September 10, 2021

China Passes Personal Information Protection Law

Attorneys
Katherine Wang
David Chen

On August 20, 2021, the Standing Committee of the National People's Congress promulgated the Personal Information Protection Law (PIPL), which will become effective on November 1, 2021. The PIPL is the first comprehensive national level personal information protection law in China, which systematically regulates the processing of personal information by entities and individuals. The PIPL, together with the Cybersecurity Law, which was promulgated in 2017, and the Data Security Law, which was promulgated earlier this year, form the three pillars of China's comprehensive data protection legal regime.

This Alert provides a summary of the highlights of the PIPL, discusses the implications on domestic and foreign businesses operating in China, and compares the PIPL with the European Union (EU) General Data Protection Regulation (GDPR), which has greatly influenced many of the concepts included in the PIPL.

Jurisdictional Scope and Extraterritorial Applicability

The PIPL applies to all data processing activities conducted in China involving personal information of individuals located in China. Additionally, the PIPL also applies to data processing activities conducted outside of China involving personal information of individuals located in China under the following circumstances: (1) where the processing is for the purposes of providing products or services to individuals located in China, (2) where the processing is for analyzing and evaluating the behavior of individuals located in China, or (3) under circumstances prescribed by laws and administrative regulations. This closely mirrors the jurisdictional scope and extraterritorial applicability of Article 3(2) of the GDPR, and, as a result, foreign businesses that process personal information of individuals located in China will need to review their data processing activities to determine whether such activities will require them to comply with the PIPL and subject them to the possibility of significant penalties for non-compliance under the PIPL. Notably, the PIPL also contains a catch-all provision that authorizes the Chinese government to further expand the PIPL's extraterritorial applicability in other laws or regulations.[1]

In addition to having to comply with the data privacy and protection requirements for personal information processors under the PIPL, similar to Article 27 of the GDPR, offshore personal information processors must appoint a representative located in China to be responsible for matters related to personal information protection, and report the representative's contact information to relevant data protection regulators.[2] Notably, the PIPL requirement does not contain the exceptions for occasional processing, certain lower-risk processing, or processing by public authorities or bodies as in Article 27 of the GDPR. For foreign businesses that do not have subsidiaries in China, this will require engaging a third party to act as its local agent or representative. But, as has been the experience in the EU with the implementation of Article 27 of the GDPR, it remains to be seen how foreign business without local subsidiaries will be able to meet this requirement or whether third parties will be willing to serve such role and bear data privacy and protection liabilities on behalf of foreign businesses.

Personal Information and Sensitive Personal Information

The PIPL regulates the processing of personal information and defines personal information as information related to identified or identifiable natural persons recorded by electronic or other means, excluding anonymized information. This definition is almost identical to the definition of personal information under Article 4 of the GDPR. The exception for anonymized information, which is defined as personal information processed so that it is impossible to identify certain natural persons and that such identification cannot be recovered, also appears to take the strict anonymization approach of the GDPR.[3]

Under the PIPL, sensitive personal information is defined as personal information that may lead to harm to the dignity of natural persons or serious harm to the safety of persons or property if disclosed or unlawfully used, including information relating to biometric characteristics, religious beliefs, specifically designated status, medical health, financial accounts,

and individual location tracking, as well as the personal information of minors under the age of 14.[4] This definition is broader in scope when compared with the analogous concept of special categories of personal data under the GDPR, as it additionally covers financial accounts and individual location tracking. Processing of sensitive personal information is subject to stricter requirements. An organization or an individual may only process sensitive personal information when necessary and for specific purposes, and is required to obtain the separate consent of the individual data subject. They must also notify the individual data subjects of the need for processing their sensitive personal information and the impact such processing may have.[5] Life sciences companies and healthcare service providers will need to pay special attention to these requirements.

In particular, the requirement for "separate consent" is introduced in the PIPL, and notably also applies where personal information is being provided to third parties or transferred to a party located outside of China. While it remains to be seen how the separate consent requirement can be met, the PIPL appears to impose a higher requirement for consent where separate consent is required, which will require businesses to review how they plan to obtain consent in such circumstances.

Legal Basis of Processing Personal Information

The PIPL adopts a similar approach to GDPR in that processing—which includes collection, storage, use, transfer, provision, publication and deletion[6]—of personal information is not permitted unless a legal basis exists. The legal bases for processing personal information are enumerated in the PIPL and include (1) where it is on the basis of consent of the individual concerned, (2) where necessary to conclude or perform a contract with the individual concerned, or to implement human resources management in accordance with labor rules and regulations and collective contracts formulated in accordance with law; (3) where necessary for the performance of statutory duties or obligations, (4) where necessary to respond to public health emergencies or for the protection of the life, health, and property safety of individuals, (5) for news reporting and supervision of public opinion for the public interest where the processing is reasonable in scope, (6) where it involves the processing of personal information that has been publicly disclosed by the individual concerned or otherwise lawfully publicly disclosed, where the processing is in accordance with the PIPL and is reasonable in scope, and (7) under circumstances prescribed by laws and administrative regulations.[7]

Notably, there is no equivalent legal basis for "legitimate interests" as under GDPR. Also, the contractual necessity legal basis specifically includes a reference for processing human resources data. This provides a clear legal basis to process human resources data based on human resources policies and labor contracts that have been properly implemented in accordance with Chinese labor laws. Nonetheless, obtaining employee consent to process human resources data is expected to continue to be the recommended market practice. Finally, the legal basis for processing publicly disclosed personal information is relevant to web data-scraping activities, but the scope of activities permitted under this legal basis remains to be seen.

Cross-Border Data Transfer

The PIPL also regulates the cross-border transfer of personal information. Entities that need to transfer personal information outside China need to meet at least one of the following conditions: (1) pass a security assessment established by the Cybersecurity Administration of China (CAC), China's top cybersecurity regulator, (2) obtain a personal information protection certification from professional institutions in accordance with provisions of the CAC, (3) enter into a contract with the data recipient in accordance with a standard contract prescribed by the CAC, or (4) fulfill conditions stipulated in other laws or regulations.[8] Notably, all of the enumerated pathways to legitimize cross-border transfers of personal information require further guidance and implementation by the CAC. Therefore, until such guidance and implementation is available, it remains unclear how businesses will be able to comply with this requirement. However, it is expected that in most cases, businesses will need to rely on contractual means to legitimize cross-border transfers of personal information using a similar approach as the use of standard contractual clauses under the GDPR, and so businesses should begin preparing to comply with this requirement by reviewing their contractual arrangements with off-shore data recipients.

Additionally, when transferring personal information outside of China, the transferor must notify the individual data subject of the identity of the foreign recipient, a method of contacting the recipient, the purposes and methods of the recipient's processing, the types of personal information involved, and how the individual data subject can exercise his/her rights against the recipient. Also, the transferor must also obtain the individual data subject's separate consent to the transfer.[9] In order to meet these stricter notice and consent requirements, the general cross-border data transfer notice and consent language often used by companies in the past will need to be reviewed and updated, and in many cases, consent will need to be re-obtained in case there are new off-shore recipients.

Under the PIPL, requirements to store in China personal information collected or produced through activities conducted in China have been expanded to not only include critical information infrastructure operators (CIIOs), as is the case under the Cyber Security Law, but also non-CIIO personal information processors that process a certain volume of personal information that meets or exceeds the as-to-be-determined threshold established by the CAC. Where it is necessary for them to provide such information abroad, they need to pass a security assessment conducted by the CAC.[10]

Furthermore, the CAC has the authority to add foreign organizations or individuals to a blacklist, which has the effect of prohibiting any business or individual from providing personal information of individuals in China to such entities.[11] This will likely be a powerful vehicle to compel compliance with the PIPL by foreign businesses.

Legal Liability

As an impetus for compliance, the PIPL imposes significant penalties for serious violations, including rectification orders, confiscation of illegal gains, business suspension, revocation of business licenses, and, most notably, fines of up to CNY 50 million or 5% of turnover in the previous year. The potential for high penalties under the PIPL mirrors that of the GDPR and will require businesses to undertake compliance efforts similar to those taken to comply with GDPR in order to comply with the PIPL.

Additionally, the directly responsible person inside such personal information processor and other directly responsible persons can incur personal fines between CNY 10,000 and CNY 100,000, and can be prohibited from holding certain management and director positions for a certain period.[12] The potential for personal liability is expected to have a strong deterrence effect on the conduct of managers and business leaders.

Important Internet Platforms and Automated Decision-Making

The PIPL is also innovative in attempting to address privacy concerns that have arisen due to the recent rise of internet platform businesses and the use of data to drive decision-making and personalized content. In this regard, the PIPL imposes additional obligations on important internet platform services providers with a large number of users and complex business models, which include the establishment of independent personal information protection oversight bodies and the regular release of social responsibility reports. The PIPL also intends to level the playing field for the benefit of internet users by requiring use of personal information for automated decision-making to be transparent and fair and providing convenient opt-out options, as well as by prohibiting unreasonably discriminatory pricing or transaction terms.[13]

What to Expect

With the recent promulgation of the Data Security Law and the PIPL and the Chinese government's recent cybersecurity probe against some internet platforms, we are witnessing a heightened legislative and enforcement focus on information privacy and security. The Chinese government attempts to ease the tensions caused by the amassing of large amounts of personal information by for-profit businesses, the privacy interests of Chinese citizens and China's national security interests. While uncertainties remain as to the application of certain provisions of the PIPL, Chinese and foreign business operating in China should commence compliance programs directed at bringing their China-related personal information processing activities into compliance with the PIPL. We encourage companies to continue monitoring the promulgation of relevant laws and regulations and the CAC's administrative and enforcement activities in order to adapt their operations to the new legal regime.

1. Art. 3, PIPL.
2. Art. 53, PIPL.
3. Art. 73, PIPL.
4. Art. 28, PIPL.
5. Art. 29-32, PIPL.
6. Art. 4, PIPL.
7. Art. 13, PIPL.
8. Art. 38, PIPL.
9. Art. 39, PIPL.
10. Art. 40, PIPL.
11. Art. 42, PIPL.
12. Art. 66, PIPL.
13. Art. 24, PIPL.