中倫律師事務所
ZHONG LUN LAW FIRM

Commentary on the Chinese Personal Information Protection Law

By Jihong CHEN, Jiawei WU, Eva YANG, Yating JIAO, Yulang CHEN, Jiabin SUN

On 20 August 2021, the *Personal Information Protection Law of the People's Republic of China* ("PIPL") was adopted at the 30th session of the Standing Committee of the 13th National People's Congress, effective as of 1 November 2021. The PIPL is the fundamental law in the personal information ("PI") protection sphere and, together with the *Cybersecurity law* ("CSL") and the *Data Security Law* ("DSL"), it outlines the data regulatory framework in China. The PIPL embraces a new era of PI protection as well as corporate compliance and may materially change product design and compliance setting practices. In this article, we will analyze the key contents of the PIPL and provide you with a practical compliance guideline to help you better grasp the implications of the law.

1. Basic concepts of the PIPL

1.1. Applicable scope

The PIPL applies to any handling of PI that is carried out within the territory of the People's Republic of China.[1] That is to say, any organization or individual conducting PI handling activities within the territory of China is subject to the PIPL. This law also possesses extra-territorial effect. Para.2 of Art.3 specifies that any handling of PI of an individual residing in China that is carried out outside the territory of China is subject to the law where any of the following circumstances exists: (1) the handling activity is related to offering of any goods or services to that individual residing in China, (2) the handling activity is related to analysis and assessment of behavior of that individual residing in China, or (3) any other circumstances as provided by laws and administrative regulations. For instance, overseas online shopping websites with setting options of Chinese language, Chinese currency, direct shipping services or even local marketing promotion engagement may be deemed as meeting the criteria prescribed by para.2 of Art.3 and therefore subject to the PIPL.

The law also requires an organization or individual that is subject to the PIPL under the para.2 of Art.3 to establish a specific agency or appoint representative(s) (equivalent to the Representatives under Art.27 of the GDPR) within China to fulfil related PI protection obligations. Contact details

[1] Personal Information Protection Law of the People's Republic of China, para. 1 of Art.3.

of such specific agency or delegated representative shall be filed with relevant authorities for record.[2]

1.2. Legal accordance

The very first article of the PIPL states that the law is enacted in accordance with the Constitution of China to protect PI rights and interests, regulate activities of PI handling and promote reasonable use of PI, reflecting that China respects and protects human rights and dignity of citizens as well as their freedom and confidentiality of communications.

1.3. Key definitions

The PIPL defines the following key concepts relating to PI handling:

- **Personal information** refers to any kind of information related to an identified or identifiable natural person as electronically or otherwise recorded, excluding information that has been anonymized.[3]

- **Handling of personal information** includes collection, storage, use, processing, transmission, provision, disclosure and deletion of PI.[4]

- **Personal information handler** under the PIPL refers to any organization or individual that independently determines the purpose and method of handling in their activities of processing of personal information, which is substantially equivalent to the concept of controller under the GDPR.[5]

It is worth noting that the PIPL introduces a notion called "small-scale PI handler". We understand that the Cyberspace Administration of China ("CAC") together with other relevant authorities will issue specific PI protection rules in the near future to clarify the definition and other aspects of that notion.[6]

2. Seven principles relating to handling of PI

The principles relating to handling of PI must be implemented throughout the full lifecycle of PI handling activities and are closely related to the PI protection obligations as well as internal PI

[2] Personal Information Protection Law of the People's Republic of China, Art.53.

[3] Personal Information Protection Law of the People's Republic of China, Art.4.

[4] *Ibid.*

[5] Personal Information Protection Law of the People's Republic of China, Art.73.

[6] Personal Information Protection Law of the People's Republic of China, Art.62.

compliance management of PI handlers. In this section we will elaborate on each of the principles especially with regard to compliance practices and enforcement of the PIPL, among other issues.

PIPL	GDPR (Art.5)
Lawfulness, legitimacy, necessity and good faith (Art.5)	lawfulness, fairness and transparency
Purpose limitation (Art.6)	Purpose limitation
Data minimisation (Art.6)	Data minimisation
Transparency (Art.7)	lawfulness, fairness and transparency
PI quality (Art.8)	Accuracy
Accountability (Art.9)	Accountability
Data security (Art.9)	Integrity and confidentiality
/[7]	Storage limitation

Chart 1. Principles (PIPL v. GDPR)

- **Lawfulness, legitimacy, necessity and good faith.** Art.5 specifies that PI shall be handled in accordance with the principle of lawfulness, legitimacy, necessity and good faith, and no manner of means that is misleading, fraudulent or coercive is allowed in PI handling. It is worth noting that the PIPL puts necessity in equal importance with lawfulness, legitimacy and good faith, demonstrating that necessity has become a focus of PI protection administration. Together with the *Rules on the Scope of Necessary Personal Information for Common Types of Mobile Internet Applications* recently released by the CAC as well as the principle of purpose limitation and data minimisation described below, the necessity requirement obliges companies to ensure that their PI handling is directly related to intended purposes and their PI collection is limited to the minimum scope necessary for achieving the purposes.

- **Purpose limitation and data minimisation.** Art.6 stipulates that PI handling shall be conducted for explicit and reasonable purposes and connect directly to the purposes of the handling. But how to determine "connect directly" needs further clarification.[8] In addition, PI collected shall be limited to what is necessary in relation to the purposes for which they are processed.

[7] Though the PIPL, as opposed to the GDPR, does not include storage limitation in the principles relating to PI handling, it specifies in its Art.19 that PI shall be the minimum period necessary for achieving the purpose of handling, unless any law or administrative regulations stipulate otherwise.

[8] The GB/T 35273—2020 PI Specification defines "directly connected" as the function of the product or service cannot be realized without the PI collect.

- **Transparency.** Art.7 and Art.17 (information to be provided) lay down the transparency fundamentals under the PIPL. Such requirements are generally implemented through companies' privacy policy making. Art.17 stresses that, before handling any PI of an individual, the handler shall fully inform the individual of information relating to PI handling in a complete manner, which indicates that companies should avoid using wording of "etc." and "such as" in their privacy policy and relevant documents. In terms of content, companies shall include all items required under the Art.17 in their privacy policy. Moreover, the PIPL puts additional disclosure requirements for certain scenarios such as PI transmission under merger, acquisition, dissolution, etc.,[9] sharing of PI,[10] handling of sensitive PI[11] and PI cross-border transfer.[12] Privacy policy shall be delivered to each individual in a notable manner like on the account registration page via a tick box or pop-up window before collection of PI. Besides, privacy policy shall be easily accessible. Companies may consider placing their privacy policy on their website homepages, App user setting sections, etc.

- **PI quality.** The quality of PI shall be ensured to avoid any negative impact of inaccurate or incomplete PI on personal rights and interests.

- **Accountability and data security.** Art.9 is the underlying cornerstone of Chapter V "Obligations of PI Handlers", which deals with, among others, establishment of an internal data security management system and operating procedures, access control, compliance awareness training at both technical and organizational levels[13], as well as designation of PI protection officer.[14]

3. Legal bases for PI handling

The PIPL provides seven legal bases for PI handling as listed in the chart below and breaks the situation set by the CSL where consent was the only legal basis recognized.[15] The PIPL, as opposed to the GDPR, innovatively creates the legal bases of "necessary for the performance of human resource management under labor rules or a collective labor contract made in accordance with law" and "utilization of public PI (self-disclosed PI and PI otherwise disclosed legitimately) within a reasonable scope".

[9] Personal Information Protection Law of the People's Republic of China, Art.22.

[10] Personal Information Protection Law of the People's Republic of China, Art.23.

[11] Personal Information Protection Law of the People's Republic of China, Art.30.

[12] Personal Information Protection Law of the People's Republic of China, Art.39.

[13] Personal Information Protection Law of the People's Republic of China, Art.51.

[14] Personal Information Protection Law of the People's Republic of China, Art.52.

[15] Personal Information Protection Law of the People's Republic of China, Art.13.

PIPL (Art.13)	GDPR (Art.6)
Consent	Consent
Necessary for the performance of a contract or for human resource management	Necessary for the performance of a contract
Necessary for performance of statutory obligations	Necessary for compliance with a legal obligation
Vital interests under public heath incidents or emergencies	Vital interests
Public interests	Public interests
Utilization of public PI	/
Otherwise prescribed by laws and administrative regulations	/
/	Legitimate interests

Chart 2. Legal bases (PIPL v. GDPR)

3.1. Conditions for valid consent

The PIPL specifies that a consent shall be obtained in a way that the owner of PI is fully informed in order for the consent to be valid. A consent also needs to be freely given, specific and easy to withdraw.[16] "Tying" the provision of a contract or a service to a request for consent to process PI that is not necessary for the performance of that contract or service is not allowed.[17] Where PI handling activities are conducted on the basis of consent, PI subjects have the right to withdraw their consent and the PI handler shall provide a convenient channel for such withdrawal. Validity of any PI handling activity conducted based on the consent prior to such withdrawal is not affected.[18] Companies shall establish an internal standard for valid consent obtainment and review and provide effective ways for withdrawal of consent. Though the PIPL does not require as the GDPR does that withdrawal shall be as easy as granting of consent, good industrial practices such as providing a direct withdrawal option on the App account setting page are highly suggested.

3.2. Separate consent

[16] Personal Information Protection Law of the People's Republic of China, Art.14, Art.15.

[17] Personal Information Protection Law of the People's Republic of China, Art.16.

[18] Personal Information Protection Law of the People's Republic of China, Art.15.

The PIPL sets separate consent requirement for various scenarios such as sharing of PI, handling of sensitive PI and PI cross-border transfer. Though what constitutes separate consent under the PIPL requires further clarification, we understand that PI handlers shall at least ensure that PI subjects are allowed to give consent to certain handling activities separately rather than to a bundle of handling purposes. The separate consent requirement will have a great impact on PI handlers with respect particularly to the legality of their handling activities concerned as well as product compliance settings. We recommend that companies sort out the scenarios of their services that require separate consent in advance and pay close attention to the latest good industrial practices.

4. Specific scenarios relating to PI handling

- Sharing of PI. Art.20 and Art.21 specify requirements with respect to joint handling and entrusted handling under the PIPL, which resemble those of the GDPR. Joint handlers shall determine their respective compliance responsibilities through arrangement and bear joint and several liability for damage caused by infringement upon PI rights and interests. Entrusted parties (substantially equivalent to Processors under the GDPR) shall conduct data handing as instructed and shall also fulfill PI security and assistance obligations as required by the law.19

- Automated decision making. Art.24 of the PIPL, responding to certain social concerns, specifies that where a PI handler uses PI to make an automatic decision, it shall ensure the transparency and fairness of such decision and shall not impose unreasonable discriminatory treatment on individuals in respect of transaction price and other transaction conditions. A handler shall provide convenient exit option or non-targeted option to users when conducting promotional marketing or message push via automated decision making. Individuals have the right to require PI handlers to make explanation and reject decisions solely made through automatic decision-making.

- Handling of sensitive PI. Sensitive PI as defined in Art.28 refers to personal information that is likely to cause detriment to dignity of a natural person or damage to one's personal or property safety once leaked or illegally used. The PIPL specifically includes PI of minors under the age of 14 as sensitive PI. PI handlers shall obtain parental consent and set specific PI handling rules. 20 In addition, handling of sensitive PI shall meet specific transparency requirement regarding the necessity of the handling concerned as well as the impact of such handling on one's personal rights and interests. PI handler shall obtain separate consent and conduct PI protection impact assessment. In practice, we recommend that companies take

[19] Personal Information Protection Law of the People's Republic of China, Art.59.

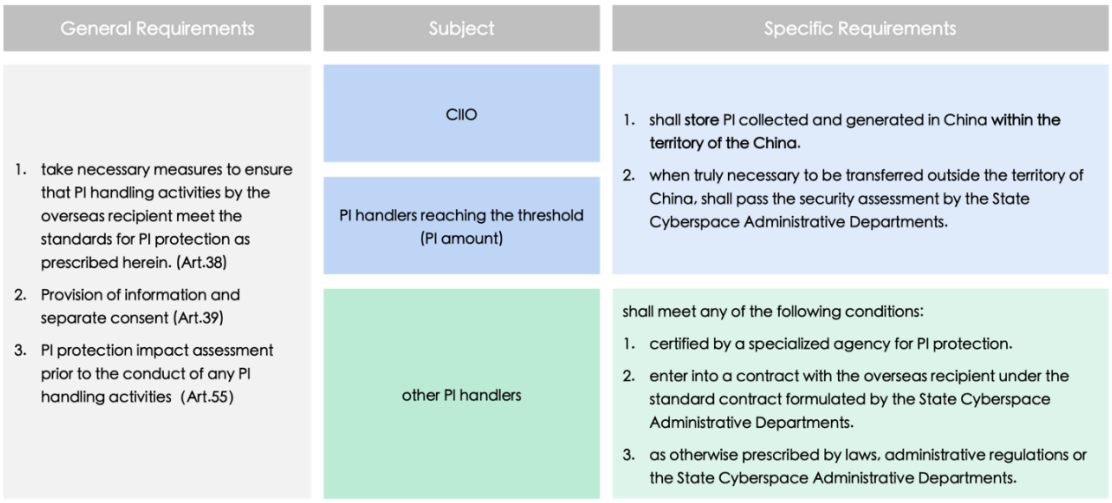
[20] Personal Information Protection Law of the People's Republic of China, Art.31.

more stringent measures concerning sensitive PI protection based on PI classification, develop their minor mode with respect to their products and services, and incorporate verifiable parental consent setting via for example email and publicize children privacy statement respectively.

In addition, the PIPL also sets specific rules with regard to PI handling at public places necessary for maintaining public security and handling of public PI, which further indicates the intention of the PIPL to improve its administration of PI handling activities in response to social development.[21]

5. Cross-border transfer of PI

Cross-border transfer of PI has always been a compliance focus. The PIPL proposes a set of comprehensive PI cross-border transfer paths suitable to China's national conditions. It is worth noting that the PIPL stresses PI handlers' obligation to ensure no PI cross-border transfer will compromise the PI protection level prescribed by this law, which lays down substantial compliance requirements on PI handlers.[22]



Picture 1. PI cross-border transfer mechanism

5.1. General requirements

Companies involved in cross-border transfer of PI shall take necessary measures to ensure that PI handling activities by overseas recipients meet the standards for PI protection as prescribed by the PIPL. In practice, such substantial requirement can be fulfilled through contractual arrangements, regular review and audits and technical monitoring. In addition, PI handlers shall meet the

[21] Personal Information Protection Law of the People's Republic of China, Art.26, Art.28.

[22] Personal Information Protection Law of the People's Republic of China, Art.38.

transparency requirement and provide adequate information with respect to such cross-border transfer activities (e.g., name of the overseas recipient, contact information, purpose and method of handling, type of PI, etc. as required in Art.39 of the PIPL) and conduct PI protection impact assessment (equivalent to Data Protection Impact Assessment (DPIA) under the GDPR) before carrying out any PI cross-border transfer activities.

As regards obtainment of separate consent, one interpretation is that separate consent is only required where such handling is conducted on the basis of consent, as para.2 of Art.13 specifies that no consent is required if any other prescribed legal base suffices. Another interpretation is that separate consent prevails over other legal bases. Further clarification may need to be provided.

In addition to the general requirements above, companies shall also pay attention to industrial specific regulations. For instance, newly released *Several Provisions on Automotive Data Security Management (for Trial Implementation)* stipulates that PI of more than 100,000 PI subjects will be classified as Important Data and subject to the localization requirements.

5.2. Localization of storage

Art.40 of the PIPL specifies that critical information infrastructure operators ("CIIOs") and data handlers reaching the threshold of the amount of PI under processing prescribed by the State Cyberspace Administrative Departments shall store the PI generated and collected in China within the territory of China and CIIOs and data handlers shall pass the security assessment by the State Cyberspace Administrative Departments when such PI is necessary to be transferred outside the territory of China. That is to say, companies, especially MNCs with a global system, can no longer transfer regulated data that are subject to localization requirements to its overseas servers directly. The needs to set up a local IT infrastructure and data center are getting unavoidable. In addition, remote access by a parent company to the data centers of its subsidiaries located within the territory of China would also fall into the regulatory scope of cross-border transfer.

In term of determination of Critical Information Infrastructure ("CII"), the newly released *Security Protection Regulations for Critical Information Infrastructure* (the "Regulations") would shed some light on the definition of CII.[23] According to the Regulations, relevant authorities shall, in light of the actual conditions of respective industries and fields, develop specific rules for identification of CII and file with the public security departments under the State Council for record.[24] That said, further details about security assessment, for instance, whether assessment

[23] Security Protection Regulations for Critical Information Infrastructure, Article 2.

[24] Security Protection Regulations for Critical Information Infrastructure, Article 9.

should be conducted on an annual basis or in accordance with related PI handling purposes, need to be clarified. We recommend that companies keep a close eye on any legislative developments.

5.3. Chinese SCCs and certification

The PIPL Art.38 states that besides as provided in Art.40, data handlers shall either enter into contracts with the overseas recipients in accordance with the Standard Contracts to be formulated by the State Cyberspace Administration Departments (substantially equivalent to SCCs under the GDPR) or conduct personal information protection certification by designated institutions unless otherwise prescribed by laws, administrative regulations or by the State Cyberspace Administrative Departments. The Chinese Standard Contracts have yet been released, but we understand that, by reference to EU SCCs and ASEAN MCCs, at least the nature and scope of handling, method and frequency of handling as well as respective rights and obligations of parties involved would be specified.

6. China's blocking provision and others

The PIPL imposes control on request for data by foreign judicial or law enforcement agencies. Art.41 stipulates that no organization or individual within the territory of China can provide foreign judicial or law enforcement authorities with data stored within the territory of China without the approval of competent authorities. The PIPL sets substantial liability for violating this provision. For example, competent authorities may order rectification, suspension or termination of App or services, confiscate illegal gains, revoke related business licenses and permits of the violator, and levy a fine of up to RMB 50 million or 5% of its turnover of the previous year at the company level and up to RMB 1 million on a directly responsible person in charge.[25] When confronting unreasonable request by foreign judicial or law enforcement agencies, companies can resort to this provision as legal basis. Therefore, the approval mechanism under Art.41 serves as an important system to protect data sovereignty and the legitimate rights and interests of companies and individuals. Yet it is worth noting that such provision may affect domestic companies or MNCs involving in evidence disclosure and information gathering requests in foreign criminal proceedings, civil proceedings, and administrative investigations. Specific approval procedures remain to be further specified.

Art.43, echoing the current international situations, states that China may adopt reciprocal countermeasures against any prohibitive or restrictive measures imposed by any country or region in terms of data related investment or trade. Where any overseas organization or individual engages in a PI processing activity that infringes upon any PI rights or interests of a Chinese citizen or

[25] Personal Information Protection Law of the People's Republic of China, Art.66.

endangers the national security or public interests of China, the CAC may add such organization or individual to the restrictive or prohibitive lists of subjects and take corresponding measures.[26]

7. Rights of PI subject

The PIPL in its Chapter IV prescribes ten rights of a PI subject as shown in the chart below. The PIPL incorporates the right to data portability which states that where a PI subject requests to transfer his/her personal information to another designated PI handler, such request shall be fulfilled by PI handlers when conditions stipulated by the CAC are met.[27] Such provision may help partially reverse the current data monopoly situation or "data island" situation. Art.50 requires that a PI handler shall establish a convenient response mechanism for request of a PI subject to exercise his or her rights. If the PI handler refuses such request, the PI subject may file a lawsuit with the People's Court in accordance with laws.

PIPL	GDPR	CCPA
right to know (Art.44)	information to be provided	right to be informed
right to decide (Art.44)	/	/
right to restrict (Art.44)	right to restriction of processing	/
right to refuse (Art.44)	right to object	/
right to access (Art.45)	right of access	right of access
right to copy (Art.45)	right of access	right of access
right to data portability (Art.45)	right to data portability	right to portability
right to rectify (Art.46)	right to rectification	/
right to delete (Art.47)	right to erasure ('right to be forgotten')	right to delete
related rights in automated decision making (Art.24)	related rights in automated decision making	/
/	/	not to sell

Chart 3. Rights of PI subject (PIPL v. GDPR v. CCPA)

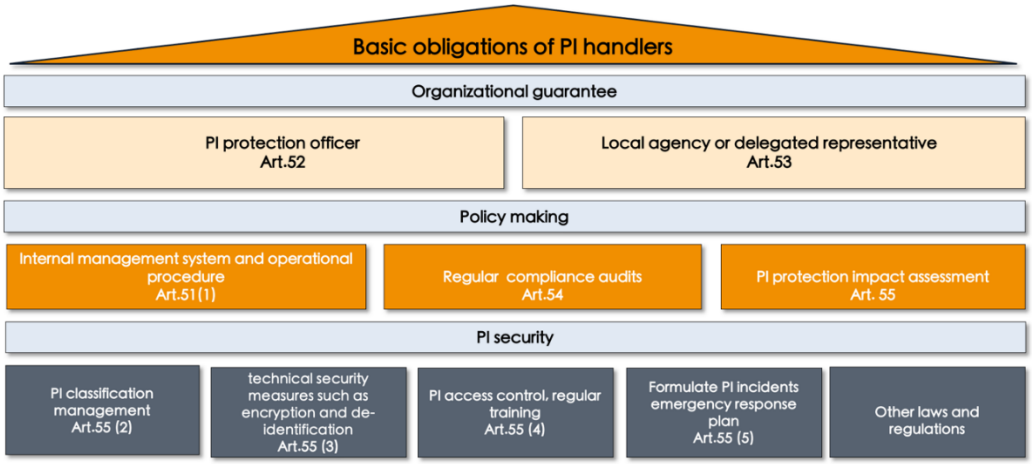
[26] Personal Information Protection Law of the People's Republic of China, Art.42.

[27] Personal Information Protection Law of the People's Republic of China, Art.45, para.2.

Art.49 specifies that where a natural person dies, his or her close relatives may for the purpose of their own lawful and legitimate interests, exercise such rights as accessing, copying, rectifying and deleting the relevant PI of the deceased as prescribed in the PIPL, unless otherwise arranged by the deceased prior to his or her death. The company responding to such request can require the close relatives of the deceased to specify their purposes and at the same time review whether the deceased has made other arrangements.

8. Obligations of PI handlers

Art. 51 to Art. 57 describe the basic obligations of PI handlers and require companies shall set up internal PI protection scheme with the guarantee of organizational structuring and policy making based on PI security. Obligations of PI handlers are categorized as shown in the picture below.



Picture 2. Basic obligations of PI handlers

Art.58 innovatively imposes certain obligations on PI handlers who provide important Internet platform services with a large number of users and complicated business types. Such larger internet platform services provider shall, among others, establish an independent supervisory body mainly composed of external members to supervise its PI protection work, formulate platform rules specifying the standards for PI handling by products or service providers within the platform and corresponding obligations, monitor related conducts of on-platform operators and regularly release social responsibility reports on PI protection for social supervision.