China's New Cybersecurity Law: Clarifications, Implementation Delay Announced

By China Briefing
Editor: Alexander Chipman Koty
Word Count: 985

China's sweeping new Cybersecurity Law ("the Law") came into effect on June 1 amid widespread anxiety from the foreign business community. Many in the private sector were concerned by the Law's stringent requirements, ambiguous language, and unclear implementation plan.

To allay these concerns, the Cyberspace Administration of China (CAC) modified the language of certain parts of the Law, and delayed implementation of cross-border data localization provisions until the end of 2018. While the last minute changes add a degree of clarity to the Law, and give additional time for companies to organize compliance, many of the fundamental issues that concerned foreign companies remained unchanged.

As a result, companies with operations or customers in mainland China should review the Law. Professional advisors can help determine whether your business needs to make changes to its business structure to comply with the new Law.

Data localization delayed, security reviews reduced

Prior to June 1, rumors circulated in the business community that the authorities would delay the implementation of the Law. Despite the concerns of foreign companies, and the dearth of supporting guidelines from the authorities, the Law ultimately came into effect on June 1, 2017; the

CAC stated that it would publish all supporting implementation guidelines and regulations within a year.

However, in a meeting with representatives of foreign businesses and governments, the CAC offered a 19-month grace period for companies to comply with the cross-border data flow requirements. Companies now have until December 31, 2018 to comply with that part of the Law.

The other aspects of the Law, including the controversial security review requirements, are still effective as of June 1, though authorities removed the provision for automatic security reviews of overseas transfers of 1,000 GB or more by a network operator. The revised draft Measures also state "internal company data transfers will not be subject to a security review if the company does not use its network to commercialize data externally." This suggests that companies who solely use their networks for internal purposes might not be subject to security reviews.

Scope of data localization clarified

A Q&A posted on the CAC's website on May 31 states that data localization requirements only apply to personal information and/or important data collected or generated by critical information infrastructure (CII) operators. This was the language used in the original Law that passed in November 2016.

The draft Measures for the Security Assessment of Personal Information and Critical Data Leaving the Country ("the Measures"), released on April 11, 2017, appeared to extend data localization requirements to "network operators" in addition to CII operators. Since an extremely wide swathe of companies could be considered "network operators" with the broad definition used in the Measures, the CAC's confirmation that the data localization requirements only apply to CII operators is a relief for foreign companies who may have been affected.

It should be noted that this clarification appeared in a Q&A posted by the CAC, but does not constitute an official amendment to the Law or the Measures. As such, those who could be considered network operators should await further official updates and announcements before making a final determination about whether or not they might be affected by the data localization provisions.

Although the CAC responded to the confusion surrounding network operators, it did not narrow the vague definition of CII operator. According to the Law, CII operators are entities providing services that, if lost or damaged, could endanger China's national security, economy, or public interest.

Examples provided in the Law include public communications and information services, energy, transportation, water conservancy, finance, public services, and e-government, among others. The State Council will release measures to further define CII operators at a later date.

"Important data" and "personal information" clarified

The CAC clarified that "important data" will be assessed as data important from the perspective of the state, rather than the perspective of a company or individual.

In the draft Guidelines for Cross-border Transfer Security Assessment released on May 27, 2017, "important data" is broadly defined as data that can "influence or harm the government, state,

military, economy, culture, society, technology, information… and other national security matters." Relevant bureaus are required to further clarify the specifics of what is "important data" within its industry.

The expansiveness of this definition, though slightly more detailed than before, does little to allay fears over government access to critical information, such as propriety data and source code, since it leaves considerable room for the government to define "important data".

The revised draft Measures also clarified that "personal information" can be sent outside of China with implied consent, such as by sending an email abroad. Previously, it was unclear whether express consent to export personal data abroad would be needed.

Proactive compliance recommended

Although businesses have until the end of 2018 to comply with the data localization requirements, and many supporting regulations and guidelines have yet to be finalized or issued, it is recommended that companies proactively take steps to review their exposure to the Law.

The CAC recently shut down dozens of celebrity news and gossip accounts on Chinese platforms, such as Sina Weibo, WeChat, NetEase, and Baidu, citing privacy provisions included in the new Law as the basis. Further, the Central Commission for Discipline Inspection criticized the CAC soon after the Law came into effect, stating that it had "for a period not carried out general secretary Xi Jinping's important instructions and requirements resolutely and promptly enough."

As CAC regulators have already taken steps to enforce the Law, and may be under pressure from higher authorities to swiftly enact them, companies are advised to take proactive steps to comply. Although many of the exact steps to take are unclear thanks to the Law's ambiguity, a proactive approach demonstrates a willingness to comply with regulators.

In the meantime, businesses with operations and customers in China are advised to monitor for further clarifications and supporting measures to the Law.