ARTICLE

China's New National Privacy Law

On August 20, 2021, the top legislative body in the People's Republic of China passed China's first comprehensive data privacy law, the Personal Information Protection Law (PIPL). The PIPL will take effect on November 1, 2021.

At this time, the final version of the law has not yet been released. However, initial drafts of the PIPL suggest the law bears a striking resemblance to the world's most robust framework for privacy protections, Europe's General Data Protection Regulation (GDPR).

The GPDR and the PIPL have similar definitions for "personal information." And the PIPL, like the GDPR, contains provisions that require organizations or individuals handling Chinese citizens' personal data to minimize data collection and to obtain prior consent. In addition, the PIPL requires companies handling personal user data to have a clear and reasonable purpose for doing so and must limit collection and handling to the "minimum scope necessary" based on the stated purpose.

One key aspect shared by both the PIPL and the GDPR is the territorial scope. Like the GDPR, the PIPL extends its territorial scope to the processing of personal information conducted outside of China, provided that the purpose of the processing is: (i) to provide products or services to individuals in China, (ii) to "analyze" or "assess" the behavior of individuals in China, or (iii) for other purposes to be specified by laws and regulations.

In addition, the PIPL requires offshore "personal information processing entities" subject to the PIPL to establish a "dedicated office" or appoint a "designated representative" in China for personal information protection purpose. This requirement largely follows the GDPR's requirement for the appointment of an "EU representative" for offshore controllers.

In terms of enforcement, if an entity violates the PIPL, Chinese regulators may issue warnings, order corrective actions be implemented, confiscate illegal income, suspend services or issue a fine. The fine can be up to 50 million Renminbi (RMB – the official currency of China) or 5% of an organization's annual revenue. Unlike the GDPR, the PIPL does not specify whether the annual revenue refers to the worldwide turnover or revenue generated specifically in China. Chinese regulators have significant discretion with respect to penalties. In addition, entities subject to the PIPL will be liable for civil damages if they are found to have violated individual protections provided by the PIPL.

Notwithstanding the similarities between the PIPL and the GDPR, some obligations set forth within the PIPL are, arguably, more stringent than those set forth within the GDPR. And, to make matters even more complicated, some obligations found in the GDPR are not included in the PIPL. This poses a significant compliance challenge to companies operating internationally.

The enactment of the GDPR triggered an international focus on broad-based data privacy laws. Broad privacy laws have been moving across the globe like wildfire; quietly, in the background of the pandemic. In the span of the last 18-24 months we have seen activity in China, Brazil, New Zealand, California (the CCPA and CPRA), Singapore, Australia, Canada and many more. Any organizations with an international footprint should review and update data privacy compliance programs and re-evaluate the adequacy of risk transfer mechanisms – whether they be contract-based or insurance.

Kelly Geary
National Executive Risk & Cyber Practice Leader
kelly.geary@epicbrokers.com
(847) 385-6832

Let's Talk

Find out how EPIC Insurance Brokers & Consultants can help your business.

Visit epicbrokers.com →