Published on *The National Law Review* https://natlawreview.com

Five Immediate Steps to Take in Preparation for China's New Comprehensive Privacy Law

Article By:

Elizabeth (Liz) Harding

L. Hannah Ji-Otto

China has recently joined the list of countries that have adopted the world's strictest data-privacy laws. Given China's desirability as both a market for and a source of data, companies worldwide have started making early efforts to mitigate the impact of these new requirements on their businesses. This client alert provides five concrete steps that an organization can take now that China's new privacy law has become effective.

For background, China's first attempt to regulate the internet was its Cybersecurity Law ("CSL") of 2017. The year of 2021 is a significant year in privacy for China. Earlier this summer, China passed the Data Security Law of the P.R.C ("DSL"), which came into effect on September 1, 2021. Thereafter, China passed the Personal Information Protection Law of the P.R.C. ("PIPL"), which came into effect on November 1, 2021. The PIPL resembles EU's General Data Protection Regulation ("GDPR") in many aspects and is promising to reshape the handling of personal information in China.

Upon reviewing the PIPL, our firm has identified five steps an organization may take to shore up their privacy compliance programs to meet or exceed the requirements of the PIPL:

Review all data processing activities to decide whether the PIPL applies

The PIPL applies to organizations processing data *outside* of China's territory. Article III of the PIPL states that in addition to any data processing activities within China, it is also meant to encompass:

Processing outside of China, of personal information of natural persons who are in China, if such processing is: (1) for the purpose of providing products or services to natural persons in China; (2) to analyze/evaluate the behavior of natural persons in China; or (3) other circumstances prescribed by laws and administrative regulations.

Further, organizations outside of China subject to this part of Article III must establish special entities or designate representatives in China, register their identities with the Chinese government, and report certain additional information to relevant governmental authorities.

Similar to the GDPR (which applies to non-EU data controllers or processors under many circumstances) many organizations outside of China will suddenly find themselves subject to this new comprehensive privacy law. Those organizations will need to decide between investing resources in complying the strict requirements in the PIPL or reorganize their operations to minimize the ability for Chinese regulators to assert jurisdiction over their operations in China.

Based on the statute the statute, China intends to regulate the data of any company performing marketing, transacting business, or performing data analysis in China. We recommend that organizations doing business in China work with their attorneys to review all of their data processing activities and take inventory of all data processing activities that fall under Article III of the PIPL.

Find a lawful basis for each of your data processing activity

Similar to the GDPR, the PIPL requires a company to establish a lawful basis for its activities prior to performing any processing of personal information. The PIPL provides the following legal base for processing personal information, at least one of which a company must meet to comply with Chinese law:

1. The processing was expressly consented to by the data subjects;

2. Is necessary for concluding or performing contracts to which the data subject is a party, or necessity for implementation of human resources management in accordance with legally adopted labor rules and systems and legally-concluded collective contracts;

3. Is necessary for performing legal duties or legal obligations;

4. Is to respond to public health emergencies, or is necessary necessity for the protection of natural persons' life, health, and property safety under emergency circumstances;

5. Constitutes processing, within the reasonable scope, of personal information for conducting news reports, public opinion supervision, and other acts for the public interest;

6. Constitutes processing, within the reasonable scope and in accordance with the PIPL, of personal information that has been made public by data subjects or through other lawful means; and

7. Other circumstances as stipulated by laws and administrative regulations.

The breadth with which the above legally recognized purposes will be interpreted by Chinese regulators remains uncertain due to how recently the law was passed. However, once an organization has identified all the data processing activities subject to the PIPL, it should analyze those data processing activities and assign each of them as least one legal basis. Any of the identified activities that cannot fit within the above categories are prohibited by the new law.

Establish a mechanism to respond to data subjects' requests

Chinese individuals have a new set of privacy rights under the PIPL and covered organizations are required to establish "easy to use" mechanisms to respond to any requests made under the PIPL. These individual rights are:

- The right to know and to make decisions relating to their personal information;
- The right to restrict or prohibit the processing of their personal information;
- The right to consult and copy their personal information from the processors;
- The right to data portability;
- The right to correct and delete their personal information; and
- The right to request the processors to explain their processing rules.

Importantly, individuals have standing to sue in court if organizations reject their requests to exercise their rights. To promptly honor those data subjects' requests in compliance with the PIPL, an efficient mechanism vetted by the legal and adopted by the business is a must-have. Some organizations have invested in establishing mechanisms and processes to receive and respond to consumers requests under the GDPR and the California Consumer Protection Act ("CCPA"). Since many of the data subjects' rights resemble the rights provided under the GDPR and the CCPA, those organizations with existing mechanisms have a head start in complying with the portion of the PIPL. If a company does not have any mechanism to respond to such requests in place, it is a good time to do so as requirements such as these are quickly becoming commonplace worldwide.

Data Processor's[1] Obligations

The PIPL imposes various obligations on the processors of personal information, including obligations to:

- Formulate internal management systems and operation procedures;
- Implement classified management of personal information;
- Adopt corresponding technical security measures such as encryption and de-identification;
- Reasonably determine the operational authorizations for personal information and provide regular security education and training for operational staff;
- Formulate and implement response plans for security incidents relating to personal information;
- Conduct regular compliance audits; and
- Adopt other security measures as stipulated by laws and regulations.

Certain companies such as operators of critical information infrastructure ("CIIO"), processors of sensitive personal information, companies offering important Internet platform service involving a huge number of users, and complex types of businesses are subject to more onerous obligations such as appointing a personal information protection officer and/or an independent supervisory board, conducting privacy impact assessments for the processing activities, and publishing regular

“social responsibility reports.”

To comply with this portion of the PIPL, organizations must do two things: (i) determine applicable PIPL requirements by analyzing the types the businesses using the data, the types of data it processes, and the volume of the data; and (ii) examine its existing technical and organizational measures against the applicable requirements. It is recommended that businesses work together with both their internal data privacy officers as well as their legal teams to perform this analysis and update it on a regular basis.

Set up a mechanism to legally transfer data out of China

China’s CSL of 2017 contains a notorious data localization requirement, which makes transferring data outside of China difficult. Unfortunately, the PIPL significantly increases this level of difficulty. Under the PIPL, organizations are prohibited from transferring personal information outside of China, unless the transfer satisfies one of the four enumerated conditions in the PIPL. These conditions are:

- The transfer passes a security review organized by the Cyberspace Administration of China (“CAC”) if the transferor is an CIIO or the volume of the affected personal information reaches the threshold specified by CAC[2];
- The covered organization has a personal information protection certification from a professional agency in accordance with the rules of the CAC;
- The covered organization has entered into an agreement with the overseas recipient based on a standard contract formulated by the CAC; or
- The transfer satisfies other conditions provided by laws, administrative regulations or the CAC.

Additionally, the organization subject to the PIPL must notify data subjects of certain information and obtain their informed consent on the transfer, on top of any other consents the organization may already have.

To transfer data outside of China in compliance with the PIPL, the first step is to determine whether your organization is a CIIO or an organization that processes important data or a large volume of personal information. China’s regulators have a high preference to keep data collected by those organizations in China. However, if an international data transfer is truly necessary, such organizations must pass a mandatory security assessment conducted by the CAC[3]. For all the other organizations, until the CAC authorizes other means, the choices are between either obtaining certifications from the CAC, or signing CAC authorized standard contractual clauses with data recipients.

Violations of the PIPL may lead to an administrative fine of up to RMB 50 million or 5% of the organization’s turnover in the last year. Other penalties include order for rectification, warning, confiscation of illegal gains, suspension or cessation of service, cessation of operation for rectification, and revocation of operating permits or business licenses. The person-in-charge or other directly liable individuals may also be individually liable and fined or otherwise penalized. Due to PIPL’ extraterritorial reach, its broad coverage and added scrutiny, and the potential liabilities for violations, the compliance costs for overseas organizations to operate under the new framework

established by the PIPL will likely increase. Given the size and scope of markets in China, many businesses will likely determine that the gain is worth the risk. Any such organizations would do well to start preparing now.

[1] Different from the GDPR, the term “Processor” under the PIPL means “an organization that is subject to the PIPL.” This could include both data controllers and data processors as they are defined by the GDPR.

[2] The Cyberspace Administration of China is the main enforcement authority in China for privacy and security laws.

[3] According to the drafted “Regulation on Cross-Border Data Transfers” released by the CAC on October 29, 2021, organizations must apply for such mandatory security assessments conducted by the CAC before transferring data outside of China under the following four scenarios: (1) when exported data were collected by CIIOs; (2) when exported data include Important Data ; (3) when processing the personal information of over 1 million data subjects; (4) when an organization intends to export personal data of 100,000 data subjects or sensitive personal data of 10,000 data subjects.

National Law Review, Volume XI, Number 306