An overview of the Chinese «Personal Information Protection Law»

YANG Jun
Jun.yang@jadefountain.com
Jade & Fountain PRC Lawyers

The long-awaited "PRC Personal Information Protection Law" ("PIPL") was finally unveiled on August 20, 2021 and will take effect on November 1, 2021. As the last piece of the Chinese legislative trilogy in data protection area (after "Cyber Security Law" ("CSL") in 2016 and "Data Security Law" ("DSL") earlier this year), this legislative milestone will have immediate and lasting impact on the data protection in China. PIPL which was released amid Beijing's continued regulatory crackdown on Chinese tech giants would not only help the Chinese regulator to end the wild practices in the local market in short term but also achieve a rebalance between commercial exploitation of personal information and protection of data subjects. PIPL will profoundly change our daily life and the way how the corporate citizens operate in China (and in overseas jurisdictions) in various fronts ranging from the design of their products/services, defining(redefining) their operating rules to internal decision-making process. This article is intended to offer you an overview of some key aspects of this new law.

The definition of "Personal Information[1]" and "processing" under PIPL

The "Personal Information" is defined in a consistent fashion in Chinese legislative texts prior to PIPL.

Article 76 of the CSL provides that "*'personal information' refers to the "information recorded by electronic or other means which may identify an individual by such information alone or in conjunction of other information, including but not limited to name, date of birth, ID document number, <u>biometrics</u>[2], residential address, phone number.* "

Article 1034 of the PRC Civil Code defines "personal information" as "*information recorded by electronic or other means which may identify an individual by such information alone or in conjunction of other information, including name, date of birth, ID document number, biometrics, residential address, phone number, email address, health information and itinerary*."

Definition of "personal information" under PIPL appears however partly inspired by article 4 of

[1] The term "data" is defined under DSL as "information recorded by electronic or other means". The term "data subject" used in this legal note refers however to "personal information subject".

[2] The PRC Supreme Court released on July 28, 2021 certain judiciary interpretations regarding the cases involving the application of facial recognition technology.

"General Data Protection Regulation" ("GDPR") and it reads: *"information relating to an identified or identifiable individual recorded by electronic or other means*" and "*Such information, if technically anonymized,*[3] *shall be no longer considered as personal information*" (article 4 of PIPL).

The term "processing" above is defined under PIPL as "*collection, storage, use, processing, transmission, provision, disclosure and erasure*" (article 4).

Scope of application

- Territorial scope

The PIPL applies to not only the processing of personal information in Chinese territory but also the following processing activities of personal information involving individuals in Chinese territory[4] **by a processor** [5]**based in an overseas jurisdiction** (article 3):

(a) such processing (in an overseas jurisdiction) aims to supply products/provide services to individuals in Chinese territory;
(b) behavioral analysis and assessment of individuals in Chinese territory;
(c) other activities provided by law and regulation.

The term "individuals in Chinese territory" above covers both Chinese nationals and foreign national/stateless individuals.

The above quoted text of PIPL clearly highlights that the underlying consideration for territorial application of PIPL is whether the data subjects in Chinese territory are concerned by the processing in question. This is obviously different from the territorial scope clause of GDPR which reads "*this regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.*"

[3] The "anonymization" is defined by article 73 of the PIPL as a technical process whereby the information after processing is unlikely to identify an individual or to be restored to its original status.

[4] The above term "Chinese territory" refers to the "mainland China" only for purpose of the PIPL and accordingly the term "overseas jurisdiction" above covers Hong Kong SAR, Macau SAR and Taiwan region which are constitutionally part of Chinese territory and remain as separate jurisdictions from the mainland China.

[5] The term "processor" is defined under PIPL as "entity or individual which decides on its own the purpose and modality of processing".

The overseas processors covered by article 3 of PIPL above shall set up a structure or designate a representative responsible for personal information protection and report the name of the structure/representative and their contact details to the competent authorities in charge of personal information protection. PIPL specifies neither the legal form of the above "structure" nor the qualification of the "designated representative" and these technical details are expected to be further clarified by implementation rules of PIPL or other applicable regulations to be released.

- Material scope

The application of PIPL shall be excluded in the following circumstances:

(a) Processing by an individual for personal or family matters;
(b) The processing in statistical activities and files management by governmental agency and other competent department in application of law

The Fundamental principles governing the processing of personal information

PIPL sets a number of fundamental principles:

(a) Personal information shall be processed lawfully, fairly with honesty and to the extent necessary in relation to the purposes for which they are processed;
(b) Personal information shall be processed for clear and reasonable purpose and the personal information processed shall be directly associated with the purpose for which they are processed;
(c) Personal information shall be processed with openness and transparency with the rules applicable to processing made known to the data subject;
(d) Personal information shall be processed with accuracy.

The General rules governing the processing of personal information

Typically, the processing of personal information shall be subject to prior consent of the data subject concerned.

The above consent from the data subject shall be a fully informed consent made in voluntary and clear manner. To this end, the processor shall inform in advance the data subject concerned of the following in a distinguishable form and in clear and plain language and in a sincere, accurate and complete fashion (article 17):

(a) *the identity and the contact details of the processor (save otherwise exempted by applicable law or regulation on the ground of confidentiality);*
(b) the purpose, modality of processing, the categories of the personal information concerned and retention period for the personal informaiton;
(c) the modalities and procedure whereby the data subject may exercise its rights under the PIPL;
(d) other information requested by law and regulation.

A further consent shall be secured from the data subject concerned in case of any change of the items in the preceding paragraph.

On top of the information above substantiated in article 17 of PIPL, a processor shall additionally inform the data subject of the necessity of processing his/her personal information and the potential impact of such processing upon the data subject in case where any “sensitive personal information” is involved (see the Section below entitled as “Special rules governing the processing of personal information”).

A “Separate” consent shall be secured from the data subject under certain circumstances including outbound transfer of personal information (please also see Section below named “Outbound transfer of personal information”), processing involving biometrics and other sensitive personal information.

The data subject shall be entitled to withdraw his/her consent and the data subject shall be granted user-friendly route for his/her withdrawal of consent. Such withdrawal shall not retroactively affect the validity of the processing based on consent prior to the withdrawal of the consent.

The processor is prohibited from declining supply/provision of products/services to the data subject concerned should the data subject object to grant his/her consent or withdraw the consent unless precessing of the relevant personal information is indispensable for supply/provision of products/services in question.

Article 13 of the PIPL provides also that processing of personal informaiton without prior consent from the individual concerned is permitted in any of following circumstances:

(a) *where the processing is required for concluding and performing a contract of which an individual is a contracting party or required for human resources management in application of internal rules and collective labor contracts legally formed;*
(b) where the processing is indispensable for performing statutory duties or obligation;
(c) where the processing is indispensable for reacting to outbreak of public health incident or for

protection of an individual's health, safety or property in an urgent situation;
(d) processing of personal information to extent reasonable in course of media report for sake of public interest;
(e) processing to extent reasonable of personal information made known to the public on the individual's own initiative or by other lawful avenues
(f) other circumstances provided by law and regulation.

The special rules governing processing of personal information

- Processing of sensitive personal information

"Sensitive personal information" refers to "*personal information which, if disclosed or used for illegal purpose, is likely to undermine the dignity/honor of an individual or expose his/her personal safety/property to danger, including biometrics, religious belief, specific identity, health, accounts opened with financial institutions, itinerary tracking and personal information of a minor under age of 14 years.*[6]"

A processor may process sensitive personal information only when justified by specific purpose and sufficient necessity and equipped with strict protective measures in place.

In addition to the foregoing, the separate consent from the data subject shall be secured and a consent in writing, if required by law and regulation, shall be secured as well.

Separate consent from the parents or guardians shall be imperatively solicited in case where a minor under age of 14 is involved and the processing of personal information involving a minor under age of 14 shall be governed by specific operating rules elaborated by the processor.

- Processing by a governmental agency

The processing by a governmental agency is also governed by the PIPL and the processing shall be conducted within the scope of power of the governmental agency concerned and in accordance of process specified by applicable law and regulation and a governmental agency shall not proceed with processing out of the scope or extent necessitated by its statutory duties.

Outbound transfer of personal information

[6] The Chinese Civil Code provides that a natural person under the age of 18 is a minor. The reference to "a minor under age of 14" appears however consistent with the "Regulations on Children's Personal Information Protection" effective as of October 1st, 2019 which defines "child" as "a minor under age of 14".

A processor, if justified by a business reason, may proceed with outbound transfer of personal information if one of the following conditions is fulfilled:

(a) pass successfully the security assessment by competent authorities;
(b) receive personal information protection certification by professional agency;
(c) A contract based on the template elaborated by competent authorities entered into with the recipient of personal information based in overseas jurisdictions to clearly stipulate the rights and obligations of the each party.
(d) other conditions specified by law, regulation or the competent authorities

The processor shall take necessary measures to ensure that the processing of the recipient of the personal information in overseas jurisdiction be under the protection no less favorable than PIPL.

In addition to the above measures, the processor shall inform the data subject of the following information and secure the separate consent from the data subject:

(a) the identity and contact details of the recipient;
(b) purpose and modality of processing;
(c) the categories of personal information to be processed;
(d) the modality and procedure whereby the data subject may exercise his/her rights under PIPL vis-a-vis the recipient in overseas jurisdiction.

CIIO (Critical Information Infrastructure Operator)[7] and other processor whose processing breaching the quantitative threshold set by applicable regulation shall store in China the personal information collected and generated in China. They have to pass successfully the security assessment by competent authorities if outbound transfer of personal information is justified.

Processor shall be prohibited from providing personal information stored in Chinese territory to any foreign judiciary or law enforcement department unless duly approved by Chinese competent authorities.

The Rights of Data Subject

A data subject has right of information and decision-making and is entitled to restrict or object others to process his/her personal information save otherwise provided by the law and regulation. A novelty in this regard embodied by PIPL is that a data subject is entitled to request a processor to provide explanation/information with respect to a “decision significant to his/her individual rights” based on automated decision-making mechanism and object any decision made

[7] The term “critical information infrastructure” is defined in CSL.

by the processor entirely based on automated decision-making mechanism.

A data subject is entitled to request for access, copy, rectification and (conditionally) personal information portability[8].

The data subject is also entitled to request the processor to erase his/her information if the latter fails to do so in one of the following circumstances:

(a) the purpose of processing is fulfilled, unlikely to be fulfilled or no longer necessary;
(b) the processor has ceased to supply/provide relevant products/services or the personal information retention period has expired;
(c) the data subject has withdrawn his/her consent;
(d) the processing in breach of law, regulation or agreement;
(e) other circumstances provided by law and regulation.

In case where the statutory retention period has not expired or the erasure of the personal information is technically infeasible, the processor shall immediately cease all processing other than the storage and necessary measures to safeguard the personal information.

Save otherwise arranged by the deceased during his/her lifetime, the close relatives[9] of a deceased shall be entitled to review, copy, rectify and erase the relevant personal information of the deceased for sake of their own legitimate interests[10].

The obligations of processor

A processor shall take the following measures in light of (1) its purpose and modality of processing , (2) categories of personal information concerned and (3) potential impact on the individual rights and risk exposure to ensure its processing be in line with applicable law and regulation and to prevent unauthorized access to and leakage, falsification and loss of personal information:

(a) elaborate internal management system and operating rules;
(b) classification of personal information;

[8] Unlike the GDPR which explicitly requires "a structured, commonly used and machine-readable format" ready for data portability at the request of data subject, the PIPL provides conditionally the right of data portability only to extent where the conditions under relevant regulation are fulfilled. The Chinese legislature has obviously taken into account the reality and contest where such right is to be exercised.

[9] The term "close relatives" is defined in article1045 of the Civil Code as "spouse, parents, children, brothers/sisters, paternal/maternal grandparents, paternal/maternal grandchildren.".

[10] This appears consistent with the judiciary interpretations released on July 28, 2021 PRC Supreme Court regarding the cases involving the application of facial recognition technology.

(c) adopt encryption, de-identification technology;
(d) reasonably define the scope of power of its operating staff processing personal information and offer training to staff regularly;
(e) elaborate and implement backup plan to address the personal information incident;
(f) other measures provided by law and regulation.

A processor whose processing attaining the quantitative threshold shall appoint a person responsible for personal information protection and the contact details of this person shall be made known to the public. The identity and contact details of this person shall be filed with the competent authorities in charge of personal information protection. Several questions may arise with respect to this “person responsible for personal information protection”, seemingly an equivalent to the “Data protection officer” under GDPR: What will be the qualifications required for this position? Will the responsibilities of this position under PIPL be entirely covered by “person in charge of data security” as per the DSL or a separate position should be created? Such issues need to be further clarified by implementation rules of PIPL.

A processor shall conduct compliance audit periodically with respect to the processing.

A processor shall conduct prior assessment on personal information protection impact and have the processing documented in case of occurrence of any of the following circumstances:

(a) *processing of sensitive personal information;*
(b) automated decision-making based on personal information;
(c) entrusting others to process personal information, transfer personal information to other processors, disclose personal information to the public;
(d) outbound transfer of personal information to overseas jurisdiction;
(e) other processing having significant impact upon individual rights

The personal information protection impact assessment report and processing log shall be kept for a retention period of 3 years minimum[11].

The processor providing critical internet trading platform service or other processors having significant number of users or complex business portfolio (“Gatekeeper” processor) shall observe a number of additional obligations including: (1) set up personal information protection compliance system and independent personal information protection monitoring structure comprised of external experts; (2) design trading platform rules to regulate the processing of personal information by vendors on the platform and their obligation for personal information

[11] This 3-year retention period requirement is consistent with the statutory limitation under the Chinese Civil Code.

protection; (3) cessation of service provision to vendor in serious breach of law and regulation governing processing of personal information; (4) regular release of its personal information protection social responsibility report.

Liabilities

- Administrative liabilities
- Breach of PIPL may result in administrative sanctions under PIPL for both corporate processor in question and the person in charge:

(a) administrative sanctions against breaching processor range from order of rectification, warning, confiscation of illegal revenues to suspension of breaching app;
(b) for those breaching processor resisting to rectify, a fine up to one million RMB may be concurrently imposed;
(c) a fine ranging from RMB10k to 100k may be imposed on the person in charge and those directly held accountable for the breaching acts identified.
(d) in case of serious circumstances, the competent authorities at provincial or national level may issue order of rectification, confiscation of illegal revenues and concurrently impose a fine up to RMB50M or up to 5 percent of the processor's business turnover in preceding year plus order to suspend the business operation or withdrawal of operation or business license of the processor. The persons in charge or other persons directly held accountable may be fined in an amount ranging from RMB100K to RMB1M and barred from assuming position such as director, director, senior manager or person in charge of personal information protection within certain time period.

- Civil liabilities

A data subject is entitled to claim damages from the processor concerned where the latter infringes the legitimate rights of the data subject and causes the damages thereby. The damages shall be in first place determined in light of the actual losses suffered by the data subject or the benefits gained by the processor. The damaged shall be determined in light of the "actual circumstances" in case where neither actual losses suffered by the data subject nor the benefits gained by the processor may be ascertained.

The burden of proof is also reversed in favor of data subject if the data subject suffers any damages: the processor shall be held liable for damages if it fails to prove there is no fault on its part for the damages identified.

Where two or multiple processors decide jointly the purpose and modality of personal information processing, such processors shall agree on their respective right and obligation among them. Such agreement shall not be opposable to the data subject concerned to exercise his/her rights under PIPL vis-à-vis any of such processor and the above processors shall be held liable on a joint and several basis should they jointly undertake processing of personal information processing.

- Criminal liabilities

The entity/individual concerned is likely to incur criminal liabilities as well under Chinese law.

YANG Jun
Partner
Jade & Fountain PRC Lawyers
Email: Jun.yang@jadefountain.com

The above note is for informative purpose only and it shall be in no event considered and relied upon as a formal legal advice/opinion. You shall solicit professional counseling from a qualified attorney for the above subject matter.