DECEMBER 2021

Understanding China's New Personal Information Protection Law – Key Questions and Answers with attorney (Shan) Jessica Chen at Mazzola Lindstrom LLP

Overview:

On August 20, 2021, the Standing Committee of the National People's Congress of the People's Republic of China passed the Personal Information Protection Law, which went into effect November 1, 2021.

The PIPL works together with the existing Cybersecurity Law and the Data Security Law, creating a broader regulatory architecture governing cybersecurity and data privacy protection in China. As a result, this new law will now have a significant impact on the data compliance practices of both domestic and multinational companies to the extent they process or use the personal information of individuals located within China.

As the first comprehensive legislation on personal information protection in China, the PIPL specifies the scope of personal information; clarifies the legal bases for processing personal information; lays down the obligations and responsibilities imposed on processors; and imposes stringent requirements on data localization, safeguarding the interests of China in the case of cross-border transfer of personal information.

To better understand the PIPL, Ms. (Shan) Jessica Chen answers key questions concerning this new law. Jessica handles cross-border commercial litigation and transactions and is a member of the firm's China Practice group.

Q — Can you give us a general overview of China's new IT compliance ruling that went into effect on November 1, 2021? What are the overarching restrictions and implications, and what are the penalties for violations?

A — Sure. This law, officially called "The Personal Information Law of the People's Republic of China," is the first national data privacy statute passed in China. The PIPL builds upon China's Cybersecurity Law and Data Security Law and is partially based on the European Union's General Data Protection Regulation. The primary purposes of the PIPL are to protect personal information, rights, and interests; standardize personal information handling activities; and promote appropriate use of personal information.
Notably, *The Wall Street Journal* described the PIPL as "one of the world's strictest data privacy laws." It's important to note that this new data privacy law specifically focuses on protecting personal information and redressing personal data leakage. The PIPL extends to the handling of all personal information of natural persons within the borders of China and in Article 3 even extends its reach beyond China's borders under certain circumstances. This means that the PIPL will affect almost every major business in the world.

The PIPL addresses individual privacy through mandated limitations on how companies can collect, use, store, and process personal information. Article 4 defines "personal information" as any information related to an "identified" or "identifiable person," not including "anonymized" data. By including the word "identifiable" in the text of the law, the PIPL greatly expanded the scope of data that is covered by the law.

Companies found to have violated the PIPL's rules face penalties and other redress. For example, unlawful income may be seized, and the businesses could face fines of up to RMB 50 million (approximately US $7.825 million as of today's rate) or 5% of their annual revenue.

Other possible penalties include suspension of certain business activities or cessation of the business itself and reporting to relevant authorities for revocation of professional licenses and permits. In addition, violations may negatively affect a business's credit score.

Under Article 66, persons found directly responsible for the violations may be fined between 100,000 and RMB 1 million and may be banned from serving in certain roles (such as a director, supervisor, high-level manager, or personal information protection officer) for a certain period.

Q — How does China plan to enforce PIPL violation penalties for companies outside China?

A — We don't have clear answers to this yet. It remains to be seen how Chinese authorities will interpret and enforce the PIPL's provisions for conducts outside China. Overall, we anticipate seeing vigorous enforcement.

Moreover, since the PIPL only gives companies two months of preparation time, in the beginning, it is not certain who the law will focus on and what the priorities will be. That being said, businesses should undoubtedly make good-faith efforts to comply with the PIPL and adjust their strategies as more details and clarities evolve.

Businesses should be aware that the PIPL stipulates that if personal information handlers reject an individuals's privacy requests to exercise his or her rights, the individual may file a court proceeding in accordance with Article 50. The PIPL thus provides a mechanism for individuals to receive compensation from data handlers for the damage they suffer or the unlawful benefits that the violators obtain, "if the handling of personal information infringes upon the rights and interests and results in harm." Importantly, Article 69 places the burden of proof on the personal information handler; if personal information handlers cannot prove they are not at fault, they will be held liable. Article 67 provides that acts found to have been illegal will be made public and recorded in the credit files.

Finally, if a violation harms many individuals, a lawsuit may be filed pursuant to Article 70 by the People's Procuratorates – the government prosecutor – or by specifically designated consumer organizations and organizations designated by the state cybersecurity department.

Q— Does this law affect data privacy for both B2B businesses and B2C businesses?

A — It applies to both B2B and B2C, so long as they are handling the personal information of a natural person. There is no exception.

This may be more complicated, however, for cross-border scenarios. Suppose a US company signs a purchase contract with a clothing manufacturer in China. The PIPL likely does not apply because the US company is not "providing products or services to natural persons inside the borders" within the scope of Article 3. However, if a US company were to sell its products to a Chinese company, the personal information of the contact person at the Chinese company might be deemed to be protected by the PIPL. On the other hand, it may be argued that the US company's purpose is to provide products to a company rather than to a natural person and that, therefore, the long extraterritorial arm of PIPL would not apply depending on how "any other circumstance as provided by law or administrative regulations" is interpreted.

Q — How does this law compare to the European Union's General Data Protection Regulation restrictions?

A — The PIPL consists of 74 articles in 8 chapters, and the GDPR consists of 99 articles in 11 chapters. Some notable similarities and differences are as follows.

Similarities:

1. Both the PIPL and the GDPR are extraterritorial, meaning they apply to personal data wherever it may be processed.
2. Both the PIPL and the GDPR define personal data as involving identified and identifiable natural persons.
3. Both the PIPL and the GDPR rely upon consent as the primary legal justification for the use of personal data and provide multiple legal bases for protecting personal information in addition to consent.
4. Both the PIPL and the GDPR have a data breach notification requirement.
5. Both the PIPL and the GDPR require data protection impact assessments in certain situations.
6. Both the PIPL and the GDPR provide various rights to individuals, such as the right to access information, correct or amend the information, and object to/restrict processing.

Differences:

1. Some terminologies are different. For example, the PIPL uses "individuals" instead of "data subjects" used in the GDPR. The PIPL uses "personal information handlers" instead of "persona data controllers." The PIPL uses "entrusted parties" rather than "personal data processors."
2. The PIPL has a strong data localization requirement while the GDPR does not.
3. Article 13 of the PIPL strictly enumerates the bases for collecting personal information. The GDPR, however, allows for personal information to be collected if there is a "legitimate interest" to do so. Among the enumerated bases available under the PIPL are where consent is obtained, where necessary for human resources management, where necessary to respond to public health and security matters, news reporting and opinion polling, and where otherwise required by law.
4. Unlike the GDPR, which has a closed list of "special categories" of personal data, the PIPL has an open list of "sensitive information."
5. The PIPL requires special treatment for children below the age of 14 years, which is different than the age threshold of the GDPR.
6. The PIPL empowers the next of kin to exercise the rights of deceased persons.
7. The PIPL requires a representative in China for foreign data handlers.
8. Unlike the GDPR's specific 72-hour deadline, the PIPL requires "immediate" notifications of data breaches.
9. Unlike the GDPR, the PIPL further requires a controller to conduct a data protection impact assessment – DPIA – in advance of certain situations, such as transferring personal data across the border, contracting a third-party data processor, and providing personal data to another controller.
10. The fines under the PIPL can be up to RMB 50 million or 5% of the organization's annual revenue. In contrast, the GDPR sets fines up to €20 million or 4% of annual global turnover, whichever is greater.

Q — Will my business be affected by the PIPL? What are some of the key rules to keep in mind?

A — Due to the PIPL's significant breadth, almost every business operating in or doing business with China must ensure they are in compliance with the PIPL since November 1, 2021.

Of course, a comprehensive strategy has to be in compliance with all the PIPL's requirements, which requires a thorough understanding of the PIPL, a clear understanding of the differences between the PIPL and the GDPR, and preferably an understanding of the Chinese governmental, cultural and business practices.

Some key rules to keep in mind are:

1. If your organization is outside China but handles the personal information for the purpose of providing products or services to natural persons inside the borders, analyzing or assessing activities of natural persons inside the borders, or other circumstances provided in laws or administrative regulations, you must establish a dedicated office or appoint a designated representative in China.
2. You need consent for nearly everything. You also need to provide individuals the right to withdraw their consent, and individuals can revoke their consent at any time.
3. You need to establish a valid lawful basis for processing personal data, based upon the seven lawful bases set forth in the PIPL.
4. You need a plan to respond to data breaches.
5. If your organization is involved in cross-border data transfers with China, you may only transfer personal information out of China with the informed consent of the individuals, where necessary "for business purposes" and after completing a risk assessment. You must also meet one of the following conditions:
   a. Pass a security assessment organized by the Cyberspace Administration of China.
   b. Obtain a personal information protection certification by an organization authorized by the CAC.
   c. Enter a contract with the foreign recipient based on a standard contract formulated by the CAC.
   d. Comply with such other rules and regulations promulgated by the CAC.
6. You need to formulate internal management structures and operating rules.

Another tip for organizations is that businesses should pay close attention to any developments, supplemental documents, and enforcement actions as they continue to evolve. For example, on November 14, China released its draft of Network Data Security Management Regulations for public comments until December 13th, 2021.

Of course, businesses that are unfamiliar with these rules or are unsure about their meaning and application should seek advice and guidance from experienced legal counsel.

*This Q & A does not constitute legal advice from either Ms. Chen or Mazzola Lindstrom LLP.