BRACEWELL

INSIGHTS

# China's New Data Privacy Law Is Sweeping and Serious: Avoid the High Cost of Noncompliance

August 24, 2021

*By:* ***Seth D. DuCharme*** ***Lucy Porter***

Last Friday, China passed the world's harshest data privacy law, threatening violators with fines of up to 50 million Yuan (or about $7.7 million at the time of publication) or 5% of annual revenue. The ***Personal Information Protection Law*** ("PIPL") builds on China's security-focused data protection regime, but it is the country's first law that purports to provide individuals with rights and protections related to their personal information.

PIPL, which goes into force November 1, 2021, applies to entities, including entities that do business entirely outside of China, that collect, store, use, transmit, provide, or otherwise handle personal information belonging to natural persons within China's borders. Entities governed by PIPL are called "personal information handlers," and personal information handlers based outside of China must "establish a dedicated entity or appoint a representative" within China to be responsible for PIPL compliance.

GDPR-compliant companies have a leg up on PIPL compliance. But GDPR compliance will not pass muster under PIPL, which is why IAPP VP and Chief Knowledge Officer Omer Tene ***recommends*** that "[i]f you're doing business in China, get legal advice. They're not playing around."

Some PIPL provisions, such as those related to overarching data protection principles and individuals' access and erasure rights, look similar to GDPR, but PIPL is different in a number of important ways. For example, companies that rely on GDPR's "legitimate interest" provision as a lawful basis for processing employee data will note that PIPL does not have a similar provision.

The circumstances under which individuals must be notified under the two regulations differ, as PIPL requires explicit notice to be provided before data collection occurs, except where laws or regulations provide that confidentiality may be preserved or notification is not necessary. PIPL also addresses a few unique, hot-button areas of privacy law, such as facial recognition. Additionally, unlike GDPR, PIPL does not regulate or limit access by the PRC central government to personal information.

Perhaps the most important differences between PIPL and GDPR, however, come from PIPL's data transfer restrictions. These provisions build on China's ***Cybersecurity Law*** and the new ***Data Security Law*** ("DSL"), both of which establish a protectionist, security-focused framework through mechanisms like data-localization requirements, which require certain

types of data to be stored on servers within China.

When DSL becomes effective September 1, Chinese organizations and individuals will be prohibited from transferring data stored in China "to the justice or law enforcement institutions of foreign countries without the approval of" Chinese authorities. The PIPL will expand this prohibition to Chinese residents' personal information, requiring all personal information handlers to receive permission from Chinese authorities before transferring that information to foreign courts or law enforcement.

PIPL also requires all cross-border data transfers of personal information to meet a "necessity test," and individuals must receive notice and give specific consent prior to the transfer. And, even if the transfer passes the necessity test and is consented to, the transfer must meet one of the following conditions:

- Receive approval from government authorities following a security assessment;
- Obtain certification from government authorities;
- Conclude a contract with the foreign entity receiving the data that comports with a standard contract drafted by government authorities; or
- Comply with "other conditions" in law or regulations (a catch-all provision).

In addition to entity fines, individual fines between 100,000 and 1 million Yuan are included and violators of PIPL can be publically called-out on China's social credit system or be prohibited from doing business in China. And, like GDPR, PIPL provides individuals with a private right of action to be compensated for any losses suffered due to a handler's improper processing of personal information.

The consequences of non-compliance with PIPL are harsh, and PIPL's passage is just one of many recent indications that Chinese authorities are eager to ramp up cyber enforcement. Companies that do business in China should seek legal advice as soon as possible to ensure compliance. Bracewell's Data Security & Privacy team team is well-versed in compliance program reviews and ready to help clients navigate China's sweeping new data privacy and security regime.