China issues draft Personal Information Protection Law for consultation

November 2020

Introduction

On 21 October 2020, China’s top legislative body issued the draft Personal Information Protection Law ("Draft PIPL") for public consultation. This indicates a major step towards finalising China’s national data law.

The Draft PIPL lays down significant new obligations in relation to collection, use, processing and transfer of personal information. The PIPL, together with the China Cybersecurity Law and the Data Security Law (the draft of which was issued for public consultation earlier in 2020) will constitute the cornerstones for building up China’s legal regime for data sovereignty, personal data protection and cybersecurity. If enacted, the PIPL will become China’s most comprehensive data law and will have a far-reaching impact on businesses in China as well as outside China.

This briefing highlights the key provisions of the Draft PIPL and discusses the significant implications the PIPL may have for businesses.

Key provisions of the Draft PIPL

The draft PIPL contains eight chapters and 70 sections. The following provisions are worth noting:

<table>
<thead>
<tr>
<th>Provision</th>
<th>Explanation</th>
</tr>
</thead>
</table>
| Processing of personal information | • The Draft PIPL sets out the principles of legality, appropriateness, accuracy, transparency, use minimization and good faith for data processing.  
• The Draft PIPL does contain a structure of data processor and entrusted party, which is similar to data controller and data processor under the European General Data Protection Regulations (GDPR), although the language described in the Draft PIPL may cause some confusion to those who are more used to the GDPR. Under the Draft PIPL, “Personal Information Processing” is defined broadly to cover collection, storage, use, processing, transmission, provisions, disclosure and other activities relating to personal information and “Personal Information Processor” refers to those who can independently determine the purpose and means of the processing of personal information. |
| Extra-territorial application   | • The Draft PIPL seems to be modelled on the GDPR in relation to its extraterritorial reach. The Draft PIPL will apply to data processing OUTSIDE China if such data processing activity is for the purposes of providing products or services to Chinese individuals or for analysing or evaluating the behaviours of individuals in China.  
• Data processors outside China are required to set up a specialised agency or appoint a representative in China to take responsibility for handling matters in relation to personal information protection. It is not clear at this stage what enforcement actions Chinese authorities will take in exercising this extraterritorial power specially when a violator is a foreign entity with no presence in China. |
Legal basis for processing and exemptions for consent

- The Draft PIPL provides for six kinds of legal basis for processing personal data:
  - consent by data subjects;
  - essential for entering into or performing contracts;
  - essential for performing statutory responsibility;
  - essential for responding to public health emergencies or for protecting life, health or property safety under emergency situations;
  - publication of news and supervision of public opinion for public interest; or
  - other circumstances as permitted by laws and regulations.

- The above legal basis appears to be a major development from the China Cybersecurity Law, which provides that data collection and use must be based on consent from data subjects and does not contain any express exemptions from the consent requirement, which has generated quite some debate in the industry on whether such a rigid consent requirement is workable in practice.

- Efforts to build some flexibilities into the consent requirement have been reflected in a few subsequent regulations, for example:
  - the Personal Information Security Specification, a non-binding industry specification which provides that a network operator can collect and use personal information without consent for execution of contract or for national security, public interest and criminal investigation, or for protecting the data subject’s life or important property; and
  - the Civil Code of China, which provides that consent from data subjects is not required if (i) data processing is for protecting public interest or the data subject’s legitimate right; or (ii) the personal information of the data subject is already publicly available, unless the data subject expressly objects to such data processing.

- The scope of permissible exemptions set out in the Draft PIPL is wider than the Civil Code but narrower than the Personal Information Security Specification and this appears to imply that Chinese law makers are trying hard to strike a balance between the protection of personal data and the business efficiency for the industry. Whether and how the exemption scope will be changed in the final version of the PIPL remains to be seen.

New developments on consent requirement

- Where consent is necessary, the Draft PIPL provides that valid consent must be freely given, unambiguous and the data subject who gives the consent must be fully informed.
- This appears to mirror the GDPR, which defines consent in Article 4(11) as “any freely given, specific, informed and unambiguous indication of the data subject’s wishes by which he or she, by a statement or by clear affirmative action, signifies agreement to the processing of personal data relating to him or her.”

Sensitive personal information

- Under the Draft PIPL, a higher regulatory requirement is imposed on data processors when handling sensitive personal information such as race, nationality, religious belief, biometric information, medical history, health information, financial account information and geological information.
- The Draft PIPL requires a specific purpose and sufficient necessity for processing sensitive personal information. Separate consent is required before collecting sensitive personal information and data processors must conduct a risk assessment before processing sensitive personal information.

Cross-border data transfer

- Under the Draft PIPL, where data processors need to transfer personal information abroad due to business necessity, they must satisfy one of the following conditions:
  - if the data processor is categorised as a critical information infrastructure operator or processes personal information exceeding the volume prescribed by Chinese cyberspace regulators, the data process is required to pass a security assessment before the transfer, unless otherwise required under applicable laws and regulations; or
  - where a data processor does not fall into the category above, it may either arrange for the cross-border data transfer to be certified by a professional institution, or enter into an agreement with the foreign data recipient for the purposes of specifying the rights and obligations of the parties and monitoring the data recipient located outside China to ensure that the processing meets the protection standard as required under the Draft PIPL.
- The Draft PIPL provides that certain retaliation measures can be taken against foreign organisations or individuals who have damaged Chinese citizens’ personal data rights or against foreign countries that have imposed unreasonable sanctions against China in relation to personal information protection.
### Automated decision-making

- Nowadays, user profiling and automated decision-making have been used widely in business scenarios, for efficiency and convenience. But the deployment of these technologies can bring privacy concerns because personal data can be abused.
- The Draft PIPL tries to strike a proper balance on the use of technologies and protection of personal data. It is provided in the Draft PIPL that data processors must guarantee the transparency of the automated decision-making and the fairness of the results. The data subject concerned has the right to require the data processor to provide an explanation and/or refuse automated decision-making, if his/her rights and interests are materially impacted by the automated decision-making.
- The Draft PIPL further requires that if an automated decision-making process is used for marketing or information push delivery to data subjects, data processors are required to offer data subjects an option to not target their personal characteristics.

### Penalties and liabilities

- One of the most eye-catching provisions in the Draft PIPL is the augmented enforcement against non-compliance. Companies found to be in violation of the legal requirements under the Draft Law will be subject to administrative fines of up to RMB50 million (approximately USD7.6 million) or 5% annual turnover of the preceding year plus civil compensation; any directly responsible individuals within such companies could be administratively fined up to RMB 1 million (approximately USD152,000).
- The Draft PIPL also states that Chinese regulators will adopt a blacklist system, where organisations or individuals found to have damaged the rights of Chinese citizens or harmed the national security or public interest of China will be put on a blacklist and made public.

### Implications for businesses

In the era of big data, data has become a strategic asset for many businesses and it presents huge opportunities as well as compliance challenges for international and Chinese companies. China’s data regime has been evolving at an extremely quick pace as demonstrated by the issuance of multiple important laws in the data and cybersecurity space in recent years. Upon implementation, the PIPL will become a significant legislative piece and will have profound and far-reaching impacts on international and Chinese businesses in all industries.

Many companies already process huge amounts of private data and the volume may continue to grow exponentially. Identifying personal data across on-premises, cloud or hybrid IT environments, and enforcing security policies based on data type, is very challenging. In order to meet privacy and compliance requirements with less effort and expense, many organisations now widely adopt technology solutions such as the following:

- Applying privacy identification rules by using regular expressions, proximity of text and algorithms through automation tools, and applying custom tags, flags, and notes to datasets that are accessible in the UI, reports, or via API.
- Automatically quarantining critical or sensitive data stored in unsecure locations or accessible by large groups of users to minimise its exposure until the company can make a thoughtful remediation decision.
- Integrating privacy tools into a more comprehensive data security platform. These solutions should be able to provide additional behaviour reporting, and continuous auditing and monitoring for easier data management.
- Cleaning privacy information through data sanitisation tools and removing unnecessary data permanently.

The Draft PIPL introduces significant new obligations for companies to comply with in their business operations and the augmented liability and penalty provisions in the Draft PIPL clearly demonstrate Chinese authorities’ intention to strengthen the protection of personal data. It is anticipated that Chinese regulators will stay active in enforcing the law against non-compliance. The violation cost is hugely lifted compared with what is provided in previous laws and regulations and it is imperative that companies should formulate or update their data compliance and risk management strategies for the China market.

It is interesting to note that a considerable number of stipulations in the Draft PIPL share commonalities with the GDPR. This helps to bring the PIPL in alignment with international practice. This is obviously a positive move for international companies, especially those which are familiar with the GDPR.

The deadline for submitting comments on the Draft PIPL is 19 November 2020. It is anticipated that Chinese authorities will fast track the finalisation of the PIPL. Companies are strongly advised to keep a close watch on the legislative development and get ready in anticipation for the issuance and implementation of the PIPL in the near future.
Let's talk

For a deeper discussion of how this impacts your business, please contact:

**Rui Bai Law Firm**

Barbara Li
Head of Corporate
TMT and Data Practice Lead
+86 10 8540 4686
barbara.xb.li@ruibailaw.com
WeChat: Barbara_Lawyer

**PwC China**

Lisa Li
Partner
Cyber Security
+86 10 6533 2312
lisa.ra.li@cn.pwc.com
WeChat: lisatsai

The information contained in this article is of a general nature only. It is not meant to be comprehensive and does not constitute the rendering of professional advice or service by PwC or Rui Bai Law Firm. PwC or Rui Bai Law Firm has no obligation to update the information as law and practices change. The application and impact of laws can vary widely based on the specific facts involved. Before taking any action, please ensure that you obtain advice specific to your circumstances from your usual PwC or Rui Bai Law Firm client service team or your other advisers. The materials contained in this article were assembled in November 2020 and were based on the law enforceable and information available at that time.

© 2020 PwC. All rights reserved. PwC refers to the PwC network and/or one or more of its firms, each of which is a separate legal entity. Rui Bai Law Firm is an independent law firm and a member of the PwC global network of firms. Please see www.pwc.com/structure for further details.