Regional

China Enters a New Era of Personal Information Protection

Introduction

On 20 August 2021, the 13th National People's Congress of the People's Republic of China ("**PRC**") passed the Personal Information Protection Law (中华人民共和国个人信息保护法)[1] ("**PIPL**"), which will take effect on 1 November 2021. The PIPL, together with the Cybersecurity Law which came into effect on 1 June 2017, and the Data Security Law which came into effect on 1 September 2021 (see our client update here), form the core tenets of cybersecurity and data protection in China.

Compared with the second draft of the law, the enacted draft of the PIPL introduced several important new rules that will have a significant impact on how Personal Information Processors ("**PIPs**") such as Internet and social media giants may handle and process Personal Information. This update will examine some of the key highlights of the PIPL.

Key Highlights

Extraterritoriality

The PIPL applies to Personal Information processing activities within the territory of the PRC. In addition, it is also applicable to Personal Information processing activities outside the territory of the PRC, if such activities relate to:

(1) The provision of goods or services to natural persons within the territory of the PRC,

(2) the analysis and evaluation of the actions of natural persons within the territory of the PRC, and

(3) other situations provided for by laws or administrative regulations.

Definitions of relevant terms

According to the PIPL, "**Personal Information**" means all kinds of information related to *identified* or *identifiable* natural persons that are electronically or otherwise recorded, but excluding information which

[1] Full text of the PIPL may be found here.

has been anonymised. It is noteworthy that "anonymisation (匿名化)" is different from "de-identification (去标识化)". Unlike the anonymised information, de-identified information is still Personal Information

"**Processing**" includes, amongst others, the collection, storage, use, processing, transmission, provision, disclosure and deletion of Personal Information.

"**Personal Information Processor**" or "**PIP**" means the organisation or person processing Personal Information who can determine the purpose and method of processing.

Bases for processing

Compared to the sole base for processing Personal Information under the PRC Cybersecurity Law, which is the data subject's consent, the PIPL for the first time extends the bases to include the following:

(1) The individual had provided his/her consent;

(2) It is necessary for the conclusion or performance of a contract which the individual is a party to, or it is necessary for the implementation of human resource management in accordance with the employment policies developed in accordance with the law and the collective employment contracts signed in accordance with the law;

(3) It is necessary for the performance of lawful duties or obligations;

(4) It is necessary to respond to public health incidents, or to protect the lives, health and property of natural persons in an emergency;

(5) Personal Information is processed within a reasonable scope for the purpose of carrying out news reporting or public opinion oversight in the interest of the public;

(6) Personal Information that had been disclosed by the individual or is otherwise already lawfully disclosed is processed within a reasonable scope in accordance with the PIPL; or

(7) Any other situations provided for by laws or administrative regulations.

Separate or written consent

The PIPL for the first time requires a separate or written consent from the individual to be obtained under one of the following circumstances:

(1) Separate consent is required when one PIP transfers the individual's Personal Information processed by it to another PIP or outside China (Article 23 and Article 39);

(2) Separate consent is required when a PIP publicises the individual's Personal Information processed by it (Article 25);

(3) Separate consent is required when the individual's image or identification information collected by the data collection equipment installed in the public area is to be used for purposes other than public security purposes (Article 26); and

(4) Processing of sensitive personal information requires separate consent from the individual, and if required by the laws and administrative regulations, a written consent should be obtained (Article 29).

Data Minimisation Principle

The PIPL sets out various principles which PIPs must comply with when processing Personal Information. Such principles include:

(1) **Legality, legitimacy, necessity, and good faith**. The PIPL provides that Personal Information must be processed in accordance with the principles of legality, legitimacy, necessity, and good faith, and shall not be processed through means such as misleading, fraud, or coercion (Article 5).

(2) **Necessity / Data Minimisation**. The PIPL provides that the processing of Personal Information must be for a clear and reasonable purpose, relate directly to that purpose, and adopt the method of processing which will have the smallest impact on the individual's rights and interests. Further, the Personal Information to be collected must be limited to the smallest scope necessary for achieving the purpose of processing, and not be excessive (Article 6).

Compared to the second draft, Article 6 of the PIPL now makes clear that the data minimisation principle is also applicable to the *collection* of Personal Information, which must be limited to the smallest scope that is needed to fulfil the purpose of processing, and excessive collection of Personal Information is not permitted.

(3) **Openness and Transparency**. The PIPL provides that Personal Information must be processed in accordance with the principles of openness and transparency, and the rules for the processing of Personal Information must be disclosed, setting out the purpose, method and scope of processing (Article 7).

(4) **Accuracy**. The PIPL provides that PIPs should ensure the quality of the Personal Information being processed, to avoid adversely impacting an individual's rights and interests due to inaccurate or incomplete Personal Information (Article 8).

Retention of Personal Information

The PIPL provides that unless otherwise stipulated under applicable laws or regulations, the retention period for Personal Information must be the shortest time necessary for achieving the purpose of processing (Article 19). However, there is no clear definition as to what constitutes the shortest time necessary for achieving the purpose of processing either under the PIPL or other laws, regulations and standards.

Operationally, it is advisable that PIPs shall therefore keep track of the Personal Information that they have collected and ensure that they can justify why they need to retain Personal Information for such a period. When the purpose for which such Personal Information was collected has been achieved, Personal Information should be promptly anonymised or deleted.

Automated decision making

Article 24 of the PIPL now clarifies that PIPs using Personal Information for automated decision making ("**ADM**") must ensure the transparency of the decision-making process and that the results are fair and equitable, and must not unreasonably discriminate against individuals on trading conditions such as trading prices.

In addition, where ADM is used to push information to individuals, or conduct commercial marketing, individuals should be provided with either the option to not be targeted based on specific personal characteristics, or a convenient method of opting-out.

In recent years, there have been stories of e-commerce platforms using the insights they have gained on existing customers (such as their spending habits, spending power, personal preferences, and price sensitivities, amongst others) through data profiling to charge these customers a higher price for the same goods and services, with the knowledge that such inflated prices would still be acceptable to the customers. Such practices are also known as "大数据杀熟" in the PRC, literally meaning "using big data to 'exploit' or 'kill' existing customers". It is envisaged that Article 24 will go a long way in curbing such practices.

Sensitive Personal Information

Article 28 of the PIPL now makes clear that *biometric information*, *location tracking information* and *Personal Information of minors under the age of 14* are considered to be sensitive Personal Information,

alongside an individual's religious faith, specific identity, medical and health information, and financial status. PIPs may only process sensitive Personal Information for specific purposes where fully necessary, and must implement strict protective measures when doing so. In addition, PIPs are required to establish special rules for the processing of Personal Information of minors under the age of 14.

Cross border provision of Personal Information

Article 38 of the PIPL provides that the transfer of Personal Information out of China for business or other necessity shall fulfil at least one of the following conditions:

(1) Passing a safety assessment by the national cyberspace authority;

(2) Obtaining personal information protection accreditation from a professional agency appointed by the national cyberspace authority;

(3) Entering into a contract with the overseas recipient in a standard form formulated by the national cyberspace authority; or

(4) Any other conditions provided for under laws and regulations, or those set by the national cyberspace authority.

Except for Designated PIPs (as defined below), Item (3) above would be the most cost-effective option and may be an ideal option for, in particular, intra-group data sharing. As of the date of this legal update, the Cyberspace Administration of China ("**CAC**") has not yet published any template of such a standard contract.

In addition to the above, Article 38 of the PIPL now makes clear that where PIPs transfer Personal Information overseas, they must employ necessary measures to ensure that the overseas recipient's Personal Information processing activities satisfy the protection standards accorded to Personal Information under the PIPL.

Notwithstanding the options provided under Article 38, it is noteworthy that Critical Information Infrastructure Operators ("**CIIOs**") and PIPs that are processing Personal Information above a certain threshold[2] as determined by the CAC ("**Designated PIPs**") must store the Personal Information that they have collected or generated in the PRC within the territory of the PRC and must pass a security assessment administered by the CAC if it is necessary for such entities to transfer Personal Information out of the territory of the PRC.

[2] As of the date of this update, the CAC has not specified the said threshold.

Requests by foreign judicial or law enforcement agencies

Article 41 of the PIPL now makes clear that requests for Personal Information by foreign justice or law enforcement bodies must be made to competent PRC state organs, where such requests will be handled based on relevant laws and international treaties or agreements concluded or participated in by the PRC, or in accordance with the principle of reciprocity. On the other hand, PIPs are strictly prohibited from providing Personal Information stored within the PRC to foreign justice or law enforcement bodies without the permission of the competent state organs, which is reminiscent of Article 36 of the Data Security Law which just came into effect on 1st September 2021. This will pose a significant compliance issue for organisations that are storing Personal Information within the PRC, if they are also subject to legal obligations to disclose Personal Information to judicial or law enforcement agencies in their own jurisdictions.

Data subjects' rights

The PIPL recognises various rights of individuals in relation to his/her Personal Information, including:

- Right to withdraw consent (Article 15);
- Right to object to ADM (Article 24);
- Right to information (Article 44);
- Right to restrict or reject the processing of Personal Information (Article 44);
- Right to access and make copies of his/her Personal Information (Article 45);
- Right to data portability (Article 45);
- Right to correction or amendment of Personal Information where the Personal Information is inaccurate or incomplete (Article 46);
- Right to request deletion of Personal Information (Article 47); and
- Right to the explanation of the rules of Personal Information processing (Article 48).

Compared to the second draft, the PIPL also introduced a new right to data portability for individuals which will make it easier to transmit Personal Information to another data platform. Article 45 of the PIPL provides that where individuals request for their Personal Information to be transferred to designated

PIPs, and where such requests satisfy the conditions imposed by the state Internet information departments, PIPs shall provide channels for such transfer.

Article 50 also requires PIPs to establish a *convenient* mechanism for accepting and addressing requests from individuals to exercise their rights. Where a PIP had refused to accede to an individuals' request to exercise his or her rights, Article 50 also now clarifies that the individual may commence legal proceedings in the people's courts in accordance with the law.

Obligations of PIPs

A) Measures to ensure compliance and protection

PIPs are required to adopt measures to ensure the Personal Information processing activities comply with applicable laws and regulations, and prevent unauthorised access, leaking, alteration and loss of Personal Information, having regard to, amongst others, the purpose and method of processing, the types of Personal Information to be processed, and the impact and potential risks to individuals' rights and interests (Article 51). Such measures include:

(1) Formulate internal security management systems and operating procedures;

(2) Categorise and manage Personal Information based on their categories;

(3) Employ technical security measures such as encryption and de-identification of Personal Information;

(4) Impose access restrictions on individuals appointed to process Personal Information;

(5) Conduct security education and training for employees periodically;

(6) Formulate and implement Personal Information security incident response plans; and

(7) Any other measures required by applicable laws and regulations.

PIPs are also required to conduct periodic audits of whether their Personal Information processing activities are in compliance with applicable laws and regulations (Article 54).

B) Important Internet Service Providers

Article 58 of the PIPL has been amended to require PIPs that (a) provide important Internet platform services, (b) have a larger number of users, or (c) operate under complex operational models

(collectively "**Important Internet Service Providers**") must:

(1) Establish comprehensive Personal Information protection and compliance institutional system in accordance with state regulations, and establish an independent organisation comprising primarily of external members to carry out oversight;

(2) Comply with principles of openness, fairness, and equity when drafting platform rules, and make clear its standards for processing Personal Information by products or services on the platform and protection of Personal Information;

(3) Stop providing services to products or service providers on the platform that handle Personal Information in serious violation of laws and administrative regulations; and

(4) Periodically publish social responsibility reports on the protection of Personal Information, and accept societal oversight.

It is worth noting that the concept of Important Internet Service Providers is only mentioned once in the PIPL, and the PIPL also does not provide further clarifications on what constitutes "important Internet platform services", "a large number of users", or "complex operational models", although the reference to "providers of goods or services" would suggest that many of the renowned large Internet platform players (particular those that sustain an entire ecosystem) may be caught under this provision. It is expected that these issues will be clarified by further subsidiary legislation to be released in the future.

C) Appointment of DPOs

The PIPL provides that Designated PIPs must appoint a person in charge of Personal Information protection ("**DPO**") who shall be responsible for overseeing Personal Information processing activities and implementation of protective measures (Article 52).

The PIPL further provides that those overseas PIPs who are subject to the PIPL (*please refer to the section on "Extraterritoriality" in this legal update*) must establish a special institution or appoint representatives within the PRC for handling matters relating to the protection of Personal Information, and report the name and contact details of such institution or representative to the relevant authorities. (Article 53). It awaits further clarifications from the authority as to whether the offshore parent company which processes the Personal Information collected by its Chinese subsidiaries within China, the quantity of which data does not meet the threshold set by the CAC, are required to establish such a special institution or appoint such representatives within the PRC, and report the contact information to the relevant authorities.

Regional

Enforcement

Where Personal Information is processed in violation of the PIPL, or where Personal Information is processed without adherence to the Personal Information protection obligations stipulated under the PIPL, the penalties that may be imposed against the PIPL include:

- Issuance of an order for rectification;
- Issuance of a warning;
- Confiscation of illegal gains;
- Issuance of an order for suspension or cessation of service by the application that is illegally processing Personal Information;
- Imposition of financial penalties against the PIP (up to RMB 1 million) if it refuses to rectify its breach; and
- Imposition of financial penalties on the DPO or other directly liable individuals (above RMB 10,000 up to RMB 100,000).

Where the breach is particularly egregious, in addition to the penalties listed above, the PIP and DPO or other directly liable individuals may be subject to additional penalties, including:

- Imposition of financial penalties against the PIP (up to RMB 50 million or 5% of the PIP's turnover in the previous year);
- Issuance of an order for suspension of the relevant business, or the cessation of the relevant business for an overhaul;
- Revocation of operating permits or business licenses of the PIP;
- Imposition of financial penalties on the DPO or other directly liable individuals (above RMB 100,000 up to RMB 1 million); and
- Prohibiting the DPO or other directly liable individuals from holding office as directors, supervisors, senior managers or DPOs for a period of time.

Conclusion

The PIPL marks a significant step in China's refinement of its Personal Information protection regime. On one hand, it further strengthens individuals' autonomy and protection for individuals' rights. On the other hand, it also steps up regulatory oversight on PIPs.

In particular, the articles addressing:

- the data minimisation principle;
- the prohibition against the use of ADM to unfairly discriminate against individuals; and
- increased emphasis on individual autonomy, and heightened obligations on PIPs providing important Internet platform services

will all have significant and far-reaching impacts on PIPs, especially key Internet and social media giants holding a significant amount of Personal Information.

With the new PIPL being scheduled to come into effect on 1 November 2021, PIPs should take this time to review their internal processes to ensure that they will be compliant with the new Personal Information protection regime. The interplay between the PIPL and other data-related laws and regulations passed recently should also be closely examined and monitored.

In light of the recent legislative changes, businesses carrying out data processing activities in China should ensure that they establish and adopt robust data protection frameworks internally to ensure compliance with the new laws. In particular, businesses should:

(1) Ensure that they establish and implement adequate data handling and protection policies to provide employees with adequate guidance on how to handle and use data in compliance with the laws;

(2) Adopt a security-by-design approach in their data processing activities;

(3) Conduct regular internal and external audits to ensure existing systems and processes are sufficiently robust to fulfil the legal requirements; and

(4) Regularly conduct training for employees to ensure they keep updated with the best practices.

Our data protection teams can most certainly assist with the above.

Regional

Disclaimer: *Rajah & Tann Singapore LLP Shanghai Representative Office is a foreign law firm licenced by the Ministry of Justice of the People's Republic of China (the "**PRC**"). As a foreign law firm, we may not issue opinions on matters of PRC law. Any views we express in relation to PRC laws and regulations for this matter are based on our knowledge and understanding gained from our handling of PRC-related matters and through our own research, and also from our consultations with PRC lawyers. Therefore, such views do not constitute (and should not be taken as) opinion or advice on PRC laws and regulations.*

Contacts

Benjamin Cheong
Partner, Rajah & Tann Singapore LLP

T +65 6232 0738

benjamin.cheong@rajahtann.com

Chen Xi
Partner (Foreign Lawyer),
Rajah & Tann Singapore LLP

T +65 6232 0158

chen.xi@rajahtann.com

Linda Qiao
Senior International Counsel,
Rajah & Tann Shanghai Representative Office

T +86 21 6120 8818

linda.qiao@rajahtann.com

Chia Lee Fong
Chief Representative,
Rajah & Tann Shanghai Representative Office;
Partner (Foreign Lawyer),
Rajah & Tann Singapore LLP

T +86 21 6120 8818

lee.fong.chia@rajahtann.com

Please feel free to also contact Knowledge and Risk Management at eOASIS@rajahtann.com

Our Regional Contacts

RAJAH & TANN | *Singapore*
Rajah & Tann Singapore LLP
T +65 6535 3600
sg.rajahtannasia.com

R&T SOK & HENG | *Cambodia*
R&T Sok & Heng Law Office
T +855 23 963 112 / 113
F +855 23 963 116
kh.rajahtannasia.com

RAJAH & TANN 立杰上海
SHANGHAI REPRESENTATIVE OFFICE | *China*
Rajah & Tann Singapore LLP
Shanghai Representative Office
T +86 21 6120 8818
F +86 21 6120 8820
cn.rajahtannasia.com

ASSEGAF HAMZAH & PARTNERS | *Indonesia*
Assegaf Hamzah & Partners

Jakarta Office
T +62 21 2555 7800
F +62 21 2555 7899

Surabaya Office
T +62 31 5116 4550
F +62 31 5116 4560
www.ahp.co.id

RAJAH & TANN | *Lao PDR*
Rajah & Tann (Laos) Co., Ltd.
T +856 21 454 239
F +856 21 285 261
la.rajahtannasia.com

CHRISTOPHER & LEE ONG | *Malaysia*
Christopher & Lee Ong
T +60 3 2273 1919
F +60 3 2273 8310
www.christopherleeong.com

RAJAH & TANN | *Myanmar*
Rajah & Tann Myanmar Company Limited
T +95 1 9345 343 / +95 1 9345 346
F +95 1 9345 348
mm.rajahtannasia.com

GATMAYTAN YAP PATACSIL
GUTIERREZ & PROTACIO (C&G LAW) | *Philippines*
Gatmaytan Yap Patacsil Gutierrez & Protacio (C&G Law)
T +632 8894 0377 to 79 / +632 8894 4931 to 32
F +632 8552 1977 to 78
www.cagatlaw.com

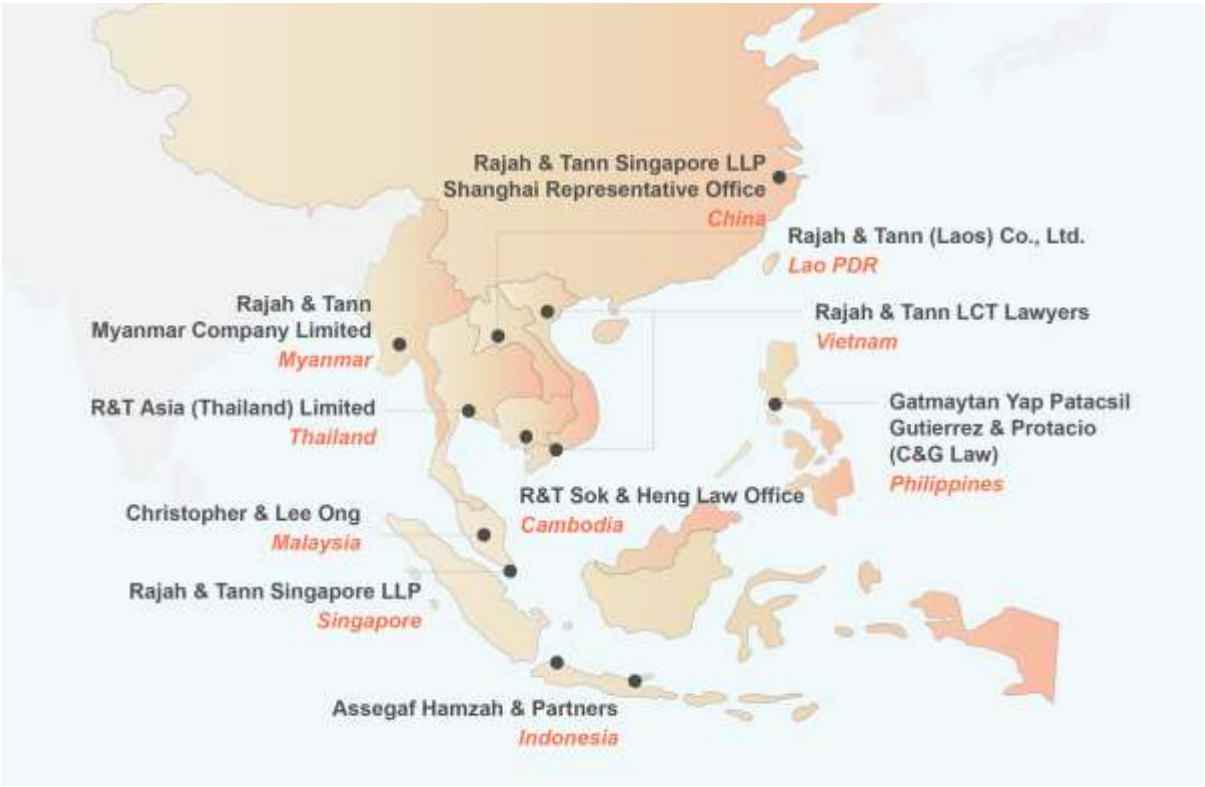
RAJAH & TANN | *Thailand*
R&T Asia (Thailand) Limited
T +66 2 656 1991
F +66 2 656 0833
th.rajahtannasia.com

RAJAH & TANN LCT LAWYERS | *Vietnam*
Rajah & Tann LCT Lawyers

Ho Chi Minh City Office
T +84 28 3821 2382 / +84 28 3821 2673
F +84 28 3520 8206

Hanoi Office
T +84 24 3267 6127
F +84 24 3267 6128
www.rajahtannlct.com

Our Regional Presence



Rajah & Tann Singapore LLP is one of the largest full-service law firms in Singapore, providing high quality advice to an impressive list of clients. We place strong emphasis on promptness, accessibility and reliability in dealing with clients. At the same time, the firm strives towards a practical yet creative approach in dealing with business and commercial problems. As the Singapore member firm of the Lex Mundi Network, we are able to offer access to excellent legal expertise in more than 100 countries.

Rajah & Tann Singapore LLP is part of Rajah & Tann Asia, a network of local law firms in Cambodia, China, Indonesia, Lao PDR, Malaysia, Myanmar, the Philippines, Singapore, Thailand and Vietnam. Our Asian network also includes regional desks focused on Brunei, Japan and South Asia.