DS NEWSLETTER savoir, faire
NEWSLETTER – LEGAL INFORMATIONS
PROPOSED BY DS AVOCATS

Will the Chinese "GDPR" affect you? Get ready for the PRC Personal Information Protection Law

ASIE

GENERAL INTRODUCTION

Though it is a Chinese law, many entities from other countries whose data activities are active with China have also waited for this Chinese "*General Data Protection Regulation* ("***GDPR***")" for a long time. After being discussed and reviewed for almost a year, the P*ersonal Information Protection Law of the People's Republic of China* ("***PIPL***") was finally released on August 20th, 2021. As a "late comer" of the Chinese cyber laws (i.e. the Cyber Security Law ("***CSL***"), and Data Security Law ("***DSL***")), PIPL will become effective on November 1st, 2021.

The extraterritorial effect of PIPL may explain why it takes the limelight globally. It would be applicable to entities in China (i.e. individuals, private enterprises, governmental authorities, institutions, etc.) but also to those who do not even have any presence in China but target natural persons in China by their personal information ("**PI**") processing activities.

Therefore, PIPL will affect not only Chinese entities but also those foreign entities subject to the extraterritorial jurisdiction of PIPL. To answer your possible curiosities of PIPL, we will introduce it from legal and practical perspectives in this article.

STATUS OF PIPL IN CHINESE LEGISLATION

Though being the first special law of PI protection, PIPL is not the start of the legislation protecting PI in China. Early in 2012, trigged by the digital development and the emerging issues of PI, China started to protect "*electronic information that can identify the personal identity of citizens and that involves privacy of citizens*". After that, the Civil Code, CSL, DSL, regulations in both the State and local level, official guidance and national standards gradually came out, but some of them still remain drafts. From a legal perspective, they are still part of the legal basis of PI protection, reflect the general principles (i.e. notification-consent principle) and pave the way for PIPL.

Among the existing effective Chinese laws, it worths noting the relationship between Civil Code, CSL, DSL and PIPL.

<table>
<tr><td colspan="3">Civil Code[1]</td></tr>
<tr><td colspan="3">The fundamental Chinese law</td></tr>
<tr><td colspan="3">*It legally recognizes privacy and PI as part of the right to human dignity. It defines privacy and PI and confirms the general principles in PI processing.</td></tr>
<tr><td>CSL[2]</td><td>DSL[3]</td><td>PIPL</td></tr>
<tr><td>Special law for cyber security</td><td>Special law for data processing activities</td><td>Special law for PI processing activities</td></tr>
<tr><td>- It governs cybersecurity activities of network operators.
- It also includes basic principles of PI protection and require CIIOs (Critical Information Infrastructure Operators) to store PI locally and any cross-border transfer is conditional.</td><td>- It governs the data processing activities in China and overseas.
- PI is also considered as data regulated by DSL, which provides more general principles (i.e. national strategies) applicable to most types of data.</td><td>- It is the special law comprehensively governing PI protection.
- It consolidates the general principles but also provides more specific requirements for PI processors and entrusted PI processors.
- It provides severe administrative penalties for violation of PIPL.</td></tr>
</table>

1 Released on May 28th, 2020 and became effective on January 1st, 2021.

2 Released on November 7th, 2016 and became effective on June 1st, 2017.

3 Released on June 10th, 2021 and became effective on September 1st, 2021.

COMPARISON WITH GDPR

PIPL is quite similar with GDPR especially concerning the main obligations of the data controller and data processor, the rights of data subject, as well as the requirements concerning data breach scenarios etc. Please see below the table of a comparison between PIPL and GDPR in some basic aspects.

<table>
<tr><th>Aspects\Laws</th><th>GDPR</th><th>PIPL</th></tr>
<tr><td>Entities subject to the law</td><td>Data controller
Data processor</td><td>Data processor (term used in PIPL to designate the data controller)
Entrusted processor (term used in PIPL to designate the data processor)</td></tr>
<tr><td>Personal data/information</td><td colspan="2">They are similar in the definition of PI which emphasizes on the function "any kind of information related to an identified or identifiable natural persons (article 4 of PIPL)" and exclude "anonymized data/information" from the category of PI.</td></tr>
<tr><td rowspan="2">Jurisdiction</td><td colspan="2">Both are with extraterritorial jurisdiction based on similar targeting principle.</td></tr>
<tr><td>- <u>Establishment principle:</u>
The personal data processing related activities of the data controllers or data processors established in the EU, irrespective of whether the processing occurs in the EU.

- <u>Targeting principle:</u>
The personal data processing activities are
(1)for providing goods or services to a data subject within the EU, whether or not the data subject is required to pay consideration; or
(2) for monitoring their behavior as long as their behavior occurs in the EU.</td><td>- <u>Territorial principle:</u>
The PI processing activities occur in China.

- <u>Targeting principle:</u>
The PI processing activities occur outside China but targeting natural persons in China:
(1)for provision of products and/or service; or,
(2)for analyzing their behavior.</td></tr>
<tr><td>Processing</td><td colspan="2">They are similar and include the whole lifecycle of personal data/information, including but not limited to "the collection, storage, use, processing, transmission, provision, disclosure, and deletion (article 4 of PIPL, a non-exhaustive list)".</td></tr>
<tr><td rowspan="2">General principles of processing</td><td colspan="2">They are also similar in most of the principles.</td></tr>
<tr><td>1. Lawfulness, fairness and transparency;
2. Legitimate purpose
3. Data minimization;
4. Accuracy;
5. Storage limitation; and,
6. Integrity and confidentiality.</td><td>1. Lawfulness, legitimacy, necessity and good faith;
2. Legitimate purpose
3. Data minimization;
4. Openness and transparency;
5. Accuracy and completeness;
6. Security.</td></tr>
</table>

<table>
<tr><td rowspan="4">Legal Basis for processing</td><td colspan="2">Though some wordings are different, they are similar in the following aspects. Both GDPR and PIPL require controllers to meet at least one of the following conditions for PI processing.</td></tr>
<tr><td>1. Informed consent;
2. Contract performance;
3. Legal obligation;
4. Vital interest of individuals;
5. Public interest</td><td>1. Informed consent;
2. Contract and labor management;
3. Legal obligation;
4. Emergency (public health/vital interest of individuals);
5. News reporting, or for public interest purposes;</td></tr>
<tr><td colspan="2">They differ in the following conditions listed. GDPR provides a "wide door" via "legitimate interest" as legal ground for PI processing, while PIPL absenting such clause but specifies that processing PI legally disclosed to the public does not require the consent from the data subject.</td></tr>
<tr><td>6. Legitimate interest.</td><td>6. PI disclosed to the public; and,
7. other legal basis specified by other laws and regulations.</td></tr>
<tr><td rowspan="4">Rights of data subject</td><td colspan="2">They are also similar in most of the rights of data subject:
1. Right to information;
2. Right to access;
3. Right to rectification;
4. Right to erasure/to be forgotten;
5. Right to restriction of processing;
6. Right to data portability;
7. Right to object;
8. Right to not be subject to automated decision-making.</td></tr>
<tr><td colspan="2">PIPL has two more rights specified for data subjects and does not mention restrictions on the rights of data subjects.</td></tr>
<tr><td>*Transparent communication is required and the rights of data subject are with restrictions.</td><td>9. Right to make copies(associated to the right to access);
10. Right to decide on the processing activities (associated to the right to restriction and the right to deny).</td></tr>
<tr><td colspan="3">*Please contact us if you would like to know more about the comparison between GDPR and PIPL.</td></tr>
</table>

Considering these similarities between PIPL and GDPR, entities with European background should be more familiar with PIPL's regulatory framework and thus it would be easier for them to be compliant than those entities with non-European background.

HIGHLIGHTS OF PIPL

1. Enlarged scope of sensitive PI

The PI of minors whose age is under 14 shall be deemed as sensitive PI.

2. Protection of the PI of the deceased

For the PI of a deceased, his/her close relative may exercise the rights to access, make copies of, have corrected or deleted and other rights to the relevant PI of the deceased, unless the deceased has arranged otherwise before death.

3. Official testing of mobile applications

The competent authority has the right to organize the testing and evaluation of any application program etc., for PI protection, and disclosing the results to the public.

4. Restrictions on the use of publicized PI

PI processors may process PI of an individual already disclosed by the individual or otherwise legally disclosed, unless such processing is expressly refused by the individual. For the processing of any publicized PI of an individual that will have a material impact on the individual, PI processors shall obtain consent from the individual.

5. Legal audit

PI processors shall have the compliance of their activities of processing of PI with laws and administrative regulations have it audited on a regular basis.

6. Representative/branch (presence requirement) for foreign entities

Foreign entities without any presence in China but subject to the extraterritorial jurisdiction shall set up a branch or designate a representative based in China. Such branch or the designated representative shall be responsible for PI protection-related matters and their contact information shall be submitted to the relevant competent authorities.

7. Right of action by data subject

Individuals may bring a lawsuit in a people's court against a PI processor for the latter's denial of their request to exercise their rights.

8. Reversal of burden of proof

Where any damages are caused due to an infringement of PI rights and interests in the processing of PI, if the infringing PI processor is unable to prove that there is no fault on its/his/her part, such processor shall bear tort liability, including the liability for damages. Thus, company should not only implement organizational, technical and managerial measures for compliance, but also make the process "visible" by keeping records.

IMPLICATIONS FOR ENTERPRISES

1. Administrative penalties

Violation of any of the requirements of PIPL	Penalties
Normal cases	- Order of rectification; - Warning; - Confiscating illegal gains (if any); - (for applications) order of suspension or termination of the service.

Where the violator refuses to rectify the illegal activities	Beside the above, - Pecuniary fine (below 1 million RMB) upon the violator; - Pecuniary fine (10k RMB to 100k RMB) upon the person directly in charge of the violator.
Severe cases	- Order of rectification by the competent authority in provincial level; - Confiscating illegal gains (if any); - Pecuniary fine (below 50 million RMB or below 5% of the previous year's turnover of the violator) upon the violator; - Suspension or termination of business, and cancellation of the relevant approvals or business license; - Pecuniary fine (100k RMB to 1 million RMB) to the person directly in charge; and, - Such person directly in charge of the violator can be banned for a certain period of time from serving as a director, supervisor, and senior officer or PI protection officer of a relevant enterprise.

2. Checklist of missions for PIPL compliance

- Implementation of effective internal measures

Involve employees of different business departments and ensure that an internal leader is dedicated to the management of PI protection. For any compliance program, complicated issue or regular training and audit, third party professionals (legal, technical etc.) should be involved.

- Updating Internal Rules

Internal Policies;
Employees' Handbook;
IT Policy;
Contingency plans for PI security incidents, etc.

- Updating contracts:

Labor contract;
Commercial contracts involving PI processing (collection etc.);
General Terms and Conditions and Privacy Policy, (including those relate to loyalty program)
Membership Plans; and,
Non-Disclosure Agreement etc.

- Check internal systems and technical measures adopted internally

Access Control System (user right design/classification of data storage);
Entrance Guard System (to check the necessity and whether exceeding PI and/or sensitive PI is collected);
CRM (where does the PI of clients go and is it controlled securely); and,
ERP (employees' PI management) etc.

- Check if any of the following technical measures can be taken to improve security:

De-identification;
Anonymization; and,
Other encryption methods etc.

- Overall compliance (from general requirements to specific rules)

Besides PIPL, check the compliance status per CSL, DSL and other regulations governing special industries (i.e. healthcare, pharmaceutical, automobile, financial industry, ecommerce, insurance etc.), because they may have more specific requirement for PI processing, for instance, retention period for customers' PI in e-commerce industry.

UNSOLVED ISSUES

PIPL is the milestone of the Chinese legislative development of PI protection, but it does not solve all the issues haunting over entities involved with PI processing, especially multinational enterprises.

1. Data localization

PI processors, whose processing of PI reaches a certain threshold amount, likewise CIIOs, shall store in China the PI collected or generated by them in China. The threshold triggering the data localization requirement is not yet specified and thus non-CIIOs will have to wait a little longer for further detailed rules.

2. Cross-border PI transfer

PI processors subject to data localization obligation, and CIIOs, who further want to transfer PI outside China, must first pass a security assessment organized by the national cyberspace authority. The content and organization of the security assessment is subject to measures that are not yet disclosed or implemented.

3. Unclear definitions:

- "Small PI processor"

Besides PIPL, the competent authorities will release special rules and standards for PI protection regarding small PI processors, processing of sensitive PI, and facial recognition, artificial intelligence and other new technologies and new applications.

- "*PI Protection Certification*"

For processors who process PI does not reach the threshold amount (unclear yet) triggering data localization obligation, PI Protection Certification is one of the options such processors may choose in order to make the cross-border PI possible. However, details of such service providers and application process of such PI Protection Certification are not clear yet.

- "*Specific consent*"

PIPL mentioned specific consent which is required in several scenarios, but no clear definition is provided yet, neither how it should be implemented.

***

With PIPL in place, enterprises who are involved with PI processing should start the compliance program as soon as possible. It would be an ongoing team work and no one can be ready overnight. Practically speaking, as long as data flows, PI processing is a dynamic process, and so is PI protection.

For any additional information please contact:

ZHANG Beibei
Associate - Shanghai Office
beibeiZHANG@dsavocats.com

Isabelle DOYON
Lawyer- Shanghai Office
DOYON@dsavocats.com