A Brief Note on China's Personal Information Protection Law

Guhathakurta, Rahul

Veröffentlichungsversion / Published Version
Zeitschriftenartikel / journal article

IndraStra
www.indrastra.com | ISSN 2381-3652

A Brief Note on China's Personal Information Protection Law

IG indrastra.com/2022/03/China-Personal-Information-Protection-Law.html

By Rahul Guhathakurta

The *Personal Information Protection Law (PIPL)*, China's new data privacy law, entered into force on November 1. Noncompliance has severe penalties, including fines of up to $7 million or 5% of a corporation's annual income, the loss of business licenses, and even leading to shutting down of a company.

This newly enacted law has joined other data protection laws recently established by nations or regions, such as the EU's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA). Other countries, like Brazil and India, are enacting data privacy rules.

The PIPL, as a whole, applies to both enterprises and individuals that process personally identifiable information (PII) of Chinese citizens outside of China. To build a larger framework for cybersecurity and data privacy protection in China, PIPL will work alongside China's existing Cybersecurity and Data Security Laws.

To protect the personal information of Chinese citizens, PIPL requires offshore firms to set up a *"dedicated office/entity"* or a *"designated representative"* in China. The domestic authority will need to know the name and contact details of the local agent or representative.

The major PIPL definitions for protected data and entities are outlined here; they are very similar to GDPR definitions;

Personal Information is defined as *"any information (such as video, audio, or image data) relating to an identified or identifiable natural person, regardless of whether it is in electronic or other forms."*

And, ***Sensitive Personal Information*** includes *"personal information that, once leaked, or illegally used, may easily infringe the dignity of a natural person or cause harm to personal safety and property security, such as biometric identification information, religious beliefs, specially designated status, medical health information, financial accounts, information on individuals' whereabouts, as well as personal information of minors under the age of 14."*

However, de-identified data is not considered ***"personal information"*** under the PIPL. Anonymization refers to processing personal data in a way that makes it hard to identify individuals and cannot be recovered after processing.

In summary, PIPL gives Chinese citizens more control and protection over their personal data. Organizations that process personal data of Chinese citizens now face stricter regulations, including but not limited to:

- Obtaining individuals' consent to process personal information
- Addressing individuals' requests to exercise their rights over personal information
- Implementing adequate safeguards and security measures to protect personal information

Adhering to limitations on cross-border transfers of personal information outside of China

Conducting Personal Information Protection Impact Assessments

Supervising third-party processors to ensure compliance with PIPL.

Timeline

The first PIPL draft was submitted to the National People's Congress on October 13th, 2020, and released for public feedback on October 21st.

On August 20, 2021, China's Personal Information Protection Law (PIPL) was signed into law.

The law became effective on November 1, 2021

Challenges for non-Chinese cloud-based service providers

In mid-August of last year, China's Ministry of Industry and Information Technology (MIIT) warned that 43 Chinese apps, including Tencent's WeChat, had illegally shared user data and had less than two weeks to correct the issue. t is important to note that this enforcement is consistent with similar efforts by the Chinese government to protect data from the growing smart car industry. For example, the country has publicly expressed concerns about Tesla's data privacy and designated the popular ride-hailing company DiDi Chuxing as a Critical Information Infrastructure (CII) regulator, increasing the company's data privacy requirements.

However, although the full scope of what CII regulators must do in order to be compliant with data rules has not yet been released, the stakes could not be greater. Most governments have set up fines that are insufficient to deter firms from engaging in unsafe data practices; nevertheless, China has set fine amounts that range from $7.7 million to 5 percent of a company's previous year's revenues.

Also, it is imminent the operating costs for non-Chinese companies operating in China will skyrocket. Those in the technology, retail, automobile, banking, and pharmaceutical sectors should expect upheaval.

non-Chinese companies may be required to take these actions;

Redesign information systems to ensure that data is appropriately localized for the Chinese market.

To limit risk, evaluate and segment vendors and supply chains.

Deals should be reevaluated in light of altered costs and returns on investment.

Adapt legal entity structures and tax techniques to changing business operations.

Conclusion

Controlling data throughout its lifecycle is no longer an industry best practice; it has become the *"new minimum baseline"* in China. And, for non-Chinese companies doing business with China, particularly those focused on consumers and digital solutions, it is vital to assess their current condition and undertake data audits. This enables them to comprehend their position inside the new Law and any potential vulnerabilities.

About the Author

Rahul Guhathakurta (ORCID: **0000-0002-6400-6423**) is a strategic management consultant and is currently affiliated with Anaha Innovations — an Ahmedabad-based technology business incubator and private equity firm. Also, he is a primary investor in IndraStra Global — a US-based publishing company.