China's new Data Privacy Law – what does it mean for you?

October 2021

Data privacy laws in China has traditionally been fragmented, but efforts to consolidate those various regulations have intensified in recent years – culminating in the National People Congress passing the Personal Information Protection Law (**"PIPL"**) on 20 August 2021. The PIPL will become effective on 1 November 2021.

The PIPL is a substantial and significant new legislation – and it will pose significant challenges to many companies' personal data practices, both in relation to its complexity and in adding another new law to many multinational organisations' international compliance efforts.

What does the PIPL mean for you? Following on from our previous article about the draft PIPL, we set out below what you need to know and do about the PIPL.

Introduction and summary

China has historically had a patchwork of different laws (both in effect and in draft (but influential) form) containing different data protection requirements. The PIPL is China's first comprehensive law on personal data protection, and together with the Cyber Security Law (**"CSL"**) and the Data Security Law (**"DSL"**), represents China's foremost legislative efforts for regulating its digital economy. It also draws extensively from (but does not duplicate) the European Union's General Data Protection Regulation.

In short – the PIPL will significantly increase the data protection requirements in China, with a particular focus on:

- Using consent as the primary basis for data processing – and noting that, unlike the GDPR and despite various lobbying efforts, "legitimate interest" has not been included as a basis for data processing.
- Extraterritorial application and effect - on overseas processing of personal data of China-based individuals.
- Introducing significantly increased fines for breaches.
- Expectation that data controllers (i.e. data processor – see explanation below) will implement company-wide policies and procedures for data protection practices, with accompanying effect on areas such as consent management and international data transfers.

Given the short timeframe for implementation and our expectation that the Cyberspace Administration of China will issue further implementing measures and guidelines for the PIPL (including the standard contractual clauses for cross-border data transfer), it will be difficult to implement "fully compliant" solutions by 1 November 2021 – but there are various steps that can be taken right now by organisations looking to comply with the PIPL as part of its international data privacy compliance efforts.

What is a "data controller"?

At the outset, it's important to remember the following differences in PIPL terminology with various other data protection laws:

- **"Data processor"** – means the party who controls and determines the purpose and method of the data processing (i.e. "data controller" under the GDPR and various other data protection laws).
- **"Entrusted party"** – means the party processing data on behalf of and at the instruction of the data processor (i.e. "data processor" under the GDPR and various other data protection laws).

We will use the above terms in the remainder of this article – these are important differences when interpreting the PIPL.

Extraterritorial application

China's data protection-related laws have historically focused on activities within China.

A significant expansion under the PIPL is that while it focuses on data processing activities within China, it also has extraterritorial effect – specifically, it applies to the processing of PRC residents' personal data outside PRC:

- for the purposes of providing services or products to PRC residents;
- to analyse or assess behaviour of PRC residents; or
- for any other reasons as required by law.

It is not clear at this stage how any extraterritorial application of data privacy laws would occur in practice.

What are the bases for processing personal data?

The PIPL remains focused on express notice and consent as the primary basis for processing personal information. One of its biggest distinctions with the GDPR (and other jurisdictions) is that **there is no "legitimate interest" basis for processing and no explicit recognition of deemed or implied consent** – despite various international lobbying efforts. International data privacy trends is increasingly moving away from consent as the primary basis for processing personal data, so this is a surprising development in some ways.

Having said that, the PIPL provides other bases for processing personal data that, collectively, align with international standards:

- concluding or performing a contract with a data subject;
- carrying out human resources management in accordance with legally established employment policy or a collective contract (this was added in the final draft of the PIPL, and may await further clarification from authorities, e.g. whether such base is subject to the circumstances that request a separate consent);
- complying with applicable laws;

- necessary for responding to public health emergencies or to protect natural person's lives and health, or their property in an emergency;
- conducting news reporting, public opinion supervision, and other such activities for the public interests within a "reasonable scope";
- use of publicly available information within a "reasonable scope"; and
- as otherwise set out by laws and regulations.

In addition, there is a requirement for notification (rather than consent) where personal data is transferred for mergers, division, dissolution, and bankruptcy.

Any consent issued may be revoked, subject to not impacting on data processing that took place prior to the revocation. Data processors may not refuse provide products or services if the data subjects withhold or withdraw their consent to non-essential processing.

What about separate or unbundled consent?

Design of consent mechanisms is a constantly evolving area that is of key interest to companies – both in terms of legal compliance and customer-relationship management (e.g. UX design).

A key (and to be monitored) aspect of the PIPL is that it requires separate / unbundled consent for the following activities:

- transfer of personal data by data processor to third parties;
- publication of personal data;
- use personal data collected by equipment installed in the public places for security purposes, such as personal images, for purposes other than public security;
- processing of sensitive personal data; and
- cross-border transfers of personal data.

It is not clear at present what a "separate / unbundled" consent means in practice. Does it mean that consent requires a separate acknowledgement or checkbox in writing to be made? That would be particularly difficult to achieve for digital economy companies. Also, can consent be procured on an "opt out" basis or does it have to be "opt in"? Any company in the digital economy would be keenly interested in these questions (both in China and elsewhere), given the commercial focus on ensuring as little "friction" as possible in procuring consent. This is an area that we will continue to monitor for regulatory and market practice guidance.

Will we need to keep personal information in China?

China has had different draft laws and standards that applied to cross-border transfer of personal information. Many of you will note that the CSL mandated localisation of "personal data" and "important data" (i.e. data that raises national security/strategic issues to the China government), applying to "operators of critical information infrastructure" (but with draft implementing measures indicating that it may apply to "network operators" as well). For example, the CAC has issued rules requiring automakers to store drivers' data in China.

The PIPL aims to create a standard applying to all such activities, in the following manner:

- Critical information infrastructure operators are required to localize personal data in China, save except it has been approved for necessary international transfer.
- data processors handling personal data exceeding to-be-confirmed thresholds are also required to localise their personal data in China. We will continue to monitor for when these thresholds are published.
- As above, data subjects are required to provide a "separate consent" for international transfers. In addition, any international transfer must comply with one of the following:
    - a personal information risk assessment on such transfer has been taken by CAC;
    - a personal information protection certification via a certification body accredited by the CAC has been obtained; or
    - a contract (in the form of standard contract released by CAC) with the offshore data recipient has been signed, satisfying relevant requirements in and ensuing offshore processing of Personal Data complies with the PIPL.
- Data processors transferring personal data offshore will need to take "necessary measures" to ensure the recipient's activities comply with the standard under the PIPL.

In practice, the above means that if consent is withdrawn by or not procured from the data subject, the data processor will need to have local data processing arrangements in place.

Finally, we note that the PIPL requires prior approval from a "competent Chinese authority", before any personal information in China can be provided to a "foreign judicial or law enforcement agency". Neither of the quoted terms has yet been defined, and this may cause issues to foreign companies subject to overseas regulators.

Mandatory data breach notification

Data processors are required to take remedial measures and notify relevant competent authorities and impacted individuals of any data breach incidents – whether actual or potential. The notification's content includes:

- the type of information that has been leaked;
- cause of the data breach, and possible harms caused by the data breach;
- remedial measures taken by the data processor and mitigation measures that can be taken by the data subject; and
- how to contact the data processor.

However, data processors will not be required to notify breaches to individuals if remedial measures may be taken without harm being caused to individuals, unless required otherwise by authorities.

Also, under the PIPL (and unlike the GDPR or other data breach requirements globally), there is no materiality threshold or specific notification period for notifications –

Increasingly, data breach notifications are managed on a multi-jurisdictional basis. Without regulatory guidance, it is difficult to interpret how the China requirements would align with overseas requirements in the event of any multinational data breach. We await further regulatory guidance regarding this; in the meantime, we continue to advocate best and responsible practices for companies in dealing with any data breach, in managing and balancing legal, commercial and reputational risks.

Other points to note

The PIPL contains other points that are worth noting:

- **Significantly increased monetary fines and penalties.** The PIPL introduces fines of up to RMB50,000,000 or 5% of the company's annual turnover of the preceding year (note that it is not clear how this is defined). In addition, individuals materially breaching the PIPL may face fines of RMB10,000 to RMB1,000,000 and may be disqualified from acting as director, supervisor, executive manager, or data protection officer of the relevant company.
- **Security measures.** Personal information must be kept confidential, and security measures to be adopted in accordance with the technical standards as required under the CSL and DSL. Technical standards published by the PRC regulators should be closely reviewed in this regard – e.g. from the National Information Security Standardisation Technical Committee of China and any sector-specific regulators, such as the People's Bank of China for financial services. Generally, the following general security measures for personal data are required:
    - implementing internal management structures and operating rules;
    - undertaking data classification exercises;
    - adopting security measures (e.g., de-identification or encryption) to safeguard the personal data they process;
    - regularly conduct security education and training for employees;
    - formulate and implement security incident response plans; and
    - other measures specified by law.

  In addition, before a data processor can conduct high risk activities (e.g. processing sensitive personal data or cross-border transfer of personal data), it shall carry out personal information protection impact assessments.
- **Data portability.** Under the PIPL, data subjects may obtain their information held by data processors, and request that it be transferred for their own purposes. We note that this will likely be subject to further regulatory guidance.
- **Regulation of sensitive personal data –** the definition of "sensitive personal data" is open ended and references the data subject potentially suffering harm to dignity and personal or property security if such data is leaked or used illegally. There is an indicative list included in the PIPL, including biometric, religious beliefs and medical health information. Processing of sensitive personal data has the following additional requirements:
    - only permitted for a specific purpose and sufficient necessity to do so, and strict protection measures are taken;
    - data subject has been informed of such processing including the necessity of such processing and impact on data subject's rights and interests;
    - personal information protection impact assessment is undertaken prior to such processing; and

- separate/unbundled consent is obtained from the data subject.

- **Use of entrusted party.** The PIPL requires entrusted parties to be engaged using an agreement for the processing, including the purpose, method of handling, time limit of processing, personal data categories being processed and relevant security measures. The original data processor is also required to supervise the processing of the entrusted party.
- **Accountability –** influenced by the GDPR, the PIPL requires various accountability measures, including adopting security measures, training and implementing security incident responses.
- **Platform operators**. There is a strong regulatory focus on platform operators in China at present. The PIPL contains special obligations on data processors having "complex business models" and who operate "critical" internet platform services serving "massive" number of users (note that such terms have not yet been defined), and these track closely with the "gatekeeper" obligation for platform operators under the EU's Digital Market Act and Digital Services Act:
  - establish and implement compliance frameworks for personal information protection;
  - establish an independent body to supervise compliance;
  - decline to provide (or terminate provision of) services to third parties on platform that breach personal data-related laws; and
  - regularly publish social responsibility reports.
- **Automated decision making.** The PIPL has provisions regarding the use of personal information for such matter, including:
  - any such decision-making will be non-discriminatory;
  - provide data subjects with information to ensure their understanding of such decision making where it significantly impacts their rights and interests; and
  - for such decision making per above point, ensure that such decisions are not made by purely automated basis.
- **Small businesses**. The PIPL has a concept of "small personal information processors", designed to address the regulatory compliance (and cost) concerns of smaller processors – but note that no further guidance has been provided under the PIPL regarding how any exemptions/different regulatory requirements will apply.

Conclusion and next steps

The PIPL brings significant compliance challenges, particularly given the short timeframe.

In practice, how an organisation will comply with the PIPL is likely to differ on an organisation-to-organisation basis, including with reference to any further sector-specific regulations that may apply. We are currently helping a number of clients with their PIPL compliance efforts – and we recommend the following steps are taken as a first step towards compliance:

- Mapping the personal data that an organisation collects, and how they are collected, used, stored and transferred (as well as retained and deleted).
- Identifying appropriate lawful bases for data processing activities.
- Reviewing current practices and policies for personal data handling – including privacy policy, data retention policy, cross border transfer protocols, engagement of third party suppliers and data breach policies.
- Reviewing consent collection requirements and processes.
- Reviewing cross-border data flows and storage.
- Ongoing conducting of personal data protection impact assessments, and ensuring appropriate records of data processing activities are maintained.
- Ensuring that data subject requests are appropriately dealt with.
- Appointing a data protection officer and (for overseas data processors covered by the PIPL extraterritorial application) representative in China.
- Ensuring additional obligations are met for large platform operators.

We note that some of the above processes can be aligned closely with an organisation's international practices, but will also need to be reviewed in line with the DSL, CSL and other relevant requirements.

In a broader context, the PIPL marks a significant milestone for data protection in China. It is also a continuation of the China government's efforts to regulate the digital economy sector. On the same day that the PIPL was passed, the state media outlet People's Court Daily published an op-ed regarding the PIPL, calling for entities that use algorithms for "personalized decision making" — such as recommendation engines — to obtain user consent first. According to newly issued industry guidelines entitled "Automated Intelligence Ethics Guidelines" dated 25 Sep 2021, service providers should expressly inform users where AI technology is used, specify the functions and limitations of the AI products and services and provide easy solutions for users to opt out of the AI facilitated services so as to protect the privacy of users. Such guidelines are not given the status of law but are considered best industry practice and will likely have de facto binding effect if the regulators seek to proactively enforce, which will expand the scope of "consent". Organisations that use the AI technology to serve the clients shall closely monitor this space for further developments.

As both China and the world contemplate how to regulate the Internet, digital economy and the data flow – we expect the regulators in China to issue significant regulatory guidance that will affect how the PIPL is interpreted and enforced. We will continue to closely monitor this space for further developments.

With thanks to Yeqi Fei (Junior Associate, Beijing) for her review of this article.

Contacts

Hoi Tak Leung
Counsel, Digital Economy

T +852 2846 8982
hoitak.leung@ashurst.com

Patrick Phua
Practice Head, Asia,
Global Loans and Global Markets

T +852 2846 8989 \ +86 10 5936 2888
patrick.phua@ashurst.com

Joshua Cole
Practice Group Head, Asia,
Corporate Transactions

T +852 2846 8905
joshua.cole@ashurst.com

Tracy Wang
Senior Associate

T +86 10 5936 2885
tracy.wang@ashurst.com

Yeqi Fei
Junior Associate

T +86 21 6263 1819
yeqi.fei@ashurst.com

www.ashurst.com