PAUL HASTINGS

Stay Current

普衡律师事务所《法律动态》中文版

September 2021

Follow @Paul_Hastings

China's New Personal Information Protection Law and Other New Data Concerns

By Phoebe Yan, Shaun Wu, Sarah Zhu, Zoey Xie, Fengzhen Yu

Introduction

China's top legislature, the Standing Committee of the National People's Congress ("NPCSC"), passed the Personal Information Protection Law ("PIPL") of the People's Republic of China on August 20, 2021, and it will become effective on November 1, 2021. Widely recognized as China's equivalent of the GDPR,[1] the newly enacted PIPL encompasses the effective reform achievements and practices in China's data protection regime in recent years and implements the most stringent supervision and data processing duties on data processors and enforcement agencies.

The PIPL is the eighth data-related law or regulation promulgated in China in 2021.[2] Among these laws and regulations, the Data Security Law ("DSL") was passed two months ago and has already become effective on September 1, 2021. Together with the 2017 enacted Cybersecurity Law, China has formed a comprehensive regulatory landscape for data protection regulations and laws, which provide overarching principles for all types of data processing activities within and even out of the territory of China, this time implicating not only the narrowly defined Critical Information Infrastructure Providers ("CIIO")[3] but also all businesses including non-CIIOs. This article will examine the extraterritorial application of the new PIPL in the context of the new DSL and other latest legislations, its consent-based data processing rules and exceptions, individual and corporate liabilities, and special issues associated with the new laws such as cross-border transfer, implications to international compliance, automated decision, and customer profiling.

Overview of the PIPL

The PIPL consists of eight chapters and 74 articles in total, setting out: (i) general provisions; (ii) personal information processing rules; (iii) cross-border personal information transfer rules; (iv) individual's rights in personal information processing activities; (v) obligations of personal information processors; (vi) enforcement agencies of personal information protection; (vii) legal liabilities; and (viii) supplement provisions. We summarize and analyze some of the key provisions below.

Extraterritorial Application

The PIPL has extraterritorial application because it will apply to personal information processing activities that occur (i) within the territory of China or (ii) outside the territory of China if the purpose of the activities is to:

- Provide products and services to natural persons in China;
- Analyze or evaluate behaviors of natural persons in China; or

- A catch-all clause covering other circumstances to be specified by laws and regulations.[4]

Enforcement Agencies and the New Audit Power

The Cyberspace Administration of China ("CAC"), the main enforcement agency of the Cybersecurity Law, is also the key enforcement agency under the PIPL governing personal information matters. On the local level, the PIPL allows the state and provincial governments to designate competent agencies,[5] but from past practice it is likely still the local offices of the CAC that mainly governs data security, and complaints can also be made before traditional enforcers such as the public security agency, the market supervision agency, and the consumer interests and rights protection agency, among others. These government agencies are also required to disclose results of investigation to complainants.

The PIPL empowers these agencies not only with traditional investigative powers and measures, such as to interview relevant parties, review and copy relevant transactional documents and financial records, perform dawn raids or on-site inspection, and seize and detain equipment or properties used for misconduct (but subject to probable cause and internal written approval), but also the powers to interview the legal representative or chief leader of the company and request a compliance audit against the company on its personal information processing activities, when the agency deems that there are relatively high risks in personal information processing activities or that a personal information security breach has occurred.

The Scope of "Personal Information" and "Sensitive Personal Information"

The PIPL defines "personal information" as information related to an identified or identifiable natural person recorded electronically or by other means, but excluding anonymized information. The PIPL also introduces the concept of "sensitive personal information", which refers to that personal information that, once leaked or illegally used, can easily lead to the infringement of the personal dignity of natural persons or endanger personal or property security of natural persons. The examples provided under the PIPL of sensitive information include biometric information, religion, special identification, medical and health information, financial accounts, and whereabouts information. Companies can only process sensitive personal information when there are specific purposes and sufficient necessity, with strict protection measures in place.

Note that the PIPL added in its last round of the legislative process that all personal information of minors under the age of 14 should also be deemed sensitive personal information.[6] On top of restrictions on processing sensitive personal information, the PIPL requires that special personal information protection rules must be developed for processing the personal information of minors.[7]

At the same time when the PIPL was released in the third week of August, the CAC also published the Measures on Management of Automotive Data Security, setting out examples on what would constitute personal information and sensitive personal information in the automobile industry.[8] It is entirely possible that the regulators will publish similar, specific measures for other industries, especially for healthcare, internet, telecom, and finance industries, due to the large data volume, big data technology, and high sensitivity of personal information involved in these businesses.

Consent-based Rules for Personal Information Processing

Waiver of Consent

Similar to other international counterparts such as the GDPR, consent is the primary basis for personal information to be processed under the PIPL. However, the PIPL provides that consent is not required for the processing of personal information if the processing is:

1. Necessary for entering into or performing a contract to which the individual is a party, or lawfully collective employment contracts;

2. Necessary for performing legal duties or obligations;

3. Necessary for dealing with a public health emergency or for protecting an individual's health or property in the event of an emergency;

4. Carried out within a reasonable scope for public interest;

5. Processing personal information that is already publicly available and within a reasonable scope; or

6. A catch-all clause covering other circumstances permitted by laws and regulations.[9]

Note that pursuant to the first exception listed above, the PIPL in its last round of the legislative process added that processing human resources information can be subject to a waiver of consent if such processing activities are necessary for conducting human resources management in compliance with employment policies. This calls for a review of human resources policies, particularly the data collection and transfer related processes therein, to ensure compliance with the PIPL.

Separate Consent

Additionally, the PIPL specifies that a separate, specific consent is required when:

1. Providing personal information to third parties[10];

2. Publishing personal information[11];

3. Utilizing personal information collected in the public area for purposes other than maintaining public security[12];

4. Processing sensitive personal information[13]; or

5. Transferring personal information outside of China.[14]

There is no definition of "separate consent" under the PIPL, but the draft standard Guidelines for Personal Information Notices and Consent provide that separate consent can be achieved by notifying or displaying the purpose, method, and scope, among others, of information processing to individuals through intensified notification methods (such as pop-ups) and requiring the individuals to opt in and make an affirmative consent.[15]

Harsh Individual and Corporate Liabilities under the PIPL

Under the PIPL, breaches will primarily trigger administrative penalties for the corporation, starting with correction orders and warnings and then moving to penalties such as confiscation of illegal gains, suspension or termination of business services, revocation of business licenses, and a fine up to RMB 50 million (approximately US$775,000) or 5% of business revenue in the previous year. Violations will also be marked in the company's credit system and become public information.[16]

Notably, the PIPL also sets up quite harsh individual liability for management who are either in charge of the misconduct or are directly responsible for the misconduct by a fine up to RMB 1 million (just over US$150,000) and a discretionary ban prohibiting service as directors, supervisors, senior managers, or personal information protection officers of relevant companies within a certain period of time.[17]

There will also be civil law consequences because the PIPL provides statutory grounds for individuals and businesses to bring civil actions against violators in addition to the previously existed tort law or civil law based cause of actions, and also allows the People's Procuratorate Offices (i.e., the public prosecutors in China), qualified consumer associations, and other organizations identified by the CAC to bring a public interest litigation.[18]

If any violation is up to the criminal law thresholds, there can also be additional criminal law liability for both the company and the applicable management personnel.[19]

Highlights of the PIPL

Extraterritorial Reach of the PIPL in Context of Other Data Legislations

As mentioned above, the PIPL explicitly extends its jurisdiction to all personal information processing activities carried out even outside of the territory of China.[20] The extraterritoriality feature not only echoes its European counterpart GDPR but also with the previously passed DSL that just became effective earlier this month.[21]

For overseas entities that fall under the extraterritorial reach of the new law, the PIPL further requires the entity to establish a "dedicated entity" or appoint a "representative" in China to be responsible for handling personal information protection matters.[22] This could mean that overseas business operators who target the China market, or otherwise analyze or assess the behavior of individuals in China, will need to set up offices or appoint representatives in China, as well as comply with China's massive data regulatory requirements.

For overseas businesses whose business operation may not be designed for the China market nor to track behaviors of individuals in China, the PIPL also empowers the Chinese authorities to "blacklist" the operators, so long as they are deemed to have harmed China's national security, public interest, or the legal rights and interests of Chinese citizens.[23] Inclusion on the list makes it unlawful for the listed entities to receive Chinese personal information. The CAC is responsible for creating and maintaining the prohibited list.

It is worth noting that the PIPL in its last round of the legislative process changed the obligations of those entities that are further entrusted by data processors with processing activities of personal information. Rather than require such entities to meet the same obligations as those that entrusted them for the processing activities, these entities being entrusted instead must (i) take necessary measures to ensure the security of the personal information processed, and (ii) assist those data processors that entrust the entities in fulfilling the data processors' obligations specified in the PIPL.[24] This arguably could mitigate the burden of oversight for offshore data processors, and such entities can argue that if they are entrusted by other entities to process Chinese personal information, their compliance roles should only ancillary under the PIPL.

Restrictions on Cross-Border Transfer and Implications to International Compliance

The PIPL uses an entire chapter to introduce cross-border transfer rules.[25] To summarize, the PIPL takes a tiered approach and sets up cross-border requirements based on data processors' identity and volume of information involved:

- For the CIIOs, it is provided that personal information must be stored in China, and when it is necessary to provide such information abroad, a prior security assessment organized by the CAC is mandatory unless the CAC deems the assessment unnecessary or the transfer falls within some exceptions allowed or to be allowed under laws and regulations.[26]

- For non-CIIOs that process a volume of personal information reaching or exceeding the threshold to be specified by the CAC (the "materiality test"), the same rules will apply.[27] While we wait and see if the CAC will implement additional, explanatory rules on the materiality test here, it is observed that at least two draft standards on personal and important information cross-border transfer and the data security review guidance for companies to be listed overseas have established more than 500,000 individuals or more than 1 million users as the respective thresholds on whether a CAC review is warranted.

- For non-CIIOs that fall below the CAC's materiality test, although there is no mandatory prior security assessment required, the data processor must also take one of the following two means before personal information can be transferred outside of China: (i) obtaining a certificate by a third-party professional institution; or (ii) executing a standard contract to be published by the CAC between Chinese personal information transferor and overseas recipient.[28] Of course, the non-CIIOs here can also opt to take the CAC security assessment, which will be a heightened expectation, or see if it can adopt measures under any catch-call clauses set up or to be set up by the law.

The final PIPL in its last round of the legislative process also added a new provision allowing cross-border transfer of personal information pursuant to international treaties or agreements concluded or acceded by the Chinese government.[29] We take this as an important and good supplement by the legislators. This means, for example, since China signed the Regional Comprehensive Economic Partnership Agreement ("**RCEP**") with ten ASEAN countries in November 2020 and Chapter 12 of the RCEP has e-commerce related rules, there could be a potential argument that cross-border transfer of personal information in the e-commerce context can be governed by the RCEP rules, not the PIPL rules discussed above. Additionally, since China is a member of the Convention on the Service Abroad of Judicial and Extrajudicial Documents in Civil or Commercial Matters ("**Hague Service Convention**"), cross-border transfer of personal information in the internal dispute resolution context can also be governed by the existing rules and practices pursuant to the Hague Service Convention, not the new tiered rules discussed above.

The trickiest situation would probably be cross-border transfer of personal information in the international compliance context. Notably, Article 41 of the PIPL and Article 36 of the DSL both require an approval of the Chinese competent authorities when dealing with data requests from foreign judicial or law enforcement agencies for personal information or data stored within China. This indicates that the Chinese government may use the PIPL or the DSL to prevent information sharing in the international compliance context with foreign enforcement agencies, whether for anti-bribery or corruption, export control, or other enforcement purposes. Companies in these situations already must grapple with existing state-secrets considerations, but now the scope of potential restrictions will be much broader.

Automated Decision-Making and Customer Profiling

Another important aspect of the PIPL is that for the first time in legislative history Chinese law introduced rules on "automated decision-making", and these rules will have strong implications for customer profiling and how businesses perform marketing and sales activities as well as take human resources and business structure optimization reviews based on automated data analysis.

Automated decision-making is defined under the PIPL to be the activity of using computer programs to automatically analyze or assess personal behaviors, habits, interests, or hobbies, or financial, health, credit, or other status, and make decision based thereupon.[30] The PIPL calls for transparency, justification, and fairness when data processors use automated decision-making to make decisions, and bans price discrimination or any other unreasonable, data-driven special treatment with other guidelines introduced as follows:

- Performing a "personal information protection impact assessment" prior to conducting an automated decision-making process and recording the results;

- Offering options not specific to individuals' characteristics and convenient opt-out or turn-off mechanism when sending out information push and advertisement; and

- Allowing an individual the access to clarifications on the automated decision-making process and the right to deny results solely made by the automated decision-making process when the results could significantly impact one's rights and interests.[31]

Takeaways

As we have observed, the newly passed PIPL, in conjunction with the Cybersecurity Law, the DSL, and their implementation rules and supplementary standards on scope of personal information, sensitive personal information and important data, cross-border transfer, industry-based specifications, among others, demonstrates that China is in completion of its data governance framework with stricter requirements and heightened expectations on data processors, particularly those that transfer data outside of China for business or compliance reasons. While we watch closely to see when the first major enforcement action pursuant to the PIPL or DSL will be, businesses would want to proactively prepare and review their data related policies and processes, with focus on any flow of information related to international compliance (such as human resources and whistle-blower related policies and processes), any decision or business model related to automated-decision making, and any infrastructure or resources deficiencies related to consent in data processing activities. Data will be the next, big challenge for legal, regulatory, and compliance oversight in the upcoming years in China.

✧ ✧ ✧

If you have any questions concerning these developing issues, please do not hesitate to contact any of the following Paul Hastings lawyers:[If in Chinese text use SimSun font:]

Beijing

Fengzhen Yu
86.10.8567.5400
fengzhenyu@paulhastings.com

Hong Kong

Shaun Wu
86.21.6103.2988
shaunwu@paulhastings.com

Sarah Zhu
852.2867.9018
sarahzhu@paulhastings.com

Shanghai

Phoebe Yan
86.21.6103.2939
phoebeyan@paulhastings.com

Zoey Xie
86.21.6103.2701
zoeyxie@paulhastings.com

[1] *See* General Data Protection Regulation (EU) 2016/679.

[2] The other seven data-related laws and regulations passed in 2021 include: Measures for the Supervision and Administration of Online Transactions released on March 15, Notice on Promulgation of the Rules on the Scope of Necessary Personal Information for Common Types of Mobile Internet Applications released on March 22, Data Security Law released on June 10, Data Regulations of Shenzhen Special Economic Zone released on July 6, Guidelines for Outbound Investment & Cooperation in Digital Economy released on July 23, Provisions of the Supreme People's Court on Several Issues concerning the Application of Law in the Trial of Civil Cases Relating to the Use of Facial Recognition Technologies to Process Personal Information released on July 28, Security Protection Regulations for Critical Information Infrastructure released on August 17.

[3] Pursuant to the Cybersecurity Law and its subsequent implementation rules, CIIO refers to operators of network facilities and information systems that may seriously endanger national security, national economy, people's livelihood, and public interest once they are damaged, lost function, or leaked data; and a list of examples was given under the laws to include energy, finance, transportation, water conservancy, health care, education, social security, environmental protection, cloud computing, big data, national defense science and industry, large equipment, chemical industry, food and drug, and news industries.

[4] *See* PIPL, Article 3.

[5] *See* PIPL, Article 60.

[6] *See* PIPL. Article 28.

[7] *See* PIPL, Articles 29, 30, 31.

[8] *See* Measures on Management of Automotive Data Security, Article 3.

[9] *See* PIPL, Article 13.

[10] *See* PIPL, Article 23.

[11] *See* PIPL, Article 25.

[12] *See* PIPL, Article 26.

[13] *See* PIPL, Article 29.

[14] *See* PIPL, Article 39.

[15] *See* Information Security Technology – Guidelines for Personal Information Notices and Consent (still in draft, 20210985-T-469)

[16] *See* PIPL, Articles 66 and 67.

[17] *See* PIPL, Article 66.

[18] *See* PIPL, Article 70.

[19] *See* PIPL, Article 71.

[20] *See* PIPL, Article 3.

[21] *See* Data Security Law, Article 2.

[22] *See* PIPL, Article 53.

[23] *See* PIPL, Article 42.

[24] *See* PIPL, Article 59.

[25] *See* PIPL, Chapter 3.

[26] *See* PIPL, Article 38.

[27] *See* PIPL, Article 40.

[28] *See* PIPL, Article 38.

[29] *Id.*

[30] *See* PIPL, Article 73.

[31] *See* PIPL, Articles 24 and 55.