SQUIRE PATTON BOGGS

China's Personal Information Protection Law

What It Means to Companies

Asia Pacific – May 2021

On October 21, 2020, the People's Republic of China issued a new draft Personal Information Protection Law (PIPL). As the time allotted for the public to comment on the draft PIPL closed in November 2020 and a new draft was submitted to the legislators for review in early March 2021, we do not expect to wait very long for the draft to be passed into law.

At this stage, it is unclear whether the text of the PIPL will be adopted in its originally proposed form, or if significant changes have been included in the new draft in response to comments received from industry and other parties. We review the key provisions of the original, published draft of the PIPL, with a focus on the practical impact on companies doing business in China.

We note that as with many new data protection laws around the world, much of the PIPL's detail will need to be fleshed out in implementing regulations.

Note: References to "China" refer to Mainland China, where the rules directly apply. Notably, Hong Kong remains governed by its own set of data privacy laws.

Background

After focusing on protecting national security-related data in the Cybersecurity Law of 2017 (CSL), the government has proposed the far-reaching PIPL in order to provide greater protections for consumer data and create a data privacy regime that is more in line with the EU's General Data Protection Regulation (GDPR), but with some important distinctions.

In the past, China did not have a singular, comprehensive law dealing with data privacy. Although the CSL requires organizations to reasonably protect all personal information collected in China, its primary focus is to place stringent obligations, including data localization requirements, on personal information relating to "Critical Information Infrastructure" (quite broadly defined). After enacting the CSL, China passed various implementing guidelines and rules, and also published a series of draft implementation obligations involving personal information, such as the draft Security Assessment Measures on the Cross-Border Transfer of Personal Information (published in June 2019), which has yet to pass. It is unclear how the PIPL will interact and correlate with the CSL rules and subsequent guidelines.

PIPL Highlights

Territorial Scope of the PIPL

By contrast with the CSL, which governs entities in China that collect personal information, the draft PIPL applies to not only the processing of personal information within China, but also the extraterritorial processing of the personal information of natural persons within the territory of China under certain circumstances. Like the GDPR, the extraterritorial scope of the PIPL extends to such information if it is processed outside of China for the purpose of (1) providing products or services to natural persons within China, or (2) analyzing and evaluating the activities of people within China. The PIPL, however, is broader in scope insofar as it also allows for the extraterritorial application if "otherwise required by law."

Echoing the GDPR, overseas processors of personal information that fall within the extraterritorial scope of the PIPL must establish "special institutions or designated representatives" within the territory of China to deal with PIPL matters on behalf of the overseas entity.

Key Definitions

As is the case under the GDPR, the PIPL's definition of Personal Information (PI) is quite broad, but excludes anonymized data. The PIPL incorporates the fair processing principles found in the GDPR, including lawfulness, fairness and transparency; purpose limitation; data minimization; data accuracy; storage limitation; and data integrity.

The principal obligations prescribed by the draft PIPL fall on "Personal Information Processors" (PIPs), which the PIPL defines as "organizations or individuals that independently make decisions on personal information processing matters such as the purpose and measures of processing." This term appears to correlate with the GDPR's "data controller" definition.

The PIPL includes the concept of joint PIPs (similar to the GDPR "joint controller" concept), and requires such entities to enter into joint PIP agreements setting out the parties' respective rights and obligations. The PIPL provides that joint PIPs bear joint and several liability for any infringement of an individual's rights in regard to their PI.

The PIPL also makes reference to "entrusted party" (though the term is not specifically defined), which by application seems similar to the GDPR's concept of "data processors." Requirements related to entrusted parties are discussed below.

Bases for Processing PI

Like the GDPR, the PIPL requires there to be a lawful basis for processing PI. Under the PIPL, the processing of ordinary (non-sensitive) PI may be carried out with one of the following:

- With the individual's consent
- If necessary for the conclusion or performance of a contract
- If necessary for the performance of legally prescribed duties or obligations
- If necessary to respond to public health incidents or other public emergencies
- For news reporting and public opinion oversight in the public interest
- As otherwise permitted by law or regulations

By contrast with the GDPR, the draft PIPL does not authorize the processing of PI based on the legitimate interest of the PIP or a third party, balanced against the rights and interests of the individual. Nonetheless, it is helpful that the draft PIPL now specifies a number of lawful bases for processing PI beyond consent.

If consent is the basis for processing PI, such consent must be a clear and voluntary declaration of intent under the premise of full knowledge of the individual and capable of being withdrawn. PIPs may not refuse to provide products or services if an individual declines to consent or withdraws their consent, unless the processing of such data is necessary for the provision of the services. In regard to individuals who the PIP knows, or should know, are minors under the age of 14, the PIP is required to obtain the consent of the individuals' guardians.

Sensitive PI

Special rules apply to the processing of sensitive PI, which is broadly defined to include "information that once leaked or illegally used may cause individuals to suffer discrimination or serious harm." The definition of sensitive PI expressly includes PI concerning race, ethnicity, religious beliefs, personal biological characteristics, medical health, financial accounts or personal location. In addition, the consent for the sensitive PI must be "separate" – that is, a separate consent only relating to the sensitive PI to be collected or processed. For example, it may not be "bundled" into a consent to non-sensitive PI or a privacy policy covering multiple distinct processing activities.

Privacy Notice Required

Prior to the processing of data, the PIP must provide a privacy notice that contains, at a minimum, the PIP's contact information, the purpose of the processing, the categories of personal information that will be processed, the need to process sensitive PI, the retention periods and the method/procedure for individuals to exercise their rights. The notification must be made easily accessible to the public and capable of being downloaded. The notice requirements are similar to those required in the CSL, as well as the GDPR.

Data Subject Rights and PIP Obligations

The PIPL contains a set of data subject rights that are similar to those found in the GDPR (access, correction, deletion, etc.). Individuals also have the right to request the PIP to explain any automated decision-making where the individual believes that such processing has had a significant impact on the individual's rights and interests, and they may also object to any decisions based solely on automated processing.

Similar to the GDPR, the PIP is under an obligation to only retain the data as long as it is necessary for achieving the purpose of processing. However, the PIPL also obligates the PIP to delete on its own initiative or at the request of the individual where:

I. The agreed storage period has expired or the purpose of processing has been achieved

II. The PIP stops providing products or services

III. The individual withdraws consent

IV. The PIP processes in violation of the agreement, laws or regulations

V. There are other circumstances as prescribed by law and administrative regulations

PIPs are required to take "necessary measures" to ensure compliance with the PIPL, including having in place management/operational procedures, data classifications, technical security measures, protecting against unauthorized access, training for employees and implementing an incident response plan. Regular audits are required and risk assessments are required in specified circumstances, including for processing of sensitive PI, processing that involves automated decision-making, data sharing with third parties, transferring PI abroad, or activities that could have a major impact on the individual.

PIPs must keep records (in a designated format) of processing involving sensitive personal information or that which may have a significant impact on individuals, automated decision-making, third-party processing and cross-border data transfers. Such records must be retained for three years. PIPs processing specified volumes (still to be defined) of PI must appoint a person in charge of personal information protection who is responsible for supervising processing the PI and the adopted protection measures. The PIP must make public, and provide to the relevant administrative authority, the name and contact information of the individual.

Transfers to "Entrusted Parties" and "Third Parties"

Transfers to entrusted parties (which appear to be similar to "data processors" under the GDPR) must process PI in accordance with an agreement with the PIP that establishes the purposes and methods of the "entrusted processing," the categories of data to be processed, security measures, etc. The entrusted party must process the data within the scope of the agreed methods and purposes, must return or delete the PI when the contract terminates, and may not share the entrusted PI with any other party without the consent of the PIP.

For transfers to third parties (presumably other PIPs that are not acting as "entrusted parties," though the term "third party" is not defined), the PIP must notify the individuals whose data will be transferred of the identity of the third party, along with their contact details, the categories of data to be transferred and the purposes and methods of the processing. In addition, the PIP must obtain the individual's separate consent to the transfer. The third party must process the information in accordance with the specified purposes, or must obtain the individual's consent to change the original purpose of the processing/transfer. If anonymous PI is transferred to a third party, the third party must not re-identify the data.

Cross-border Transfers

Cross-border transfers of PI may only be made with the consent of the individual after the PIP provides notice of the overseas recipient's identity, contact details, the purpose and method of processing, the types of PI to be transferred and the process for exercising the data subject's rights against the overseas recipient. In addition, the PIP must have complied with at least one of the following:

- Passed the government security assessment organized by the responsible state authorities
- Obtained a certification from a professional body in line with the requirements of the responsible state authorities
- Concluded a contract with the overseas recipient to ensure the recipient's processing meets the personal information protection standards specified by the PIPL
- Satisfied other conditions for international transfers prescribed by China state laws or regulations

It is interesting to note that the PIPL seems to soften the cross-border transfer requirements contained in the draft Measures for Security Assessment for Cross-Border Transfer of Personal Information of 13 June 2019 issued for public comment. Under that draft, government approval, submission of the contract and risk assessment/reporting were all to be mandatory. Although text of the draft PIPL seems to suggest a somewhat lighter approval mechanism, the June 2019 draft rules provide important insights on the methodology and format for seeking approval and conducting risk assessments.

Note: PI transferred by Critical Information Infrastructure Operators under the CSL and PIPs that process large volumes of data (to be determined by the responsible state authorities) will remain governed by the CSL, which generally requires localization of the data in China unless specifically approved by the government for export following a security assessment.

Under the PIPL, it is important to note that PI may not be transferred overseas to law enforcement or for legal defense purposes without approvals from the relevant government departments in China.

The government may block or restrict data transfers to a particular overseas recipient, if its processing of PI harms the PI rights of Chinese citizens or endangers national security. Furthermore, the government may take reciprocal action against any country that adopts discriminatory restrictions or similar measures against the transfer of personal data to China.

Breach Notification

In the event of a data breach, the PIP shall "immediately" take remedial measures and inform the authorities and the individuals concerned with the information specified in the PIPL. PIPs do not have to notify individuals of a breach if the PIP has "taken measures to effectively avoid damage caused by the information leakage." However, the authorities may still require PIPs to notify affected individuals if they believe they could be harmed.

State Security Provisions

A PIP may not process data in violation of the laws and administrative regulations, nor endanger the national security or the public interest. Image capturing in public places may only be done to maintain public security and only with conspicuous notices. Individuals are not to be notified of a transfer to China state authorities if specified by the law.

Penalties

The responsible authorities (including the State Cyberspace Administration, the relevant departments under the State Council and the relevant departments of the local government) would have broad investigation and information gathering powers, including on-site inspections and the authority to interview the person(s) locally in charge of the PIP. Complaints alleging the unlawful processing of PI may be submitted by organizations and individuals to the responsible departments, which must publish contact information for the receipt of complaints and reports.

The relevant departments may order remedial measures, confiscate illegal gains or give warnings, and where such orders are not complied with, penalties of up to 1 million Yuan (approximately US$150,000) may be imposed on the PIP, with lesser penalties payable by the responsible individuals within the organization. However, if the illegal act leads to serious circumstances (yet to be defined), the penalty may be up to 50 million Yuan (approximately US$7.5 million) or 5% of the prior year's turnover (note: it remains unclear whether this is global or China turnover), suspension of the relevant operations or business and/or revocation of the business license, and individual fines of up to 1 million Yuan (approximately US$150,000) for those individuals responsible within the organization. In addition, compensation may be awarded to individuals who have been harmed and referred to the courts where the losses suffered, or unlawful benefits gained, are difficult to determine. Criminal liability may be imposed where an infringement constitutes a violation of public security.

Recommended Steps Pending Further Legislative Action

It is impossible to predict whether the draft PIPL will be modified in significant ways prior to final enactment. Nonetheless, because it is unclear whether a transition period will be included in the final version of the law, there are several steps that can and should be taken now by PIPs operating in China, and by overseas companies processing the PI of residents of China in ways that may trigger the law's extraterritorial application.

Key steps include:

- Carrying out a data inventory and mapping exercise
- Identifying any transfers of PI and sensitive PI
- Assessing the purposes and lawful bases for the processing of PI
- Identifying relevant "entrusted processors" and "third parties" and preparing draft agreements and conditions for transfer to same
- Evaluating cost, technical and timing issues related to the potential obligation to site some or all data processing activities in China
- Preparing template privacy notices
- Preparing template international data transfer agreements, including intra-group agreements

How We Can Help

Our Data Privacy & Cybersecurity team has established an internal working group comprising GDPR, US, Asia Pacific and China-based data privacy experts who have substantial experience advising on the CSL and other relevant regulations in China. Collectively, our experience advising clients on compliance with key data protection laws around the world will enable us to provide holistic advice on the PIPL that takes into account the Chinese legal framework together with important international precedents.

Your PIPL Advisory Team

Nicholas Chan
Partner, Hong Kong
T +852 2103 0388
E nick.chan@squirepb.com

Scott Warren
Partner, Japan/China
T +81 3 5774 1813
E scott.warren@squirepb.com

Lindsay Zhu
Partner, Shanghai, China
T +86 21 6103 6303
E lindsay.zhu@squirepb.com

Transnational Support

Rosa Barcelo
Partner, Brussels, Belgium
T +322 627 1107
E rosa.barcelo@squirepb.com

Alan Friel
Partner, Los Angeles, California
T +1 213 689 6518
E alan.friel@squirepb.com

Ann LaFrance
Senior Partner, New York
T +1 212 872 9830
E ann.lafrance@squirepb.com