November 25, 2020

China Releases Draft Personal Information Protection Law

On October 21, 2020 the Standing Committee of the National People's Congress published for public comment the first draft of the Personal Information Protection Law (PIPL). If passed, the PIPL would become China's first omnibus law regulating the collection and processing of personal information.

Attorneys
David Chen

The draft PIPL proposes to codify many data privacy and protection principles and concepts that exist in China's current data governance regime, including the Cybersecurity Law[1] and the most recent version of the Personal Information Security Specification[2] (PI Security Specification), some of which, up until now, have not yet been firmly embodied in legislation. Perhaps most significantly for foreign businesses conducting or planning to conduct business in China involving the collection of personal information of individuals located in China, the draft PIPL proposes to have extraterritorial applicability and impose significant penalties for serious violations that are in the same vein as those contained in the European Union (EU) General Data Protection Regulation (GDPR).

Extraterritorial Applicability and Penalties

The draft PIPL would apply to the processing of personal information of individuals located in China that is conducted outside of China, including by Chinese and foreign businesses and individuals, under certain circumstances, including for the purposes of providing products or services to individuals located in China, and for analyzing and evaluating the behavior of individuals located in China. This closely mirrors the way extraterritorial applicability is handled under GDPR as set forth in Article 3(2) of the GDPR. However, the provision also contains a catch-all provision that permits the Chinese government to specify other bases for extraterritorial applicability under other circumstances if provided in other Chinese laws and regulations.[3]

Additionally, the draft PIPL proposes significant penalties for serious violations, including rectification orders, confiscation of illegal gains, business suspension, revocation of business licenses, and, perhaps most notably, fines of up to CNY 50 million or 5% of turnover in the previous year.[4] The draft PIPL does not clarify how the potential fines would be calculated – in particular, whether the fines would be determined based on the turnover of the specific legal entity or individual involved alone or if the turnover of its affiliated entities in China or worldwide would also be considered. The maximum amount of fines under the draft PIPL resembles, both in terms of magnitude and calculation bases, how maximum fines are calculated under Article 83 of the GDPR.

For data processors that are personal information processors (PIP), a new term that is defined as any entity or individual that independently determines the purposes, methods, and related matters of the processing of personal information, and is akin to the concept of a data controller under the GDPR, the draft PIPL proposes that any PIP located outside China that is subject to PIPL jurisdiction would be required to establish a dedicated agency or designate a representative located in China to be responsible for matters relevant to the protection of personal information, whose name and contact information would be submitted to China data regulators and who could potentially face penalties for violations of the PIPs they represent.[5] This requirement mirrors a similar requirement found in Article 27 of the GDPR.

The draft PIPL also requires entities and individuals that infringe the rights and interests of individuals as a result of their processing of personal information to bear liability and compensate impacted individuals based on the losses suffered by the individuals, the resulting benefits obtained by the PIPs, or, if those are difficult to ascertain, as determined by a court, and appears to shift the burden to PIPs to prove that it is not at fault in order to mitigate or avoid liability.[6]

Data Localization and Cross-border Data Transfers

The draft PIPL contains data localization requirements for critical information infrastructure operators (CIIOs) that are similar to those contained in the Cybersecurity Law, which currently requires CIIOs to store personal information collected or generated in China within the territory of China. However, the draft PIPL further expands the data

localization requirement to all PIPs whose processing of personal information reaches a yet-to-be determined volume threshold determined by Chinese cyberspace regulators.[7]

The draft PIPL also continues China's preference for utilizing security assessments as a way to legitimize cross-border data transfers for CIIOs and other PIPs that are subject to the above-described data localization requirements. Security assessments have been proposed in one form or another in previous draft regulations and are currently required under the Cybersecurity Law for CIIOs. However, the draft PIPL now expands requirements to legitimize cross-border data transfers to all PIPs and proposes additional pathways to do so, including obtaining certification from special professional certification organizations designated by Chinese cyberspace regulators, and concluding a contract with the overseas data recipient and supervising its data processing activities. A catch-all provision also gives Chinese regulators flexibility to determine additional cross-border data transfer mechanisms in the future. It remains to be seen if these additional avenues would provide greater flexibility for conducting cross-border data transfers than previously proposed, particularly in respect of real-time data transfers where security assessments and pre-certification on a per-transfer basis are generally unworkable, in practice.

Additionally, PIPs that transfer personal information to a recipient outside China are required to notify the individual of the identity of the 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 can exercise its rights against the recipient, and obtain the individual's consent to the transfer.[8]

Legal Bases for Data Processing

The draft PIPL clarifies the legal bases for the processing of personal information, some of which were previously included in the PI Security Specification, but which have not yet been firmly based in legislation. Under the draft PIPL, PIPs may process personal information (1) where the consent of the data subject is obtained, (2) where necessary for the conclusion or performance of a contract with the data subject, (3) where necessary for the performance of statutory duties or obligations, (4) where necessary for public health emergencies or the protection of the life, health, and property of individuals, (5) where the processing of personal information is within a reasonable scope for carrying out news reporting and supervising public opinion, and (6) other circumstances provided by other laws and administrative regulations.

Notably, some exceptions to data processing without the consent of data subjects contained in the PI Security Specification do not appear in the PIPL – including the exception for academic research institutions when processing de-identified personal information for statistical or academic research, and where necessary to maintain the safe and stable operation of products and services being provided. Businesses that had relied on these de-facto exceptions to consent contained in the PI Security Specification that were not carried over to the draft PIPL will need to review their existing data privacy practices and policies.

Notice and Consent Requirements

The draft PIPL provides additional clarity on the requirements for notice and consent for the collection and processing of personal information. Consent requires a clear and voluntary declaration of intent by an individual who is fully aware and understands the consent being given, and if the purposes, methods or scope of the processing of personal information changes, consent must be re-obtained. PIPs that know or should know they are processing personal information of a minor under the age of 14 are required to obtain consent from the minor's guardian to such processing. Consent can be withdrawn. However, a PIP cannot refuse to provide products or services if the individual does not consent or withdraws consent, unless the processing of personal information is necessary for providing such products or services.[9]

A PIP must also inform the individual in a conspicuous manner using clear and understandable language of the identity and contact information of the PIP, the purpose and method of its processing of personal information, and the type of and retention period for the personal information that is processed, and must notify the individual if any of the foregoing

changes. Additionally, a catch-all provision is included to allow Chinese regulators to specify additional notice requirements.[10]

The draft PIPL also requires PIPs to notify and obtain the consent of the relevant individuals in the event of any third-party transfers and cross-border transfers of their personal information.[11] Notice to the relevant individuals is also required where a PIP is required to transfer personal information as a result of a merger, divestiture, or similar reason.[12]

Sensitive Personal Information

The draft PIPL defines and includes specific requirements for the processing of sensitive personal information. Sensitive personal information is defined as personal information that may lead to discrimination or serious harm to the safety of persons or property if disclosed or unlawfully used, including information relating to race, ethnicity, religious beliefs, personal biological characteristics, medical health, financial accounts, and personal whereabouts. PIPs may process sensitive personal information only for specific purposes and only where sufficiently necessary to do so, and are required to obtain consent from individuals to collect and process personal information where consent forms the basis of the processing or where specific Chinese laws and regulations require. PIPs are required to notify the individual of the necessity of processing his or her sensitive personal information and the impact such processing may have. These requirements proposed in the draft PIPL would provide a stronger legal basis to the requirements for processing sensitive personal information already recommended in the PI Security Specification.[13]

Personal Information, Anonymization, and De-identification Defined

The draft PIPL defines personal information as information related to identified or identifiable natural persons recorded by electronic or other means, excluding anonymized information. This is largely consistent with the definition of personal information in the Cybersecurity Law, except that the draft PIPL definition makes specific reference to identifiable (in addition to identified) natural persons, and is largely aligned with the definition of personal information under the GDPR.

The draft PIPL also provides definitions of anonymization and de-identification. Previously, the definitions of anonymization and de-identification were unclear, which created uncertainty for businesses relying on anonymization or de-identification of personal information as an exception to consent requirements or as a safe-harbor from needing to comply with the more onerous compliance requirements that come from the processing of personal information. Under the draft PIPL, de-identification is defined as the processing of personal information in a manner such that it is impossible to identify certain individuals without the use of additional information. Anonymization refers to the processing of personal information in a manner such that it is impossible to identify certain individuals and that such identification is unable to be recovered. As a result, the draft PIPL appears to adopt a high standard for anonymization similar to what exists under GDPR.

Necessary Measures, Risk Assessments, and Documentation

The draft PIPL requires PIPs to take necessary measures consistent with attendant security risks to ensure the security of their processing of personal information, which includes organizational and technical security measures, training, and development of emergency plans to address security incidents. PIPs that process a volume of personal information exceeding a threshold yet to be determined by Chinese cyberspace regulators are required to designate a data protection officer to be responsible and whose name and contact information is required to be made public and provided to Chinese data protection regulators. PIPs are also required to regularly audit and conduct risk assessments of their processing of personal information, and maintain related records for at least three years.[14]

Data Security Incident Response

The draft PIPL requires PIPs to notify Chinese data regulators of any security breaches involving the disclosure of personal information. Impacted individuals are also required to be notified, unless the PIP has taken measures to effectively avoid damages caused by the disclosure of personal information. However, Chinese data regulators may still

require that impacted individuals be notified if they determine that the disclosure of personal information may cause damages to the impacted individuals. Although the draft PIPL does not prescribe specific time periods for notifying regulators or individuals, it does require that notification be provided "immediately."[15]

Provisions Influenced by Recent US-China Disputes

Notably, recent US-China disputes – particularly the recent bans on TikTok and WeChat proposed by the US government – appear to have influenced some of the provisions contained in the draft PIPL.

The draft PIPL would allow Chinese cyberspace regulators to include foreign entities and individuals that process personal information in a manner that damages the personal information rights and interests of Chinese citizens, or endangers national security or public interests of China, on a "blacklist," publicly announce such inclusion, and restrict or prohibit the sharing of personal information with such blacklisted entities or individuals.16

Additionally, the draft PIPL includes a provision that allows China to take corresponding measures against countries or regions that take discriminatory measures that are prohibitive, restrictive or otherwise limiting in nature against China in respect of the protection of personal information. Similar reciprocity provisions are also included in the draft Data Security Law and the new Export Control Law. Its inclusion in the draft PIPL would expand the tools available to the Chinese government to exercise export control and respond to foreign export control measures, which traditionally have been directed at controlling the export of technology, by allowing for the use of prohibitions and restrictions on the export of personal information to achieve reciprocity.

Other Notable Provisions

The draft PIPL contains provisions addressing the issue of joint controllership. Parties that jointly determine the purposes and methods of the processing of personal information are required to agree on their respective rights and obligations, and are held jointly and severally liable if their processing of personal information infringes upon the rights and interests of individuals.

The draft PIPL also contains provisions similar to those first introduced in the PI Security Specification that are directed at the use of personal information to make automated decisions, a practice that has become commonplace in the digital economy. The draft PIPL requires use of personal information to make automated decisions to be transparent, fair and reasonable, allows impacted individuals to request disclosures and reject decisions made by automated decision-making processes, and requires options for non-automated decision-making to be provided.[17]

The draft PIPL also addresses government surveillance and the collection of personal information by or for the Chinese government. Specifically, image capture and personal identification equipment installed in public places must be necessary for maintaining public security and accompanied by conspicuous signage. The data collected may only be used to maintain public security and may not be publicly disclosed or provided to other parties, unless the individual provides his or her consent or the use, disclosure or provision to other parties is otherwise permitted or required by other Chinese laws and regulations. Personal information collected by Chinese government entities is required to be stored within China, and a security assessment is required for providing such information to an overseas party. It remains unclear how this data localization requirement would apply to state-owned enterprises.[18]

What To Expect

Although many Chinese companies or foreign businesses operating in China through Chinese affiliates may find that many of the requirements proposed in the draft PIPL, including the notice and consent requirements and requirements to implement necessary technical and organizational measures, already exist in the Cybersecurity Law and the PI Security Specification and may even have already been addressed in previous compliance efforts, the proposed increase in penalties for non-compliance in the draft PIPL will likely prompt a review of and renewed focus on data privacy compliance. For non-CIIOs, compliance with the new volume-based data localization requirements, if they apply to your business, may require a rethink of existing personal information flows and use of cloud service providers. Additionally,

existing data practices and policies and business processes concerning reliance on anonymization/de-identification safe harbors, data security incident response and personal information processing audits, risk assessments, and documentation retention may need to be reviewed.

Foreign businesses that collect personal information as part of their businesses in China, but that do not have a presence in China, need to monitor the extraterritorial applicability provisions of the draft PIPL and prepare accordingly. Starting in 2016 when the GDPR was announced and continuing beyond 2018 after the GDPR went into effect, many businesses outside of the EU and European Economic Area (EEA) that had significant business in the EU and EEA embarked on significant efforts to review their data privacy and protection practices to bring their practices into compliance with the new law. If the extraterritorial applicability and penalty provisions in the draft PIPL are finalized in the form currently proposed, we can expect the start of a similar cycle as businesses outside of China with significant business in China involving the processing of personal information of individuals located in China embark on a similar effort in respect of the new PIPL.

1. Cybersecurity Law of the People's Republic of China, effective June 1, 2017
2. Information Security Techniques – Personal Information Security Specification (GB/T 35273-2020), effective October 1, 2020.
3. Art. 3, PIPL.
4. Art. 62, PIPL.
5. Art. 52, PIPL.
6. Art. 65, PIPL.
7. Art. 38, PIPL.
8. Art. 39, PIPL.
9. Art. 14-17, PIPL.
10. Art. 18, PIPL.
11. Art. 24 and 39, PIPL.
12. Art. 23, PIPL.
13. Art. 29-32, PIPL.
14. Art. 50-54, PIPL.
15. Art. 55, PIPL.
16. Art. 21, PIPL.
17. Art. 25, PIPL.
18. Art. 27 and 37, PIPL