Cybersecurity, Privacy and Data Protection Alert

Akin Gump
STRAUSS HAUER & FELD LLP

The New PRC Personal Information Protection Law

August 27, 2021

On August 20, 2021, the 30th session of the Standing Committee of the 13th National People's Congress (NPC) adopted China's new *PRC Personal Information Protection Law* (PIPL)[1], which will take effect on November 1, 2021. The new law lays out for the first time a comprehensive set of rules around the collection, processing and protection of personal data.

The PIPL incorporates certain well-recognized data protection principles such as requiring processors to collect personal information only to the minimum extent necessary and to obtain informed consent from individuals prior to the collection or transfer of personal information. In addition, the PIPL provides for enhanced protection of "sensitive personal information", which includes information relating to biometrics, religious beliefs, medical and health, financial accounts and location tracking. There are also more stringent requirements, such as more comprehensive compliance systems and enhanced transparency, which apply to processors that provide important Internet platform services, have a "large number of users" and carry out "complex" business activities.

Cross-border transfers of personal information are only permitted under the PIPL if one of the following conditions is satisfied: (i) passing a safety assessment by the national cyberspace authority; (ii) obtaining accreditation from agency-appointed entities; or (iii) entering into standard form agreements approved by the relevant agencies with the overseas recipient. Specific consent must also be obtained from individuals prior to any cross-border transfer of their personal information.

The PIPL applies to all information processing activities in China, regardless of whether the processor is a foreign entity or whether the personal information belongs to foreign individuals. It also applies to activities outside China involving the personal information of individuals located in China, where the purpose of such activities is to provide products or services to those individuals or where the behavior of those individuals is analyzed or assessed.

Legislative Background

In 2016, China launched its first landmark legislation in the area of data protection and cybersecurity, the *PRC Cybersecurity Law* (CSL)[2], which took effect on June 1, 2017, and focuses on the regulation of activities concerning the construction, operation,

Contact Information

If you have any questions concerning this alert, please contact:

Tatman R. Savio
Registered Foreign Lawyer
tatman.savio@akingump.com
Hong Kong
+852 3694.3015

Natasha G. Kohne
Partner
nkohne@akingump.com
San Francisco
+1 415.765.9505

Michelle A. Reed
Partner
mreed@akingump.com
Dallas
+1 214.969.2713

Daniel L. Cohen
Consultant
daniel.cohen@akingump.com
Hong Kong
+852 3694.3032

Jingli Jiang
Counsel
jjiang@akingump.com
Beijing
+86 10.8567.2229

Sonia Lor
Solicitor
sonia.lor@akingump.com
Hong Kong
+852 3694.3062

maintenance and use of networks, as well as supervision and management restrictions on the transfer of personal information and business data overseas. Since then, dozens of implementing regulations, guidelines and national standards in the cybersecurity area have been released or are being drafted. In 2020, China unveiled two more significant legislative proposals in the field of data protection: the first dr afts of the PRC Data Security Law and the PIPL. The final *PRC Data Security Law* (DSL)[3] was passed in the 29th session of the Standing Committee of the NPC on June 10, 2021, and will come into effect on September 1, 2021.

While the DSL is aimed at broadly regulating data security with an emphasis on safeguarding national security, the PIPL focuses on the protection of personal information. Before the enactment of the final version of the PIPL, two drafts were issued for public consultation in October 2020 and April 2021. The release of the PIPL completes the trifecta of China's foundational data governance regime.

Key Provisions

The PIPL is composed of a total of eight chapters and 74 articles. Based on the foundation of the CSL and DSL, the PIPL further refines the principles and personal information processing rules to be followed in the protection of personal information, clarifies the boundaries of rights and obligations in personal information processing activities, and improves the work systems and mechanisms for personal information protection.

Basic Principles

The PIPL stipulates that the following basic principles must be followed in the processing of personal information:

1. *The Principle of Legality and Good Faith*. Personal information should be processed following the principles of legality, appropriateness, necessity and good faith. The PIPL emphasizes that personal information must not be processed through misleading, fraudulent or coercive methods.
2. *Clear and Reasonable Purpose*. The processing of personal information should have a clear and reasonable purpose, and be directly related to the processing purpose. The processing of personal information should use the method that has the least impact on personal rights. The collection of personal information should be confined to a minimum necessary for the designated purpose, and excessive collection of personal information is not allowed.
3. *Openness and Transparency*. The processors shall clearly disclose the personal information processing rules, the processing purpose, the processing method and the processing scope.
4. *Quality Assurance*. The quality of personal information shall be preserved when the personal information is processed to avoid any negative impact on personal rights and interests due to any inaccuracy or incompleteness of personal information. In addition, the processors are responsible to take measures to ensure the safety of personal information.
5. *Illegality*. Entities and individuals are prohibited from the illegal collection, use, processing and transfer of personal data, as well as the illegal sale, provision or publication of personal data. Processing activities that endanger national security and public interest are prohibited.

Bodi Jia
Associate
bjia@akingump.com
Singapore
+65 6579.9080

Alasdair Kan
Solicitor
alasdair.kan@akingump.com
Hong Kong
+852 3694.3069

Ciniya Huang
Associate
chuang@akingump.com
Beijing
+86 10.8567.2223

Extraterritorial Application

Article 3 stipulates that the PIPL is applicable to all data processing activities in China, regardless of whether the data processor is a foreign entity or whether the personal information belongs to foreign individuals. In addition, the PIPL draws on the extraterritorial provisions of the European personal information protection laws in stating that the law also applies to entities engaged in any activity outside China involving the processing of personal information of individuals inside China, where the purpose of the activity is to provide a product or service to those individuals or analyze or assess the behavior of those individuals. The PIPL treats processors carrying out such activity as “foreign personal information processors.” Article 53 further requires these foreign processors to set up a specific department or designate a representative within China to be responsible for handling matters relevant to data protection, and to register details of such department or representative with the government departments concerned.

Authorized Personal Information Processing Activities

Article 13 of the PIPL lists seven types of situations where the processing of personal information is authorized:

1. Informed consent has been obtained from the individual.
2. It is necessary for the conclusion or performance of contracts, or the implementation of human resource management in accordance with labor regulations and collective contracts signed in accordance with the law.
3. It is necessary for the performance of statutory duties or obligations.
4. It is necessary for responding to public health emergencies, or for the protection of health or property in emergency situations.
5. Reasonable processing of personal information in order to implement activities in the public interest, such as news reporting and supervision of public opinion.
6. Reasonable processing of personal information which has been made public by the individual or through other legal means.
7. Other circumstances stipulated by laws and administrative regulations.

Articles 14 and 15 of the PIPL identify the standards for obtaining informed consent and the withdrawal of consent. Consent should be made voluntarily and clearly by an individual with full knowledge, and the personal information processor is obliged to provide a convenient means for the withdrawal of consent. Article 16 also stipulates that personal information processors shall not refuse to provide products or services on the grounds of lack of or withdrawal of consent, unless such personal information is necessary for the provision of products or services.

Strict Protection on Sensitive Personal Information and Personal Information of Minors

The PIPL provides for enhanced protection of “sensitive personal information”, which includes biometrics, religious beliefs, specific identities, medical and health, financial accounts, whereabouts and other information, as well as personal information of minors under the age of 14. Personal information processors shall only process sensitive personal information when they have a specific purpose and sufficient

necessity, and take strict protection measures, including conducting impact assessments in advance, and informing individuals of the necessity of processing and the impact on personal rights and interests.

Rights and Obligations

Rights of Individuals. The PIPL codifies the rights of individuals in personal information processing activities, including, among others, the right to know, the right to restrict or reject the processing of personal information by others, the right to inquire and request a copy of personal information from processors, the right to rectify incorrect or incomplete information, and the right to have personal information deleted. Processors are obliged to set up a convenient mechanism for individuals to exercise the above rights.

Obligations of Personal Information Processors. For personal information processors, the PIPL requires them to formulate "internal management systems and operating procedures" (which are undefined), adopt appropriate technical security measures, designate responsible persons to supervise personal information processing activities, conduct regular compliance audits on personal information activities, and conduct prior personal information protection impact assessments for high-risk processing activities, such as those relating to sensitive personal information and transfer of personal information overseas. In the event of a data breach, the processor is obliged to undertake remedial measures immediately and notify relevant government agencies and the affected individuals.

Special Obligations. In addition, the PIPL creates special obligations for personal information processors who provide important Internet platform services, have a "large number of users", and carry out "complex" business activities. These special obligations include: (i) establishing a comprehensive compliance system designed to protect personal information and supervised by an independent organization mainly composed of external members; (ii) formulating platform rules that clearly state the protection standards and obligations relating to products or services offered on the platform; (iii) ceasing to provide services to providers of products or services on the platform that deal with personal information in serious violation of the law; and (iv) regularly publishing personal information protection social responsibility reports.

Requirements on Automated Decision-Making

In response to the specific privacy challenges brought by the adoption of artificial intelligence and other automated technologies, Article 24 of the PIPL stipulates that personal information processors who use personal information to make automated decision-making shall ensure the transparency of decision-making and the fairness and impartiality of the results, and shall not impose unreasonable differential treatment on individuals in terms of transaction prices and other transaction conditions. At the same time, personal information processors that use automated decision-making methods to push information and direct commercial marketing to individuals should provide options that are not specific to their personal characteristics, or provide individuals with convenient means to refuse.

Legal Framework of Cross-Border Transfers of Personal Information

Generally, PIPL requires personal information processors to take necessary measures to ensure that the activities of overseas recipients in processing personal information

meet the personal information protection standards set forth in the PIPL. All cross-border transfers of personal information are only permitted under the PIPL if one of the following conditions is satisfied: (i) passing a safety assessment by the national cyberspace authority; (ii) obtaining accreditation from agency-appointed entities; (iii) entering into standard form agreements approved by the relevant agencies with the overseas recipient; or (iv) any other conditions provided for under other legislation or regulations, or those set by relevant agencies, from time to time. In addition, the PIPL requires that specific consent be obtained from individuals prior to the transfer.

Besides the above general requirement, Critical Information Infrastructure Operators (CIIOs) or personal information processors that process personal information up to the amount prescribed by the national cyberspace authority shall store personal information within China. Where it is necessary to provide such information to an overseas recipient, the applicant will need to pass a security assessment organized by the national cyberspace authority.

In addition to the above requirements, we also recommend companies to pay attention to any industry-specific regulations or guidance that relevant agencies may impose. Taking the automobile industry as an example, under the *Automotive Data Security Management Regulations (for Trial Implementation)* promulgated pursuant to the CSL, DSL and other relevant laws[4], with effect from October 1, 2021, automobile data processors that store important data (including personal information involving more than 100,000 personal information subjects) may only transfer data overseas if it is necessary to do so and only after a data outbound security assessment organized by the national cyberspace authority is passed.

Under Article 41 of the PIPL, individuals and organizations are not allowed to provide personal data stored within China to foreign law enforcement authorities without the prior approval of the relevant authorities in China. It is unclear how data “stored within China” is defined and how a “data processing” entity can apply for the approval at this time; the practical enforcement of such provision will likely depend on more detailed regulations or measures to be published by the relevant regulatory bodies.

Legal Liabilities

As explained below, companies that infringe provisions of the PIPL are subject to potential administrative, civil and criminal liability.

Administrative Penalties. In the event of a breach of the PIPL, personal information protection authorities may issue a rectification order or warning and confiscate any illegal proceeds. The relevant apps may be subject to suspension or termination of services. Companies and their responsible officers that refuse to rectify breaches may be subject to additional fines. Serious breaches may be penalized by suspension of business operations, cancellation of business certificate, and levy a fine of up to RMB 50,000,000 or 5% of annual turnover. Responsible officers may be subject to fines and prohibitions from taking management or personal information protection related roles in other companies. PIPL violations may also be announced to the public and included in the relevant companies’ social credit records in accordance with the relevant regulations.

Civil Liability. If the processing of personal information in breach of an individual’s rights causes harm, and the personal information processor cannot prove that it is not at fault, the processor shall be liable to damages and other civil liabilities. Designated

consumer organizations may also bring suit on behalf of a class of individuals if a large number of individuals are harmed.

Criminal Liability. Violations of the PIPL that amount to criminal offenses may incur criminal liability.

Key Implications

The PIPL clarifies the principles to be followed in personal information processing activities, improves personal information processing rules, protects the rights of individuals in personal information processing activities, strengthens the obligations of personal information processors, and sets strict legal liability.

The promulgation and implementation of the DSL, the PIPL and relevant supporting regulations will have a sweeping impact on businesses that have domestic and cross-border operations, in the context of China's increasingly tight regulatory environment in relation to personal information and other data.

[1] PRC Personal Information Protection Law (《中华人民共和国个人信息保护法》) (in Chinese).

[2] PRC Cybersecurity Law (《中华人民共和国网络安全法》) (in Chinese).

[3] PRC Data Security Law (《中华人民共和国数据安全法》) (in Chinese). Please refer to our client alert here for an overview of the DSL.

[4] Automotive Data Security Management Regulations (for Trial Implementation) (《汽车数据安全管理若干规定（试行）》) (in Chinese).

akingump.com