porterwright

INTERNATIONAL BUSINESS ALERT

NOVEMBER 10, 2021

YUANYOU (SUNNY) YANG
412.235.1484
yyang@porterwright.com

How to prepare your business for China's Personal Information Protection Law (PIPL)

China's newly passed Personal Information Protection Law (PIPL) took effect Nov. 1, 2021. The passing of PIPL in late August has significantly changed the privacy and data protection landscape in China. With such robust legislative changes, it is critically important that companies that operate in China or process personal information of individuals located in China be aware of the new law and take affirmative steps to ensure compliance or risk being faced with serious penalties.

Get ready for PIPL compliance

Impacted companies should prepare for PIPL compliance, especially if they transfer personal information from China to the United States. At a minimum, companies should review and evaluate existing data privacy policies and procedures for PIPL compliance and make necessary updates. Companies should make sure policies and procedures include:

- a notice and consent form for obtaining consent of data subjects (particularly for standalone consent),
- a service contract with third-party data processors (if applicable) and
- a standard contract with overseas data recipients for data cross-border transfer (if applicable).

Companies should be extremely cautious over cross-border data transfer requirements, and if applicable, plan to appoint a designated office or representative within China to be responsible for personal information issues. Further, companies should take technical measures to protect personal information, including corresponding data classification,

encryption and de-identification, and communicate with employees about data privacy compliance policies and provide training on a regular basis.

Failure to comply with PIPL may result in severe administrative penalties, including large fines, and may even expose companies to civil lawsuits by private individuals.

Application of PIPL

While PIPL has similar requirements compared to the General Data Protection Regulation (GDPR), PIPL includes substantive obligations that differ from the GDPR and certain data localization requirements, including its requirements for cross-border data transfers, standalone consent, data protection impact assessment and the appointment of personal information protection officers. The Cyber Administration of China (CAC) has published its Notice of Public Comment on the Measures for Data Overseas Transfers Security Assessment Draft for Solicitation of Comments (Draft CAC Guidelines), which provide more practical guidance for compliance with the overseas data transfer requirements imposed under the PIPL. (The Draft CAC Guidelines are discussed in detail at the end of this law alert.)

For non-Chinese organizations that process personal information of individuals located in China, PIPL applies upon any of the following situations:

- the non-Chinese organization collects or processes personal information for the purpose of providing products or services to natural persons in China;
- the data will be used in analyzing and evaluating the behavior of natural persons in China; or
- under other unspecified circumstances stipulated by laws and administrative regulations.

Personal information is defined very broadly to include "various types of electronic or otherwise recorded information relating to an identified or identifiable natural person," and processing is also defined very broadly to include "the collection, storage, use, refining, transmission, provision, public disclosure or deletion of personal information."

Key PIPL provisions

General requirements

PIPL establishes guiding principles on the protection of personal information. It provides that:

- the processing of personal information should have "clear and reasonable purposes" and should be directly related to those purposes; and
- the processing of personal information must be minimized and should not be excessive.

Any personal information processing entity, or PIPE, must ensure

the security of personal information, including establishing policies and procedures on personal information protection, implementing technological solutions to ensure data security and carrying out risk assessments prior to engaging in certain processing activities.

With some exceptions, the PIPEs may only process personal information after obtaining an individual's informed consent; such informed consent must be made voluntarily and explicitly. Prior to collection of personal information, the PIPEs must disclose the name and contact information for the PIPEs, the purposes for collection and processing of personal information, the method of collection, the categories of personal information collected, the retention period, the individual's rights, and the method and procedures they may use to exercise such rights. Furthermore, this obligation to obtain informed consent is continuous, if the categories of personal information collected, purpose or method of processing changes after the initial collection.

The PIPEs must provide individuals with a convenient method to revoke their consent, and the information collected shall only be kept for the shortest period of time necessary to achieve the original purpose of collection. The PIPEs must further establish a convenient mechanism to accept and handle applications from individuals to exercise their rights, and must explain to the individuals the reasons for any rejections.

Notably, PIPL mandates that standalone consent must be obtained if the PIPEs:

- share personal information with other processing entities;
- publically disclose personal information;
- process sensitive information; or
- transfer personal information overseas.

Although PIPL does not define standalone consent, most practitioners in China believe such consent shall be obtained through a separate affirmative action by data subjects (e.g., a separate signature or clicking of a separate checkbox).

Automated decision-making algorithms

PIPL requires any PIPE that uses computer algorithms to engage in automated decision-making based on an individual's personal information to be transparent and fair in such decision-making, and further prohibits PIPEs from using automated decision-making to engage in unreasonably discriminatory pricing practices. Automated decision-making is defined as the activity of using computer programs to automatically analyze or access personal behaviors, habits, interests or hobbies, of financial, health, credit or other status, and making decisions based thereupon. When an individual's rights are significantly impacted by a PIPE's automated decision-making, that individual can demand that PIPE to explain the decision-making and has right to decline to be subject to automated decision-making.

Specific protections for sensitive personal information

PIPL further affords extra protections over sensitive personal information. Standalone consent must be obtained prior to the processing of such information. In addition, PIPEs may only process sensitive personal information when specific purpose and sufficient necessity have been demonstrated and strict security measures have been implemented. Sensitive personal information is broadly defined as personal information that, once disclosed or used in an illegal manner, could harm the dignity, persons or property of natural persons, including biometrics identification information, religious information, special status, healthcare information, financial account information, location information, and personal information of minors under the age of 14. The meaning of special status is not defined.

Cross-border transfer of personal information

Under PIPL, PIPEs who transfer personal information outside of China may be required to enter into a standard contract (along the lines of a template to be issued by CAC) with overseas data recipients. In addition, PIPEs must obtain standalone consent of data subjects (to the extent that the consent is the lawful basis for the data processing) and conduct the data protection impact assessment (DPIA) prior to the cross-border transfer. The PIPEs seeking to transfer the data must also provide the data subject with information about the foreign recipient, including its name, contact information, purpose and method of the data processing, the categories of personal information provided and a description of the data subject's rights under PIPL.

In addition, for PIPEs that process an amount of personal information that reaches a certain threshold (yet to be released by the CAC), a security assessment administered by the CAC must be passed prior to any cross-border transfer of personal information.

Notably, companies and individuals may not provide personal information stored within China to non-Chinese judicial or enforcement agencies without prior approval of the Chinese government. As of now, it is not clear how PIPEs may seek such approval.

Data protection impact assessment

Similar to the GDPR, PIPL requires the DPIA be conducted when PIPEs engage in automated decision-making and processing sensitive information. PIPEs are required to retain DPIA records for at least three years. However, PIPL further requires PIPEs to conduct the DPIA in the following cases (which are not required under GDPR): cross-border transfer of personal information, engaging a third-party data processor, providing personal information to another PIPE and making personal information publicly available.

Appointment of personal information protection officer

PIPL requires non-Chinese PIPEs to establish a dedicated office or appoint a dedicated representative within China to be responsible for personal information issues.

Administrative penalties

PIPL imposes various penalties for organizations that fail to satisfy their obligations to protect personal information. Upon discovery of any large risks or the occurrence of any personal information security incident, the Chinese government may conduct a talk with the designated representative of the PIPE to order a compliance audit and any remedial measures to be taken. Companies may be subject to fines of no more than 1 million RMB (approximately $154,378.20) if they fail to remediate conduct found to be in violation of the PIPL; responsible individuals may be subject to fines of 10,000 to 100,000 RMB (approximately $1,543.81 to $15,438.05). For grave violations (undefined in PIPL), PIPEs are subject to a fine of up to 50 million RMB (approximately $7,719,027.00) or 5% of annual revenue (it is unclear whether this is revenue in China or global revenue), with responsible individuals subject to fines of 100,000 to 1 million RMB (approximately $15,438.29 to $154,382.93).

Chinese authorities may also order to suspend the offending PIPE's business activities, or cancel its administrative or business licenses.

Private rights of actions

PIPL creates a private cause of action, which allows an aggrieved individual to file lawsuits against PIPEs that rejected the individual's requests to exercise their rights, and/or to report any suspected unlawful activities to the corresponding Chinese authorities to conduct investigations. Additionally, if a PIPE violates rights of a large number of individuals, the People's Procuratorate and other designated organizations may file public interest lawsuits.

Draft CAC Guidelines

As discussed earlier, PIPL mandates the PIPEs to conduct the DPIA when they engage in cross-border transfer of personal information. The Draft CAC Guidelines, while still in draft form, provide more clarifications as to how the DPIA should be conducted.

Under the Draft CAC Guidelines, the PIPEs must conduct a DPIA when:

- the organization is a critical information infrastructure operator (CIIO) collecting personal information and important data;
- the transferred data includes important data;
- the organization is processing data of over 1 million data subjects and intends to transfer data overseas;
- the accumulated overseas transfer amount of personal information exceeds 100,000 data subjects or sensitive personal information

exceeds 10,000 data subjects; or

- where otherwise required by the national CAC.

The DPIA first involves a self-assessment by the PIPE, which upon completion will need to be submitted to and approved by the local CAC branches. The Draft CAC Guidelines set out the scope, procedure and timescales for such process. It is important to note that the Draft CAC Guidelines mandate the submission of a copy of the data processing agreement with the overseas data recipient. In addition, the approval will need to be renewed every two years, or if the scope of the processing changes.

While the Draft CAC Guidelines provide certain clarifications, many questions remain unanswered, such as whether the DPIA is required for internal data transfers or remote access from overseas, or whether the DPIA would be required if the PIPEs process data exceeding the threshold in a single transfer or cumulative transfers.

The comment period for the Draft CAC Guidelines ends Nov. 28, 2021. As the Draft CAC Guidelines are the subject of heavy lobbying right now, we are hopeful to see more clarifications when the second draft is released.

International Business & Trade attorney Sunny Yang represents Chinese entities doing business in the U.S. and U.S. entities pursing investments and operating in China. For more information about PIPL compliance, please contact her directly or reach out to any member of Porter Wright's International Business & Trade practice.