China Passes the Personal Information Protection Law

September 1, 2021

On August 20, 2021, China's Standing Committee of the National People's Congress passed the Personal Information Protection Law ("PIPL").[1] The PIPL will take effect on November 1, 2021.[2]

A breakdown of the PIPL follows. High-level takeaways:

- With the PIPL, China is joining, if not leading, the global movement toward more and not less restriction on the processing of personal information. The PIPL has been referred to as China's version of Europe's General Data Protection Regulation ("GDPR"), given that the PIPL in substance mimics many of GDPR's restrictions on the usage and collection of personal information. In particular, the PIPL will make it harder for global companies doing business in China to move information around their global networks if the movement would take data across Chinese borders.

- The sheer amount of serial change to Chinese law adds to compliance challenges. The passage of the PIPL follows the adoption of the Data Security Law in June (Debevoise analysis available here). Companies have found that, as a practical matter, a phone call to the relevant Chinese regulator can be an essential means of understanding how the government sees data privacy and security requirements as a practical matter at any given moment. That phone call seems likely to be even more important with the adoption of yet another major new law.

WHO DOES THE PIPL COVER?

The PIPL applies to "Personal Information Processors," defined as "an organization or individual that autonomously determines the purpose and means of processing while performing activities involving processing Personal Information."

[1] 《中华人民共和国个人信息保护法》, full text accessible at: http://www.npc.gov.cn/npc/c30834/202108/a8c4e3672c74491a80b53a172bb753fe.shtml

[2] Article 73.

"Personal Information" ("PI") is defined broadly as "all kinds of information related to an identified or identifiable natural persons that is electronically or otherwise stored, excluding anonymized information."[3] As with GDPR, "processing" is the catchall term for any form of data handling. Processing includes, but is not limited to, the "collection, storage, usage, handling, transmission, provision, disclosure, and deletion" of PI.[4]

The PIPL applies to Personal Information Processors inside and outside of China. Similar to the GDPR, the PIPL states that it has extra-territorial effect. Extraterritorial processing of PI of natural persons within the PRC is subject to the PIPL if any of the following circumstances exists: (1) where the purpose is to provide products or services to natural persons within the PRC; (2) where the processing involves analysis or evaluation of activities of natural persons within the PRC; or (3) any "other circumstances as provided by laws or regulations."[5] Foreign entities engaged in such processing are also required to establish a domestic agent or designated representative within the PRC to be responsible for matters related to personal information matters. In addition, the name and contact information of such agency or representative must be reported to relevant authorities.[6]

The PIPL expressly provides that it applies to PRC government entities engaged in PI processing activities. Such government entities are limited to processing PI within the scope and limits necessary to perform their legal duties.[7]

WHAT DOES THE PIPL REQUIRE?

The PIPL requires that processing of PI be conducted in accordance with certain basic principles, such as lawfulness, fairness, good faith, clarity, necessity, relevance, and transparency. Personal Information Processors also must ensure completeness and accuracy of PI and take necessary measures to safeguard the security of the PI being processed.[8] Key requirements of the law include the following:

- Consent

[3] Article 2.
[4] Article 4.
[5] Article 3.
[6] Article 53.
[7] Articles 33 and 34.
[8] Articles 5-10.

The PIPL requires that, unless otherwise expressly exempted, Personal Information Processors obtain consent from[9] and provide notification to relevant individuals[10] prior to processing PI.

- Non-Discrimination

Personal Information Processors are prohibited from refusing to provide products or services to users who do not consent to processing of their PI, unless the processing of the relevant PI is necessary for the provision of products or services.[11]

- Security and Compliance

Personal Information Processors must take measures to ensure the safety of PI, for example (but not limited to), creating internal procedures and protocols, and conducting periodic compliance audits, etc.[12]

- Data Mining and Artificial Intelligence

The PIPL was also drafted to respond to increasing consumer complaints about big data based differential pricing strategies allegedly used by some online platforms and service providers in China. Personal Information Processors who utilize PI for Automated Decision-Making ("ADM") must ensure fairness of such processes and must not provide differential prices to consumers.[13] The term "Automated Decision-Making" means "automatic analysis and evaluation based on personal behaviors, preferences, or economic, health, credit status, and other information through computer programs."[14] Processors who engage in such ADM activities are subject to additional requirements, such as keeping relevant records of such ADM activities.[15]

- Sensitive Personal Data

The PIPL also includes additional notification and security requirements for processing of Sensitive Personal Information. That is defined as PI that, if leaked or misused, will likely infringe the personal dignity of natural persons or cause harm to personal and

[9] Article 13.

[10] Article 17. Notification must include: (1) name and contact of the processor; (2) purposes, means, categorization, and retention period; (3) the means and procedures for individuals to exercise rights under the PIPL; and (4) other information required under laws and regulations.

[11] Article 16.

[12] Articles 51-54.

[13] Article 24.

[14] Article 73.

[15] Article 55.

property safety. Sensitive Personal Information includes (but is not limited to) information related to biometrics, religious beliefs, specific identities, medical health, financial accounts, and locations, as well as PI of minors under age 14.[16]

Relatedly, the PIPL provides guidance and rules on several hot topics, including collecting facial recognition information in public spaces, processing PI of minors, and responsibilities of online platforms.

- Data Breaches

As a general rule, Personal Information Processors are required to notify "authorities performing duties related to protecting PI and relevant individual(s)" of data breaches and "immediately take remedial measures" in the event of actual or possible leakage, distortion, and loss. Personal Information Processors are not required to notify the relevant "individual(s)"[17] if the "remedial measures can effectively avoid the harm caused by such leakage, distortion, and loss," unless the "authorities performing PI protection duties" disagree and order otherwise.[18] The PIPL does not provide guidance on what are "remedial measures" or what measures would be considered effective.

WHAT ARE THE RULES FOR CROSS-BORDER TRANSFER?

Transfer of PI outside of territory of the PRC is heavily regulated.[19] Export of PI is subject to the following requirements:

- Legal Authorization

A Personal Information Processor may only transfer PI abroad if it is required for business needs and at least one of the following circumstances is fulfilled: (1) such transfer has passed security assessment organized by the cyberspace administration authorities ("国家网信部门")[20]; (2) such transfer has obtained a personal information protection certificate from a specialized agency nominated as required by the cyberspace administration authorities; (3) a contract with the foreign recipient has been entered

[16] Article 28.

[17] Although the PIPL does not define "individuals", it generally refers to data subjects.

[18] Article 57.

[19] PIPL does not specify whether Hong Kong SAR and Macau SAR should be treated as "outside of the territory of PRC" for the purpose of PI transfer. According to the general principles when interpreting PRC laws in relation to cross-border matters, the Hong Kong SAR and Macau SAR are usually treated as being outside of the jurisdiction of PRC.

[20] The term "cyberspace administration authorities" ("国家网信部门") includes but is not limited to the Cyberspace Administration of China ("CAC") (国家互联网信息办公室).

into based on the model contract to be provided by the cyberspace administration authorities; or (4) other circumstances provided in laws, regulations, or rules promulgated by the cyberspace administration authorities. In addition, PI may be exported in accordance with provisions of international treaties or agreements to which the PRC is a party. The Personal Information Processor must take "necessary measures" to ensure foreign recipients of PI abide by the requirements under the PIPL.[21]

- Risk Assessment

A Personal Information Processor must evaluate the impact of such export in advance and keep relevant records.[22] An evaluation would include (1) whether the purpose and means of processing are lawful, justified, and necessary; (2) the impact on personal rights and interests, as well as security risks; and (3) whether protective measures taken are lawful, effective, and proper for the risk level. A Personal Information Processor must retain records relating to its risk evaluation and relevant actions for at least three years.[23]

- Notification and Consent

A Personal Information Processor must notify relevant individuals of the proposed export and the foreign recipients of PI. The notification includes name(s) and contact information of the foreign recipients, the purposes and means of processing, the category of PI to be transferred, and information on how to exercise rights under the PIPL. A Personal Information Processor must obtain "individual consent" for such export of PI.[24]

- Data Localization

Article 31 of the Data Security Law requires "critical information infrastructure" ("CII") operators to localize data in China.[25] The PIPL implements that requirement for PI processed by CII operators, and requires that PI collected within the PRC must be stored locally. Where export of PI is necessary, such transfer must pass the security assessment organized by the cyberspace administration authorities, unless exempted by

[21] Article 38.

[22] Article 55.

[23] Article 56.

[24] Article 39.

[25] CII is defined under Article 31 of the Cybersecurity Law (《中华人民共和国数据安全法》第三十一条) as "information infrastructures of critical industries and sectors, such as public communications and information services, energy, transportation, water conservancy, finance, public services and e-government affairs, and as well as other information infrastructures that if breached, malfunctions, or is leaked, may seriously harms state security, national economy, or the people's livelihood." The extent of obligations regarding data localization by *non*-CII operators under the Cybersecurity Law remains unclear.

laws, regulations, or those authorities. The foregoing requirements also apply to non-CII processors, depending on whether the volume of processed data meets a "prescribed amount."[26] Any provision of PI stored within the PRC to foreign judicial or law enforcement bodies must be pre-approved by relevant PRC government authorities.

- Other Restrictions on Transfer

The cybersecurity administration authorities may bar a foreign individual or organization from receiving PI if such recipients engage in processing activities that are deemed to harm personal interests and/or rights of PRC citizens or harm national security interests or public interests. The authorities also may take "corresponding measures" if foreign nations or regions undertake "discriminatory, restrictive, or other similar measures" related to personal information protection against the PRC.

WHAT ARE THE CONSEQUENCES OF NON-COMPLIANCE?

The PIPL provides severe penalties and remedies for non-compliance and violation, including (1) warnings, correction orders, confiscation of illegal profits, and orders to suspend or shutdown services;[27] (2) up to RMB 1 million fine for relevant entities and RMB 10,000 to RMB 100,000 fine for in-charge and responsible individuals; (3) in serious cases, a fine up to RMB 50 million or 5% of the turnover of the previous year, as well as suspension or shutdown of business operations, or revocation of business license for relevant entities, and a fine ranging from RMB 100,000 to RMB 1 million plus additional restrictions for relevant individuals; and (4) publicly disclosed negative records in a credit report.

Violation of the PIPL may also lead to liabilities under other PRC civil and criminal laws, or administrative regulations, depending on the circumstances.

[26] Article 40. The PIPL is silent as to what is the "prescribed amount." Although of narrower application, we note that the Draft Amendments to the Measures for Cybersecurity Review released in July 2021 require cyber security review for operators who possess personal information of over 100 million persons before an offshore listing, which provided some visibility on what threshold the regulators might consider significant. (Article 6).《网络安全审查办法（修订草案征求意见稿）》第六条

[27] As recent actions by the Cybersecurity Administration of China involving ride-hailing app Didi Chuxing demonstrate, non-monetary consequences can be imposed swiftly and with little notice. *See* Tracy Qu and Zhou Xin, "China Takes Didi off app stores two days after Beijing announces cybersecurity review," South China Morning Post (July 4, 2021), https://www.scmp.com/tech/big-tech/article/3139786/china-takes-didi-app-stores-two-days-after-beijing-announces.

WHAT STEPS SHOULD MULTINATIONALS TAKE?

The PIPL undoubtedly presents new compliance challenges for foreign and multinational companies doing business in China. While a number of specifics remain unclear or subject to additional regulatory action, such as the rules and procedures for data transfer, the PIPL represents a significant ramping up of legal restrictions on PI processing in the Chinese market and will likely require companies to adopt GDPR-style procedures with Chinese characteristics. The PIPL will come into force in November 2021 and it remains to be seen how the PIPL will be enforced in practice. Based on the law and pending additional guidance from relevant authorities, it is advisable to consider making some adjustments or enhancements, such as below:

- Conduct a comprehensive review of Personal Information Processing activities and controls around the processing and export of PI, and determine whether ADM is used, to evaluate whether relevant activities align with the PIPL;
- Reevaluate existing data security and breach notification procedures against the PIPL and make additions or adjustments where necessary;
- Assess current records and procedures relating to individual consent and determine whether additional consent, such as individual consent to export PI abroad, needs to be obtained in light of the PIPL; and
- Stay alert to any additional regulatory action and continuously monitor updates in cyber security and data protection-related areas.

* * *

Please do not hesitate to contact us with any questions.

Debevoise & Plimpton LLP, like other international firms in China, is not admitted to practice PRC law. Our views are based on our general experience in dealing with similar matters and consultation of published compilations of Chinese law. We would be pleased to arrange for assistance from licensed Chinese counsel should you require a formal opinion as to any of the matters set forth in this update.

NEW YORK

Jeremy Feigelson
jfeigelson@debevoise.com

NEW YORK

Avi Gesser
agesser@debevoise.com

NEW YORK

Jim Pastore
jjpastore@debevoise.com

NEW YORK

Johanna N. Skrzypczyk
jnskrzypczyk@debevoise.com

SHANGHAI

Philip Rohlik
prohlik@debevoise.com

SHANGHAI

Tingting Wu
twu@debevoise.com

HONG KONG

William Y. Chua
wychua@debevoise.com

HONG KONG

Edwin Northover
enorthover@debevoise.com

HONG KONG

Emily Lam
elam@debevoise.com

WASHINGTON, D.C.

Luke Dembosky
ldembosky@debevoise.com