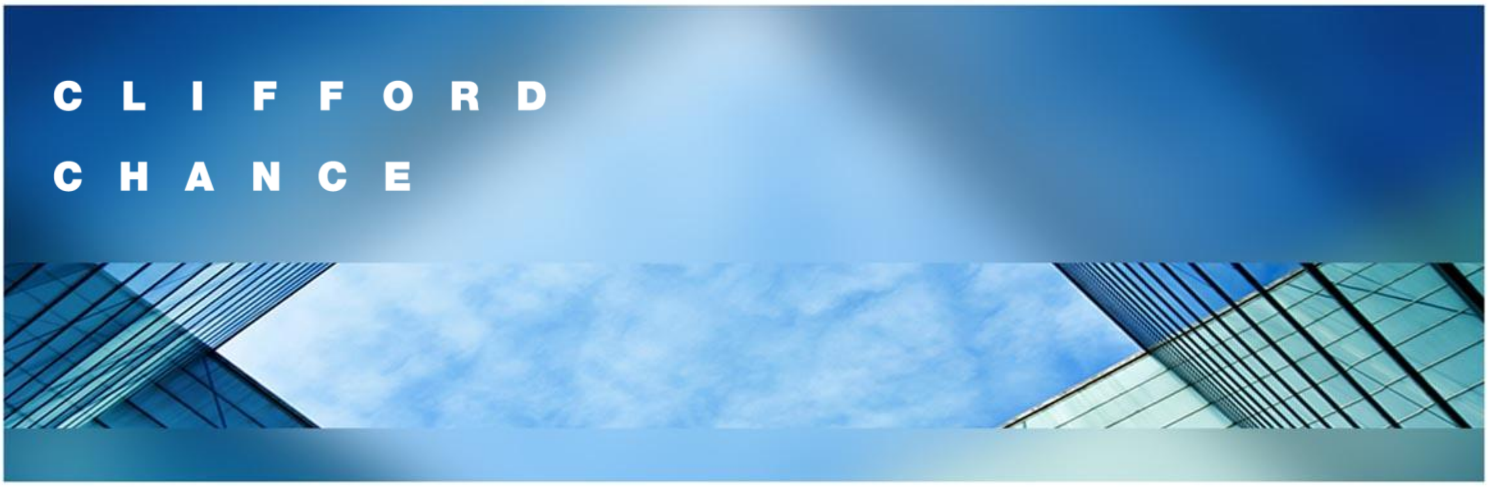

PRC PASSES MILESTONE LEGISLATION FOR PERSONAL INFORMATION PROTECTION

On 20 August 2021, the Standing Committee of the National People's Congress of the PRC passed the *PRC Personal Information Protection Law* (the **PIPL**), which will take effect on 1 November 2021. This is the most comprehensive personal information protection law enacted in the PRC so far. It will form a core component of the PRC's legal framework governing data, alongside the Cybersecurity Law and the recently enacted Data Security Law.

The PIPL marks a major milestone in the maturation of the PRC's data privacy regime. Although in many respects the PIPL echoes other personal data protection laws internationally, such as the European Union's General Data Protection Regulation (**GDPR**), multinational companies will need to be mindful of important differences when considering their compliance processes and controls.

Key points

- The PIPL is a major landmark in the regulation of personal information in the PRC and puts in place a comprehensive data privacy regime.
- Many key concepts and rules are similar to those seen internationally in privacy regulations, especially the GDPR, although there are significant differences in the detail.
- The PIPL imposes restrictions on the export of data in certain circumstances, especially with respect to critical information infrastructure operators (CIIOs) and large-scale data operators.
- A number of important issues will only be clarified through secondary implementing legislations.

Scope of the PIPL

The potential application of the PIPL is broad. All information recorded electronically or by other means, that is related to identified or identifiable natural persons is considered personal information (**PI**) and processing of PI includes the collection, storage, use, editing, transmission, provision, publishing and deletion of PI. Anonymised data, (*i.e.*, data that has been processed to the extent that it is impossible to identify a specific person and such person's identify cannot restored) is excluded from the definition of PI altogether. However, de-identified data, defined as data that has been processed to render it impossible to identify a specific person from that data set alone, without additional data, may still constitute PI and thus be subject to the relevant requirements.

In terms of scope of application, the PIPL applies to processing of PI that:

i. takes place in the PRC; or

ii. is conducted outside of the PRC, to the extent such activities are carried out to process the PI of persons within the PRC, and such processing is:

   a) for the purpose of providing products or services to persons in the PRC;

   b) to analyse or assess behaviours of persons in the PRC; or

c) otherwise required by relevant laws and administrative regulations.

Overseas companies subject to the PIPL will be required to establish a dedicated entity or appoint a representative within the PRC that will be responsible for matters related to their PI processing. The details of such representatives will need to be reported to the relevant regulatory authorities in charge of PI protection in the PRC.

Legal Basis for PI Processing

Businesses that have operations in the PRC or serve customers or otherwise collect and process data relating to persons in the PRC will want to carefully consider whether they are subject to the PIPL and what compliance measures they will need to put in place or update.

Do they process PI?

The first question is whether the business processes data that constitutes PI and is therefore subject to the PIPL. Given the broad definition of PI, this will apply to many companies with China-facing operations. Note that the PIPL, unlike some privacy regimes, does not include any express carve-outs for business contact information, so even B2B data can potentially be caught where it includes references to identifiable individuals.

Is there a legal basis for PI processing?

If business intends to process PI, it should consider on what grounds recognised by the PIPL it can carry out such processing. The PIPL provides the following seven legal grounds for processing PI:

i. having obtained the individual's consent;

ii. necessity for the conclusion or performance of any contract to which the relevant data subject is a party or human resource administration in accordance with the employment policies formulated in accordance with laws and regulations or lawfully concluded collective employment contracts;

iii. necessity for performing statutory duties or obligations;

iv. necessity for responding to public health incidents or for the protection of personal and property security in the case of an emergency;

v. media reporting and whistleblowing for public interests, subject to a reasonable scope;

vi. processing PI that is disclosed publicly by the data subject or through other legal channels, subject to a reasonable scope; and

vii. other scenarios provided by PRC laws and administrative regulations.

Compared with the Cybersecurity Law, which provided for consent as the sole basis for PI processing, the PIPL provides more flexibility by providing six additional grounds for processing. While these may be helpful to operators, the scope of "statutory duties or obligations" (ground (iii) above) and what exactly will constitute a "reasonable scope" (grounds (v) and (vi)) will need to be further clarified. We expect that subsidiary legislation and regulations under the PIPL will provide further clarity on these issues. Note also that establishing whether processing is necessary "for the conclusion or performance of a contract" (ground (ii)) may also raise issues as to whether the data subject has duly given consent, either express or implied, when entering into the relevant contract – so this ground may also ultimately boil down to a question of consent.

The PIPL allows less room than under previous legislation for operators to rely on the implied consent of data subjects. It adopts a stricter standard of consent than the Cybersecurity Law: under the PIPL, the data subject should be sufficiently informed, the consent should be freely given and should be capable of being withdrawn, and a convenient way of withdrawing consent must be provided. In addition, separate consent is required for processing sensitive PI (*i.e.*, PI the leakage or illegal use of which will cause harm to human dignity, or to personal or property security of the data subject – see further below), when sharing PI with other processors, when publishing PI or when exporting PI. The specifics of how such separate consent can be validly obtained will be important to ensuring compliance with these new requirements and operators may need to be prepared to revisit the detail of their onboarding and acceptance processes.

In what capacity does processor carry out the PI processing?

Under the PIPL, "PI Processor" refers to an organisation or individual that independently determines the purpose and method of PI processing. To readers familiar with GDPR terminology, note that "PI Processor" as used in translations of the PIPL is substantially equivalent to the GDPR concept of "data controller" – and not that of "data processor", which finds its PIPL equivalent in the concept of "Entrusted Person" (see below). PI Processors that jointly determine the purpose and method of PI processing shall agree on their respective rights and obligations, but such arrangement will not affect the data subject's ability to exercise his or her rights against either of them. Where joint PI Processors cause any damage to the data subject, they will bear joint and several liability.

An "**Entrusted Person**" is a person to which the processing of PI is delegated. A key difference between a PI Processor and an Entrusted Person is that when acting in the capacity of an Entrusted Person, the relevant operator may only act in accordance with the agreed terms under the entrustment contract. The PI Processor is required to provide the contact details of the Entrusted Person to the data subjects, so that the data subjects can conveniently exercise their rights granted under the PIPL vis-à-vis the Entrusted Person. This rule requires PI Processors to supervise downstream delegating processing. The PIPL also requires the Entrusted Person to obtain the consent of the relevant data subject if it proposes to process PI for a purpose or in a manner that deviates from the entrustment arrangement, i.e. in such cases the Entrusted Person will effectively become a PI Processor or a joint PI Processor in its own right.

Overall, by distinguishing the roles of PI Processor and Entrusted Person, the PIPL aims to provide data subjects with full visibility on the flow of their PI with respect to delegated processing, to ensure they are able to exercise their rights over that PI.

Exporting PI

The PIPL provides four bases on which PI can be transferred outside the PRC:

i. passing a security assessment organised by the relevant cybersecurity administration body;

ii. having obtained the PI protection verification by specialised institutions recognised by the cyberspace administration;

iii. having executed a standard form data contract formulated by the cyberspace administration with the offshore data recipient; or

iv. pursuant to other specific provisions under laws, administrative regulations and applicable cyberspace regulations.

As of the date of the publication of this briefing, the form of the standard data contracts referred to in basis (iii) above has not yet been issued. This approved form of contract is expected to provide a convenient basis similar to the standard contractual clauses under the GDPR and operators will be keenly monitoring its adoption.

The export of PI will trigger the following requirements, the application of which is irrespective of the amount of PI being exported:

i. **equivalent protection**: the PI Processor must take measures to ensure the processing activities conducted by the offshore data recipient will comply with the same level of PI protection as provided under the PIPL;

ii. **separate consent**: separate consent from the data subject is required. Based on the plain reading of the law, this requirement applies regardless of whether consent is the legal ground for the PI Processor to collect PI in the first place;

iii. **disclosure of information**: the PI Processor must inform a data subject of the name and contact information of the overseas PI recipient, the purpose and methods of processing, type of PI concerned and procedures for the data subject to exercise his or her rights;

iv. **blacklist**: the cybersecurity administration may formulate a list of entities to which PI export is prohibited or restricted; and

v. **self-assessment**: prior to export, a data exporter needs to conduct a self-assessment prior to the export on the potential impact on protection of the PI and the rights of the data subject. The assessment record needs to be retained for at least 3 years.

Data localisation requirements apply to critical information infrastructure operators (**CIIOs**) and PI Processors when the amount of PI processed reaches a certain scale. The concept of CIIO appeared in the Cybersecurity Law of 2016, but its definition does not receive any further elucidation in the PIPL – although guidance on CIIO designations has been provided in other instruments. Regarding the threshold amount for the second criterion, a proposed amendment to the Administrative Measures for Cybersecurity Review provides that operators processing more than one million users' information will trigger the threshold for additional approval for offshore listing, although at this stage this threshold is indicative only as the amendment has not yet been adopted.

Similar to the Data Security Law and other recent legislation, the PIPL prohibits PI Processors from providing PI stored in China to foreign judicial or enforcement authorities without proper consent from competent PRC authorities.

Processing Sensitive PI

Sensitive PI is defined as PI, the leakage or illegal use of which could cause harm to human dignity or personal or property security. The PIPL includes a non-exhaustive list of categories of sensitive PI, which includes information on race, ethnicity, religious beliefs, individual biometric features, medical health, financial accounts and individual location tracking.

Sensitive PI is afforded a higher level of protection. In particular:

i. sensitive PI can only be processed if there is a specified purpose, the processing is sufficiently necessary and it is conducted under strict protection measures;

ii. separate consent must be obtained in order to process sensitive PI (and such consent must be in writing if separately required by law); and

iii. PI Processors must conduct a self-assessment prior to processing sensitive PI.

Note the PIPL does not provide any safe harbour for sensitive PI processing that is incidental or occasional to the ordinary business of an entity or processed on a limited scale.

It is also noteworthy that the PI of children under the age of 14, is classified as sensitive PI and the consent of parents or other legal guardians is required in order to process PI of children. PI Processors must formulate separate processing rules for children's PI. Operators that may collect and process children's data will want to give particular consideration to the processes they will need to put in place to ascertain and verify the age of data subjects, to ensure they are able to identify children's PI and ensure it is processed on a sensitive PI basis.

The PIPL clarifies the concept of sensitive personal data which had previously appeared in recommended standards only. Having a category of PI that is subject to a higher level of protection is consistent with international data protection standards. However, we note that the fact the PIPL has an open definition of sensitive PI means that operators will need to make a careful qualitative assessment of the types of data they collect based on potential harm, and cannot rely on checking against a closed list of categories, such as the "special categories" of data under the GDPR.

Enforcement

Civil liability

The PIPL provides a mechanism for individuals to receive compensation from the PI Processor if the processing infringes upon their rights and interests. The judicial redress will be correlated to the harm suffered or the benefit obtained by the PI Processor. Importantly, the PIPL reverses the burden of proof for a tort action relating to a PI infringement, so a PI Processor will be liable if it cannot prove that it is not at fault for the harm suffered.

Lawsuits may be filed in a people's court: (a) by individuals who have suffered a loss due to PI Processing; or (b) by the people's procuratorates, consumer protection organisations and the relevant enforcing agencies specified by the cyberspace administration for any violations that infringe on the rights and interest of many individuals, i.e. public interest lawsuits.

On 21 August 2021, the Supreme People's Procuratorate issued a circular on strengthening the duties of the people's procuratorates' in initiating public interest lawsuits in relation to PI protection, with a particular focus on sensitive PI, including but not limited to biometric features and locations and trajectory.

Penalties

Penalties for violations of the PIPL include, among others, fines of up to 5% revenue of the previous year. It is unclear whether this will be calculated on the basis of global turnover or PRC turnover only. While this level of penalty is reserved for "grave" unlawful acts, the availability of such robust remedies clearly signals a significant enhancement in the ability of enforcement authorities to punish wayward operators and parallels the GDPR's introduction of similarly material penalties for infringement.

Other penalties include correction orders, warnings, confiscation of unlawful income, suspension or termination of data processing activities and removal or suspension of directors or senior staff within certain periods.

Personal liability may be also imposed on the directors, supervisors and senior management and the relevant person responsible for PI protection, including fines of up to RMB1 million and restriction on taking on the same role within a certain period.

Other aspects of PIPL

PI breach

Companies are required to implement measures to ensure PI processing conforms to legal requirements and to prevent and address any unauthorized access, or PI leaks, theft, distortion or deletion (**PI breach**). These measures include:

i. putting in place internal management structures and formulating operating rules;

ii. implementing tiered and categorized personal information management, and adopting corresponding technical security measures such as encryption and de-identification;

iii. determining and periodically reviewing levels of access and control of employees handling PI processing;

iv. conducting regular employee training; and

v. developing contingency plans for PI security incidents.

Companies are required to take remedial steps in the event of a PI breach and inform affected individuals of the remedial steps taken. The PIPL does not provide a specific timeline for notification of PI breaches. Notification is not necessary if the PI Processor has taken measures to effectively prevent the PI breach from causing harm, unless the competent PI protection authorities consider notification to data subjects is otherwise necessary.

Data Protection Officers

Companies processing large quantities of PI must appoint persons responsible for PI protection and publish the name and contact details of such persons. The threshold of what will constitute large quantities of PI for these purposes has not yet been clarified.

Automated decision making

Under the PIPL, automated decision-making refers to activities that use PI to automatically analyse, and assess via computer programmes, individual behaviours and habits, interests and hobbies, or situations relating to finance, health, or credit status, and decide and implement the PI Processor's commercial behaviours accordingly. PI Processors are required to perform a risk assessment prior to such processing, and must ensure transparency, fairness and reasonableness of the result. Individuals who believe the automated decision-making may have a "major influence" on their rights and interests can require an explanation of the matter and can refuse to allow decisions to be made purely on an automated basis. Companies using automated decision-making for targeted sales or marketing must at the same time provide an option for individuals to receive information and offerings that are not based on personal characteristics.

Facial recognition

The PIPL also provides that the installation of image collection or personal identity recognition equipment in public venues must be used to safeguard public security only and comply with applicable regulations. PI collected by such devices cannot be used for other purposes and cannot be published or disclosed without separate consent from the relevant data subject, unless laws and regulations provide otherwise.

Conclusion

The promulgation of the PIPL signals the beginning of a new era of data protection in China. The law was enacted as part of a broader legislative and policy programme to enhance regulatory control and scrutiny over how data is collected, processed and exploited and to limit abusive practices that benefit operators at the expense of consumers' privacy. After two decades of unprecedent growth in the Chinese digital economy, the PIPL marks a shift towards greater scrutiny by the authorities and greater powers of enforcement.

While certain features of the PIPL reflects a focus on national security and digital sovereignty that is consistent with the policy priorities of the PRC government, the emphasis on protection of the rights of individuals against abuses by businesses that process their data aligns the PRC with the growing international consensus around robust and comprehensive laws that treat the privacy of individuals as a key concern in the regulation of technology. This alignment and the clarity the PIPL brings to the issues may be welcomed by international businesses with operations in the PRC or servicing PRC customers, who should be able to update their compliance processes to a framework that is now both more transparent and more expressly consistent with international regimes such as the GDPR.

The existence of provisions allowing PRC authorities to adopt retaliatory measures against jurisdictions that adopt discriminatory data protection policies against the PRC could, if the PRC authorities felt the need to exercise them, further complicate the position of international operators who may be caught between incompatible regulatory requirements.

For multinational groups operating in the PRC, the implementation of PIPL compliance should be a high-priority issue: the short timetable for compliance (1 November 2021) may require adaptations in the short term. Given the number of open questions on important issues, they will want to closely monitor implementing legislation and guidance to be issued in the future and trends in enforcement.

CONTACTS

Ling Ho
Partner

T +852 2826 3479
E ling.ho
@cliffordchance.com

Terry Yang
Partner

T +852 2825 8863
E terry.yang
@cliffordchance.com

Lei Shi
Partner

T +86 21 2320 7377
E lei.shi
@cliffordchance.com

Kimi Liu
Counsel

T +86 10 6535 2263
E kimi.liu
@cliffordchance.com

Brian Harley
Consultant

T +852 2826 2412
E brian.harley
@cliffordchance.com

Rita Flakoll
Senior Associate
Knowledge Lawyer

T +44 207006 1826
E rita.flakoll
@cliffordchance.com

Jane Chen
Associate

T +86 10 6535 2216
E jane.chen
@cliffordchance.com

Jessy Cheng
Associate

T +86 10 6535 4935
E jessy.cheng
@cliffordchance.com

Any advice above relating to the PRC is based on our experience as international counsel representing clients in business activities in the PRC and should not be construed as constituting a legal opinion on the application of PRC law. As is the case for all international law firms with offices in the PRC, whilst we are authorised to provide information concerning the effect of the Chinese legal environment, we are not permitted to engage in Chinese legal affairs. Our employees who have PRC legal professional qualification certificates are currently not PRC practising lawyers. This publication does not necessarily deal with every important topic or cover every aspect of the topics with which it deals. It is not designed to provide legal or other advice.

www.cliffordchance.com

Clifford Chance, 10 Upper Bank Street,
London, E14 5JJ

Clifford Chance LLP is a limited liability partnership registered in England and Wales under number OC323571

Registered office: 10 Upper Bank Street,
London, E14 5JJ

We use the word 'partner' to refer to a member of Clifford Chance LLP, or an employee or consultant with equivalent standing and qualifications

If you do not wish to receive further information from Clifford Chance about events or legal developments which we believe may be of interest to you, please either send an email to nomorecontact@cliffordchance.com or by post at Clifford Chance LLP, 10 Upper Bank Street, Canary Wharf, London E14 5JJ

Abu Dhabi • Amsterdam • Barcelona • Beijing • Brussels • Bucharest • Casablanca • Delhi • Dubai • Düsseldorf • Frankfurt • Hong Kong • Istanbul • London • Luxembourg • Madrid • Milan • Moscow • Munich • Newcastle • New York • Paris • Perth • Prague • Rome • São Paulo • Shanghai • Singapore • Sydney • Tokyo • Warsaw • Washington, D.C.

Clifford Chance has a co-operation agreement with Abuhimed Alsheikh Alhagbani Law Firm in Riyadh.

Clifford Chance has a best friends relationship with Redcliffe Partners in Ukraine.