FEBRUARY 27, 2017

Legaltech news ONLINE

An ALM Publication

Are You Ready for the New China Cybersecurity Law?

A Consilio survey found 75 percent of legal tech professionals are unfamiliar with the law, but multinational companies can still prepare before the June implementation.

BY ZACH WARREN

In December 2016, China passed a comprehensive Cybersecurity Law, expanding the country's data localization requirement once it goes into effect this June and sparking heated debate among Chinese lawmakers. Some experts say even more legislation could be on the way.

With China such an important emerging market for many multinational companies, law firms and legal departments should be as aware of this change as they are of, say, the EU's General Data Protection Regulation, right? Not so, found one recent survey.

Credit: BeeBright/Shutterstock.com

In Consilio's survey of 118 legal technology professionals at Legaltech New York, 75 percent of respondents said they are not familiar with China's new Cybersecurity Law (found in English on China Law & Practice), with only 2 percent saying they were very familiar. Furthermore, just 14 percent said they are "very concerned" about this new law, despite 57 percent indicating that they had at least one legal matter in China over the past year.

The new law will require foreign companies conducting business in China to localize their data within the country's mainland, as it may contain sensitive privacy data or state secrets. Organizations that do not localize their data face potential financial penalties, including the possible loss of their ability to conduct business in mainland China. Dan Whitaker, managing director of Consilio's China operations, said this is "an effort to catch up with the rest of the world in terms of data privacy for the protection of consumers."

"For attorneys, it makes very clear the overwhelming bias of

the Chinese government that data stemming from an investigation or litigation should remain in China," Whitaker added. "China is a fan of the cloud—as long as it's a Chinese cloud. This means increased dependence on providers with a presence in China and experience in working in the market here. For enterprises, this means increased review of the types of data flowing in and out of the country."

The possible criminal penalties, though, should bring pause; Whitaker noted "public surveillance, imprisonment, and the death penalty are all listed as possibilities for violating the state secrets provision of the Cybersecurity Law." In the past, "documents as innocuous as a list of customers, a pricing spreadsheet, or even a weather report have been deemed state secrets."

With these consequences in mind, it may seem odd that foreign counsel, particularly U.S.-based attorneys, are not aware of the law. But awareness may be a matter of contact with the Chinese market, said Tiana Zhang, a partner in the Shanghai office at Kirkland & Ellis. She told Legaltech News that "U.S. in-house counsels of multinational companies (MNCs), especially those with a significant presence in China, are increasingly aware of China's new cybersecurity law," even ranking it as one of the top compliance issues they face.

"With regard to legal technology professionals' familiarity with the law, because the law was recently published and many key provisions and concepts remain ambiguous or undefined, most professionals are in the process of studying the law and related regulations," she added.

As the law does not go into effect until June 2017, there is still time for legal counsel—whether they are aware of the law's intricacies or not—to study and prepare for the data localization and other requirements of the law. And part of that preparation, Zhang noted, is having conversations with relevant authorities in the country.

"We are aware of informal discussions between cybersecurity authorities and companies, including some MNCs (mostly those that are considered potential critical infrastructure information operators) regarding compliance with the new law," she said. "Protecting space sovereignty and enhancing cybersecurity is a top priority for the Chinese government. It is very likely that when the Cybersecurity Law is fully implemented later this year, there will be a focus on enforcement of the law."

Whitaker echoed that statement, saying that he is advising Consilio clients to process and review data in the company's Shanghai data center rather than take "unnecessary risks by taking data out of China."

"The fact is that the new Cybersecurity law is a game-changer in terms of the ability to freely transmit data across borders," Whitaker explained. "Even for companies with sophisticated cybersecurity protocols, this is a new and unwelcome development which increases the cost and risk of doing business in China."

Consilio®

Dan Whitaker, Managing Director
Email: dwhitaker@consilio.com
Phone: +86 13601822938