ALLEN & OVERY | 朗悦
LANG YUE | 安理国际律师事务所

Key Regulatory Changes in China's New Legislation on Personal Information Protection

Background

On 20 August 2021, the Standing Committee of the National People's Congress adopted the Personal Information Protection Law (the PIPL), the long-awaited and first omnibus personal data protection legislation in China.

This new law will take effect on 1 November 2021. As it does not offer any statutory transition period after 1 November, it may be challenging for some players to adapt their data privacy policies and practice to comply with this new law within a two-month period.

Overview

The new law is in essence an omnibus rulebook for those who process the personal information of individuals located in China, regardless of whether those processors of personal information[1] are in China themselves or are outside of China. There are general rules for personal information processors (Chapter 2, part 1), as well as special rules for government organs (Chapter 2, part 3). There are also special rules for those that process sensitive personal information (Chapter 2, part 2).

The new law also outlines the unified rules applicable to the provision of personal information across borders (Chapter 3).

It articulates rights for individuals in connection with the activities of those who process personal information (Chapter 4) and spells out certain obligations for those who process personal information (Chapter 5). The law identifies those departments which are responsible for carrying out the protection of personal information (Chapter 6). Legal liability for violation of the law is set out in Chapter 7.

The term "personal information" is defined quite broadly in the law, leading the reader to consider other already existing laws and regulations in this area – "All kinds of information recorded electronically or through other methods related to identified or identifiable natural persons, not including information after being made anonymous (Article 4(1))." A photograph of a person along with that person's name would seem to be enough to qualify as personal information if it contains sufficient details for identifying the natural person. Or a name together with an email address might also seem to be enough, but a name alone would likely not be enough unless it was unique. Put another way, "personal information" looks to be any combination of information that allows someone to identify one person from another person. If this is the correct interpretation, multiple headaches are coming for those that hold or use the information of individuals in China.

Processing of personal information is also broadly defined:"…includes those that collect, store, use, process/improve, transmit, provide, publicize, delete, etc.") (Article 4(2)).

Key aspects

The PIPL will materially change the current regulatory framework of personal information protection in mainland China, especially the following key aspects:

1. Substantially increased penalties

The maximum administrative fine for egregious cases of unlawful processing of personal information and failure to comply with personal information protection obligations under the PIPL is up to RMB 50 million or 5% of the business revenue of the violator in the preceding year. This is much higher than that set out in the current Chinese data privacy and cybersecurity laws. As most data privacy rights and obligations scattered in current Chinese laws and regulations are restated in the PIPL, this means the maximum fine applicable to non-compliance will be substantially increased after 1 November 2021.

[1] Please note that the definition of the personal information processor under the PIPL is similar to that of the data controller under the GDPR.

Other than imposing administrative fines, the regulator under the PIPL may also (i) order corrections, (ii) issue warnings, (iii) confiscate illegal income, (iv) order the suspension or termination of the services provided by the app which unlawfully processes personal information, (v) order the suspension of relevant business activities or cessation of business for rectification, (vi) report to the relevant competent department for cancellation of corresponding professional licences or business permits, (vii) record the non-compliance in a credit system in accordance with the law, and (viii) blacklist overseas organisations or individuals who engage in personal information processing activities that infringe the personal information rights and interests of citizens of China, or endanger the national security or public interest of China, and adopt measures such as restricting or prohibiting the provision of personal information to them.

Moreover, for non-compliant legal entities, the regulator may impose an administrative fine up to RMB 1 million on the relevant directly responsible person(s) in charge and other directly responsible person(s), and prohibit them from acting as directors, supervisors, senior management and personal information protection officer during designated period.

2. Exterritorial jurisdiction

As a significant difference to the PRC's Cybersecurity Law and the recently adopted Data Security Law, the PIPL expressly provides for exterritorial jurisdiction on data processing activities outside the territory of China[2], if the such activities are:

(a) for the purpose of providing products or services to natural persons in the territory of China,

(b) for analysing or evaluating the behaviour of natural persons in the territory of China, or

(c) other circumstances stipulated by laws and administrative regulations.

As a result, these activities as well as persons carrying out these activities will be subject to the entirety of the PIPL, even if they are outside China. In addition, such persons are specifically required to establish a dedicated office or appoint a designated representative in China to deal with matters related to the protection of personal information, and to report the name of the relevant office or the name and contact information of the representative to the competent Chinese regulator.

The extraterritorial reach of the PIPL will have significant impact on foreign business traditionally relying on the fly-in-fly-out business model without an onshore presence.

3. Extended localisation and export restraints

As a significant regulatory step ahead of the Cybersecurity Law, the PIPL extends the personal information localisation obligation to cover not only the critical information infrastructure operators (CIIOs) but also those personal information processors, the volume of personal information processed by which satisfies the benchmark to be specified by the state cyberspace authority (Significant Volume Processors).

In addition, the PIPL sets up much more comprehensive and detailed regulatory requirements on cross-border transfers of personal information by all types of personal information processors, as compared to the Cybersecurity Law. This new personal information export framework is summarised as follows:

Type of processors	Pre-condition	Other obligations
CIIO and the Significant Volume Processors	✧ pass the security assessment organised by the state cyberspace authority; or ✧ if exempted by specific provisions of laws, administrative regulations or the rules of the state cyberspace authority, comply with such specific provisions	✧ conduct advanced personal information protection impact assessment ✧ give proper prior notification to data subjects ✧ obtain separate consent from data subjects ✧ implement necessary measures to ensure the personal information processing activities of the overseas data recipient meet the standards of personal information protection stipulated in the PIPL
Other personal information processors	✧ pass the security assessment organised by the state cyberspace authority; or ✧ conduct personal information protection certification via professional institutions; or ✧ enter into the standard contract formulated by the state cyberspace authority with the overseas data recipient; or ✧ satisfy other requirements provided by laws, administrative regulations or the rules of the state cyberspace authority	

[2] Excluding natural persons processing personal information for personal or household affairs.

The PIPL specifically allows cross-border transfers of personal information in accordance with applicable international treaties and agreements China has concluded or participated in.

4. Legal basis for processing personal information

Other than the consent of the individual data subject, the PIPL extends the scope of the legal basis for processing personal information to include the following circumstances (under which consent is no longer required):

(a) as necessary for the conclusion or performance of a contract to which the data subject is a party;

(b) as necessary to implement human resources management pursuant to the employment policies formulated in accordance with the law and any collective labour contract lawfully entered into;

(c) as necessary to perform legal duties and obligations;

(d) as necessary to deal with public health emergencies and protect the safety of life, health and property of natural persons in an emergency;

(e) within reasonable scope, in order to conduct news reports, public opinion supervision and other acts in the public interest;

(f) to process, within reasonable scope, the personal information that is already made public by the data subject or other personal information that is already made public in accordance with the law; and

(g) other circumstances provided by laws and regulations.

In practice, the consent requirement will likely remain the primary basis for processing personal information because (a) the above bases are limited and do not include something broader such as legitimate business interests like the EU's General Data Protection Regulation, and (b) some of the bases are limited to the extent "necessary" and may not necessarily satisfy the actual business needs of a complex business structure.

In the meantime, the PIPL reinforces the consent requirement by, for example, providing that:

(i) consent shall be explicit;

(ii) consent shall be voluntary;

(iii) if the purpose or method of the processing or the type of the processed personal information changes, then the individual data subject's consent shall be refreshed;

(iv) the individual data subjects have the right to withdraw their consent and ask for deletion of the personal information, and the personal information processor must provide convenient methods for consent withdrawal;

(v) personal information processors shall not refuse to provide products or services on the grounds that data subjects do not agree to the processing of their personal information or have withdrawn their consent, except only if such personal information is necessary for the provision of such products or services; and

(vi) separate consent is required:

- for processing sensitive personal information;
- for cross-border transfers of personal information;
- for the personal information processor to transfer personal information to another personal information processor;
- for the personal information processor to disclose personal information; and
- if personal information is collected by facilities installed in public areas for purposes other than safeguarding public security.

These requirements may be challenging to some business operators due to the cost of necessary adjustments to their IT infrastructure and maintenance.

5. Statutory notifications

Individual data subjects' information rights are a key matter under the PIPL. This is not surprising because information rights are crucial in order for individual data subjects to exercise their rights under this law as well as to give consent where applicable. Below is a short summary:

(a) *right to be informed prior to processing*: before processing personal information, personal information processors shall truthfully, accurately and completely inform individual data subjects of the following matters in a conspicuous manner and in clear and easy-to-understand language:

- name and contact information of the personal information processor;
- purpose of the processing of personal information, processing method, type of personal information processed, and retention period;
- methods and procedures for individuals to exercise their rights under the PIPL; and
- other matters that should be notified by laws and administrative regulations.

(b) *right to be notified in case of change*: if there is any change to the matters specified in the preceding paragraph, the individual data subjects shall be notified of the change;

(c) *right to be notified in case of transfer due to merger, division, dissolution or bankruptcy*: if a personal information processor needs to transfer personal information due to merger, division, dissolution or bankruptcy, it shall inform the individual data subject of the name and contact information of the recipient;

(d) *right to be informed prior to transfer to other personal information processor*: when a personal information processor provides another personal information processor with any personal information it processes, it shall inform the individual data subject of the name of the recipient, contact information, processing purpose, processing method, and type of personal information involved;

(e) *right to be informed prior to processing sensitive personal information*: when processing sensitive personal information, the personal information processor shall, in addition to the matters specified in paragraph (a) above, inform individual data subjects of the necessity of processing sensitive personal information and the impact on personal rights and interests;

(f) *right to be informed prior to data export*: when a personal information processor provides personal information outside China, it shall inform the individual data subject of the name of the overseas recipient, contact information, processing purpose, processing method, types of personal information, and methods and procedures through which the individual data subject may exercise the rights prescribed by the PIPL against the overseas recipient;

(g) *right to be notified in case of data breach*: where personal information leakage, tampering or loss occurs or may occur, the personal information processor shall immediately take remedial measures and notify the individual data subjects, unless the personal information processor takes measures to effectively avoid the harm caused by such information leakage, tampering, or loss; provided that, if the competent authority believes that it may cause harm, the authority has the power to request the personal information processor to notify the individual data subjects; and

(h) *right of access*: individual data subjects have the right to check and copy their personal information, and the personal information processor is required to grant access in a timely manner; where the personal information is inaccurate or incomplete, the individual data subject has the right to request the personal information processor to correct or supplement such information.

6. Data compliance review/assessment

For the first time, the PIPL formally imposes data compliance review and assessment obligations on personal information processors, which are summarised as follows:

(a) all personal information processors are required to carry out regular data compliance audits to review their compliance on processing personal information;

(b) personal information processors are also required to carry out an advanced personal information protection impact assessment prior to any of the following processing activities and to retain the records for no less than three years:

- process sensitive personal information;
- use personal information for automated decision-making;
- entrust third parties to process personal information, provide personal information to other personal information processors, and disclose personal information;
- transfer personal information overseas; and
- other personal information processing activities which have significant impact on the rights of individuals; and

(c) personal information processors who provide important online platform services, have a massive volume of users, and/or conduct complex types of business, are further required to, among other things:

- establish an independent supervising body primarily comprised of external persons to supervise personal information protection compliance;
- publish personal information protection social responsibility reports on a regular basis, for supervision by the public; and
- cease to provide services to the providers on the platform who seriously violate the requirements under law on personal information processing.

7. Automated decision-making [3]

The PIPL imposes the following specific regulatory requirements on business operators who use personal information to make automated decisions:

(a) the personal information processors shall ensure the transparency of the decisions;

(b) the personal information processors shall ensure 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;

(c) as for information push and commercial marketing to individuals through automated decision-making methods, the personal information processors shall also provide options that are not specific to the personal characteristics of individual users, or provide individual users with convenient ways to refuse; and

(d) for decisions that have a significant impact on personal rights and interests, individual users have the right to request personal information processors to explain, and have the right to refuse personal information processors to make decisions only through, automated decision-making methods.

8. Regulating state activities on personal information

The PIPL has a section specifically setting out the requirements on the personal information processing activities of state agencies. The key features of this section are summarised as follows:

(a) the processing of personal information by state agencies shall not exceed the scope and extent necessary to perform their statutory duties;

(b) when state agencies process personal information in order to perform their statutory duties, they shall fulfil the notification obligation as provided by the PIPL, unless such notification will impede state agencies in the performance of their duties or as otherwise provided by law;

(c) the other sections of the PIPL also apply to the processing activities of personal information by state agencies, which means data subjects would have the same rights where state agencies process their personal information; and

(d) personal information processed by state agencies shall be stored in the territory of China. Where it is necessary to transfer personal information overseas, a security assessment is required to be carried out.

[3] Automated decision-making is defined under the PIPL as the activities of automatically analysing and evaluating personal behaviours, hobbies, economic, health and credit status through computer programs, and making decisions.

9. Foreign proceedings

Matters involving proceedings overseas raise other concerns.

There are now numerous provisions of Chinese law which may be implicated when a company is faced with evaluating whether information can be transferred from Mainland China overseas in connection with a foreign investigation or litigation. Generally speaking, Chinese law regulates the export of certain types of information overseas (e.g., PRC state secrets, important data, restricted archives, personal information, etc.) and also seeks to regulate providing information overseas in connection with certain types of foreign activities (e.g, foreign listings, criminal litigation, securities investigations, foreign law enforcement activities, etc.). The new PRC Data Security Law (DSL), which comes into effect on September 1, for example, regulates the export of data when a China based company is faced with a request for data from an overseas law enforcement or judicial organ.

The PIPL is the latest law to address this important subject. Chapter 3 of the PIPL contains rules concerning the provision of personal information overseas, and, among these rules, are prohibitions regarding the transfer of personal information overseas in response to requests from foreign law enforcement or judicial organs without permission. Tracking similar language contained in the DSL (Article 36), Article 41 of the PIPL provides, in translation: "The PRC processes requests from foreign judicial or law enforcement organs for the provision of personal information stored in the PRC in accordance with treaties, international conventions, and agreements or in accordance with principles of mutual reciprocity. Without approval from competent organs of the PRC, personal information processors must not provide personal information stored in the PRC to overseas judicial or law enforcement organs." As with the DSL, it remains uncertain how these provisions of the PIPL will be implemented in practice.

Looking forward

The PIPL will establish a new comprehensive regulatory framework for personal information protection in China, significantly changing China's current data privacy regulatory landscape. The implementation of a number of provisions under the PIPL remains contingent on the further implementation of rules which are anticipated to be promulgated in the coming months, and requires clarification and guidance from the Chinese regulators. Therefore, we expect that China's data privacy regime will continue to evolve quickly, a fact local and international business operators are now well aware of. In the meantime, it is advisable to start complying with the new law, to the extent clearly set out, for example, prepare for a PIPL data compliance audit.

FOR MORE INFORMATION PLEASE CONTACT

Allen & Overy

Victor Ho
Managing Partner of A&O LLP in Beijing and Shanghai
Registered Foreign Lawyer, Hong Kong
victor.ho@allenovery.com

Richard Qiang
Counsel, Beijing
richard.qiang@allenovery.com

Jane Jiang
Partner, Shanghai
jane.jiang@allenovery.com

Jack Wang
Partner, Shanghai
jack.wang@allenovery.com

Eugene Chen
Registered Foreign Lawyer, Hong Kong
eugene.chen@allenovery.com

Richard Wagner
Registered Foreign Lawyer, Hong Kong
richard.wagner@allenovery.com

Shanghai Lang Yue Law Firm

Melody Wang
Partner, Shanghai and Beijing
melody.wang@allenoveryly.com

Ran Chen
Counsel, Beijing
ran.chen@allenoveryly.com