vague enforcement provisions, coupled with the legitimate concern that Chinese officials could require companies to provide "back doors" to a wide range of data present significant risk for companies operating in mainland China.

Chinese officials have promoted the Law as necessary to national security and have attempted to assure stakeholders that it will not create obstacles for foreign businesses. But some experts fear that the Law could stifle China's efforts to further integrate into the global economy and may dissuade foreign companies from doing business there. Bottom line, if your business operates in mainland China, it is time to take a hard look at your compliance programs and data storage methods before the law takes effect in June 2017. Although it is impossible to predict precisely how the Law will be enforced, it is important to develop a practical plan to address the challenges your business will likely face.