MAYER | BROWN

1 September 2021

Legal Update

Dawning of a New Era: China's Personal Information Protection Law

On 20 August 2021, China's much anticipated Personal Information Protection Law (PIPL) was passed. The new law will come into force on 1 November 2021. The PIPL, Cybersecurity Law and the new Data Security Law (which came into force on 1 September 2021), now form the main legal framework governing data security and the handling of both personal and non-personal data in China.

The PIPL has often been compared with the EU General Data Protection Regulation (GDPR) and while this statement is largely true there are many points of difference between the two regimes. For example, the cross border transfer restrictions and extra-territorial application of the PIPL are broader than the equivalent provisions in the GDPR. This, as well as some of the key aspects of the PIPL, are discussed below.

Scope and Extra-territorial Effect

The PIPL regulates the processing of personal information of individuals within China. Personal information is defined as any information relating to identified or identifiable natural persons that is recorded by electronic or any other means, but excluding anonymous data.[1]

The law also expressly applies to any processing activities performed outside China, if such activities are:

1. for the purpose of providing products or services to individuals located in China;
2. for the purpose of analysing or evaluating the activities of individuals located in China; or
3. they fall within any other circumstances specified under local laws or regulations.[2]

All data controllers outside of China who engage in such processing activities must establish a dedicated entity or appoint a legal representative in China to be responsible for all matters relating to the processing of personal information under the PIPL.[3] The name and contact details of such local entity or legal representative will need to be provided to the relevant authority.

Whilst on the face of it the extra-territorial scope of the PIPL appears similar to the GDPR, there are some notable differences. Unlike the GDPR, which applies to the "offering" of goods or services (i.e. the targeting criteria), the PIPL applies to the processing of personal information for the purpose of

---

[1] Article 4 of PIPL.

[2] Article 3 of PIPL.

[3] Article 53 of PIPL.

"providing" products or services to individuals in China. In the absence of further clarification, the PIPL has the potential of applying to foreign companies that are not specifically targeting individuals in China and might incidentally provide products or services to them. For example, a foreign company that operates an e-commerce site with global delivery may be caught by the PIPL simply because a customer might be based in China, even though the e-commerce site is not specifically targeting Chinese customers (e.g., it is not a Chinese website nor does it use a <.cn> domain name, etc.). Before the PIPL comes into operation, the local authorities may issue interpretations and measures to provide further clarity on the scope of application of the PIPL.

Data Controller and Data Processor

The responsibility and requirements under the PIPL are mainly imposed on personal information processors (i.e. the equivalent of data controllers under the GDPR). The personal information processor is any organisation or individual that independently determines the purpose and means of processing of personal information (data controller).[4]

Data controllers remain responsible for supervising the entities to whom they have entrusted the processing of personal information (i.e. the equivalent of a data processor under the GDPR) (data processor). The parties must agree on the purpose, period and method of processing and type of personal information covered, as well as the security measures and rights and obligations of both parties. This should be reflected in an agreement between the parties. The data processor cannot further sub-contract the processing of the personal information without the consent of the relevant data controller.[5]

Under Article 59 of the PIPL, data processors are required to adopt necessary measures to protect the personal information entrusted to them in accordance with the PIPL and other relevant laws and regulations, and to assist the data controller to comply with their obligations under the PIPL. Whilst data processors are potentially not directly regulated under the PIPL in the same way as they are under the GDPR, this Article 59 acts as a reminder that data processors may still be directly subject to the data security requirements under China's Cybersecurity Law and Data Security Law.

Grounds for Processing

Under the PIPL, personal information may only be processed if it is for a specific and reasonable purpose, and should be directly related to such purpose. Only the minimum amount of data required to fulfil such purpose should be collected, and the excessive collection of personal information is prohibited.[6] Similar to the GDPR, the PIPL imposes general principles of openness and transparency, legality, legitimacy, necessity and good faith.

The PIPL also sets out the lawful basis for the processing of personal information. Under Article 13 of the PIPL, data controllers can only process personal information if:

1. The data subject has provided their consent;[7]
2. The processing is necessary: (a) for the conclusion or performance of a contract to which the data subject is a party; or (b) to conduct human resources management in accordance with labour rules and regulations established by the employer in accordance with the laws or collective contracts signed under law;[8]

---

[4] Article 73(1) of PIPL.

[5] Article 21 of PIPL.

[6] Article 6 of PIPL.

[7] To be valid, the individual must provide their fully informed, voluntary and explicit consent. Where laws or regulations require separate or written consent, then this must be obtained. See Article 14 of PIPL.

[8] The legal basis of processing in relation to human resources management is a anew legal basis introduced in the final PIPL, which did not appear in the first and second drafts of the PIPL.

3. The processing is necessary for the fulfilment of duties or obligations imposed under laws or regulations;
4. There is a need to respond to public health emergencies or to protect an individual's life, health or property in an emergency situation;
5. The personal information is being processed for the purposes of conducting news reporting, supervising public opinion or other such activities that are in the public interest and the processing is within a reasonable scope;
6. The personal information is already publicly available (either disclosed by the data subject or has otherwise legally disclosed), and the processing is within a reasonable scope and in compliance with the PIPL; or
7. The processing is permitted pursuant to other laws and regulations.

Notably, unlike the GDPR, legitimate interest is not a ground for processing under the PIPL. However, the PIPL does specifically include publicly available information and human resources management as grounds for processing, which are absent from the GDPR.

Regardless of the basis of processing relied on by the data controller, the data controller must still explicitly notify the data subjects beforehand of the purpose of processing, the categories of personal information being handled, the mechanisms in which the data subjects can exercise their rights, and so on.[9] The notification must be accurate, clear and easy to understand. Any changes to the original notice must also be notified to the data subjects.

Separate Consent

If consent is being relied on as the basis of processing, then separate consent must be obtained if:

1. Personal information will be provided by the data controller to a third party;[10]
2. The data controller intends to disclose the personal information publicly;[11]
3. Images and other personal information collected in public areas to safeguard public security (e.g., information collected via CCTV or facial recognition technology) will be used for other purposes;[12]
4. Sensitive personal information will be processed;[13] or
5. Personal information will be transferred outside of China.[14]

What amounts to separate consent has not been defined in the PIPL. It is likely that unbundled and distinct opt-in consent may be required, separate to the general consent collected in relation to the processing of the data subject's personal information.

With regard to sensitive personal information, this is defined as any personal information that once leaked or illegally used could readily result in harm to the dignity of an individual, or the individual's personal safety or security of their property.[15] Examples include biometric identification information, religious beliefs, specially-designated status, medical health information, financial accounts, tracking an individual's location, and personal information of minors under the age of 14.

---

[9] Article 17 and 18 of PIPL.

[10] Article 23 of PIPL.

[11] Article 25 of PIPL.

[12] Article 26 of PIPL.

[13] Article 29 of PIPL. Note that for personal information of minors under the age of 14, the data controller must obtain the consent of the parent or guardian of the minor (Article 31 of PIPL).

[14] Article 39 of PIPL.

[15] Article 28 of PIPL.

Cross-border Data Transfers

In line with the Cybersecurity Law and Data Security Law, the PIPL has strict data localisation and cross-border data transfer requirements. Personal information cannot be transferred out of China, unless it is truly necessary for business or other such requirements, and one of the following conditions are met[16]:

1. A security assessment conducted by the Cyberspace Administration of China (CAC) has been passed;
2. A security certification is obtained, which is conducted by an accredited body in accordance with regulations specified by the CAC;
3. An agreement with the foreign recipient is entered into based on the "standard contract" stipulated by the CAC (still to be issued), which sets out each party's respective rights and obligations, and ensures that the personal information will be protected to the same standard as that provided under the PIPL; or
4. The transfer is in accordance with other laws or regulations or other conditions prescribed by the CAC.

Whilst most entities will likely use the standard contract once issued by the CAC, this option is not available to critical information infrastructure (CII) operators or to entities that process large volumes of personal information. Under Article 40 of the PIPL:

1. Any data controllers that process personal information at a volume exceeding the threshold specified by the CAC (still to be determined); or
2. Any CII operators,

must store all personal information within China, and can only transfer personal information overseas if a security assessment is conducted by the CAC.

The PIPL also provides that if China is a party to any international treaties or agreements, which have terms concerning the provision of personal information out of China, then those terms may be complied with. This opens up the possibility of China entering into agreements with other countries in the future in order to make cross-border data transfers easier, but it is likely that such agreements will still have strict provisions regarding access to data by the Chinese authorities and ensuring protection of the data to the same level as the PIPL.

Before any overseas transfer can take place, data controllers must also:

1. Conduct a privacy impact assessment in relation to the cross-border transfers[17] (records of the risk assessment must be retained for at least three years);[18]
2. Notify the affected data subjects of the foreign recipient's name and certain other specified information;[19] and
3. Where consent is being relied on as the grounds for processing, the data subject's separate consent must be obtained for the transfer.[20]

---

[16] Article 38 of PIPL.

[17] Article 55 of PIPL.

[18] Article 56 of PIPL.

[19] Article 39 of PIPL.

[20] Article 13, 14 and 39 of PIPL.

Providing Personal Information to Foreign Judicial or Law Enforcement Authorities

A major difference to GDPR is the restriction from the provision of personal information stored in China to any foreign judicial or law enforcement agencies, unless prior approval is obtained from the relevant Chinese authority. Chinese authorities will handle any requests from foreign judicial or law enforcement authorities in accordance with any applicable international treaties or agreements, or in accordance with the principle of equality and reciprocity.[21] This is similar to the restriction under the Data Security Law, save that the PIPL only applies to personal information while the Data Security Law applies to all data (which means any record of information in electronic or non-electronic form).

Further, if any country adopts what the Chinese authorities deem to be discriminatory measures against China in relation to personal information protection, it may implement reciprocal measures against them[22].

Automated Decision Making

Data controllers cannot use any automated decision-making that will result in unreasonable differential treatment of data subjects in terms of price or other transactional terms.[23]

It is believed that this provision was added to tackle increasing concerns about big data-enabled discriminatory pricing, which refers to the use of big data to evaluate consumers' willingness to pay and charge different prices for the same product based on their established preference and payment conditions. This is an increasingly common practice, and China has been ramping up efforts to grapple with it; for example, the Anti-Monopoly Guidelines for the Platform Economy issued in February 2021 took aim at such discriminatory treatment. On 27 August 2021, the CAC issued the draft Internet Information Service Algorithm Recommendation Management Regulations, which goes one step further and is intended to regulate the use of algorithms by companies to provide recommendations to users.

Data controllers are required to carry out a privacy impact assessment before using personal information for automated decision-making.[24] They need to be transparent about how decisions are made, and are responsible for ensuring that the results are fair and impartial. In certain circumstances, the data subjects also have the right to request an explanation on how the automated-decision was made and to refuse / opt-out of the use of automated decision making.[25]

Rights of Data Subjects

In line with the GDPR and international practice, the PIPL further strengthens a data subject's rights by introducing the right to data portability, enabling data subjects to request a data controller to transfer their personal information to another, so long as the transfer meets the requirements established by the CAC. There is no certainty yet as to what these requirements may be. Other rights granted to data subjects under the PIPL are substantially similar to those under the GDPR, such as the right to access and correct data, right to erasure, the right to object and restrict the processing of data, the right to withdraw consent, and so on. Further guidance will need to be provided on how data controllers must comply in practice with the exercise of these data subject rights.

---

[21] Article 41 of PIPL.

[22] Article 43 of the Second Draft PIPL.

[23] Article 24 of PIPL.

[24] Article 55 of PIPL.

[25] Article 24 of PIPL.

Additionally, data subjects are entitled to seek recourse from the courts in the event that their requests to exercise their rights under the PIPL are rejected by a data controller. A data subject's rights are also extended to allow a deceased person's next of kin to access, copy, correct, and delete the deceased person's personal information for their lawful and legitimate interests.

Obligations on Large Internet Platform Service Providers

Additional obligations are placed on data controllers that provide important internet platform services to a large number of users and/or who operate complex business models, including the need to establish an independent body (mainly consisting of external personnel) to oversee the data controller's processing activities, and to stop providing services to those who offer products or services via the data controller's platform, who are in serious violation of the relevant laws and regulations governing personal information.

It is still unclear what would constitute a substantial number of users or complex business models. Further measures or regulations will be required to shed light on this requirement.

Data Breach Notification

Under Article 57 of the PIPL, if any leak, tampering or loss of personal information has or may have occurred, the data controller must immediately deploy remedial measures and notify the relevant local authorities and data subjects. It is important to note that this notification obligation arises even if the data incident is just a mere possibility (i.e. "may" have occurred). Currently, there is no clarification as to the degree of likelihood that a data incident may have occurred in order for the notification obligation to be triggered, e.g., reasonably likely or mere suspicion.

The notification obligation also applies even if there has been no data leak – if the personal information has been altered or tampered with, then this will require notification.

Data controllers can elect not to notify affected data subjects, if they determine that they have taken measures which effectively prevent the data subjects from suffering any harm from the data incident. However, this decision can be overridden by the relevant authority, who can still decide that notification to the data subjects is required.

Unlike the GDPR, the PIPL does not specify an exact deadline or time limit within which to notify the relevant authorities or data subjects. This may change once further measures or regulations are issued relating to the implementation of the PIPL.

Data controllers should also note that unlike the GDPR, there is no obligation under the PIPL for data processors to notify their data controllers in the event of any data incident. It is therefore vital that such obligation is incorporated in any data processing agreement between the parties, as the data controller will still remain liable for any failure to notify the relevant authorities or data subjects.

Penalties

Breach of the PIPL can incur administrative fines of up to RMB 50 million or 5% of the data controller's annual revenue in the last year. Unlike the GDPR, it is unclear whether this revenue is calculated based on the data controller's global revenue, or only the revenue generated in China.

In addition to fines, other penalties include rectification orders, warnings, confiscation of illegal gains, suspension or cessation of services, cessation of operations or revocation of permits or business licenses, or entering the data controller on a credit list. The local authorities also have the specific power to take steps against any foreign organisation that is seen as engaging in processing activities that harm the rights and interests of Chinese citizens or which endanger national security or public interest, such as

prohibiting Chinese entities from providing any personal information to them[26].

Persons-in-charge and other directly responsible personnel may also be held personally liable and fined or prohibited from acting as directors, supervisors, senior managers or personal information protection officers.

Takeaways

While the PIPL resembles the GDPR, the PIPL appears to be one of the world's most stringent personal data protection laws and its far-reaching effect may make it more challenging for companies, especially those with global operations, to ensure compliance. As the PIPL will soon come into effect, companies are encouraged to review and update their privacy and compliance policies, align with suppliers, and have proper technical solutions integrated into their operational system in order to satisfy the requirements under PIPL. A sharp eye should also be kept out for any guidelines, measures or regulations likely to be issued by the Chinese authorities to flesh out the implementation of different aspects of the PIPL.

The authors would like to thank Sophie Huang, Intellectual Property Officer at Mayer Brown, for her assistance with this Legal Update.

Contact Us

For more information about the topics raised in this Legal Update, please contact any of the following lawyers.

Gabriela Kennedy
+852 2843 2380
gabriela.kennedy@mayerbrown.com

Karen Lee
+65 6922 2244
karen.hf.lee@mayerbrown.com

[26] Article 42 of PIPL.

Mayer Brown is a distinctively global law firm, uniquely positioned to advise the world's leading companies and financial institutions on their most complex deals and disputes. With extensive reach across four continents, we are th e only integrated law firm in the world with approximately 200 lawyers in each of the world's three largest financial centers—New York, London and Hong Kong—the backbone of the global economy. We have deep experience in high-stakes litigation and complex transactions across industry sectors, including our signature strength, the global financial services industry. Our diverse teams of lawyers are recognized by our clients as strategic partners with deep commercial instincts and a commitment to creatively anticipating their needs and delivering excellence in everything we do. Our "one-firm" culture—seamless and integrated across all practices and regions—ensures that our clients receive the best of our knowledge and experience.

Please visit mayerbrown.com for comprehensive contact information for all Mayer Brown offices.