大江橋法律事務所|翰凌律师事务所
中国法律速递
OH-EBASHI | HANLING
CHINA LEGAL NEWSLETTER

A Few Key Points of the China Personal Information Protection Law

Hanling & Partners
Yuchuan Sun
PROFILE

Protection of personal information was not a novel topic in China but was regulated and addressed separately by a few different laws, regulations and national standards. However, different regulations focus on different aspects of this area. For example, the Cybersecurity Law regulates the processing of personal information mainly from the perspective of data security while the Civil Code protects personal information as a part of natural person's "right to privacy". Such a scheme has left a fragmented implementation of the regulation mechanism to the protection of personal information.

As response to such a situation, adopted on 20 August 2021 and came into force as of 1 November 2021, the long-waited Personal Information Protection Law ("PIPL"), for the first time, lays down a coherent and comprehensive framework which marked a new era in the area of personal information protection.

In stead of go over the whole PIPL provision by provision, this article will provide the readers with an insight to some of the most important points of the PIPL.

I. Balance between Protection and Utilization

Although it is titled as "protection law", "protection" is not the only goal and theme of the PIPL. As we all know, a single piece of personal information only has a very limited value. But a much greater value can be created by processing a large quantity of personal information. The huge and rapid advancements in the fields of communication technology, algorithm, network and computer science have rendered processing of millions or billions personal information both technically and economically practical. New business concepts and tools like automated decision making, customer profiling, e-commerce and online behavioural advertisement would not have been possible without processing personal information on a large scale. Also, processing personal information could be of great help to manage public affairs. It has been clear to everyone that utilization of personal information could be of almost unlimited value both in the public and the private sectors. And because of such a great potential, we are seeing increasing unlawful actions toward personal information. Especially in China, incidents like system breaching, misappropriation, unlawful collection and transfer of personal information have been deemed as serious problems.

Therefore, balance between the protection of personal information and free flow of personal information shall be well maintained. The statutory obligations to process personal information in a lawful manner will place great responsibilities upon the processors thus may, to some extent, impair the free flow of the personal information. Like GDPR, the PIPL is clear on this point. Article 1 of the PIPL states that this law is formulated "with a view to protect personal information" as well as "promoting the reasonable utilization of personal information". When reading the rest of the PIPL, we shall bear in mind that it is the most fundamental purpose of the PIPL to balance the "protection" and "utilization" and we may find most of the mechanisms and regulations under the PIPL are designed to achieve such a balance.

II. Definition of "Personal Information"

The PIPL has generally followed the same approached of GDPR to define personal information as "information in relation to an identified or identifiable natural person that

is recorded electronically or otherwise". Before the enactment of the PIPL, definition of personal information in Chinese law has taken the approach to focus on "identification". For example, Article 1034 of the Civil Code defines the personal information as "information that can be used to identify particular natural person individually or jointly with other information". And Article 76 of the Cybersecurity Law defines the personal information as "all information that can be used to identify particular natural person individually or jointly with other information." Under such definitions, information that are not likely to be used to identify a natural person will not constitutes "personal information".

Based on the definition of personal information under the PIPL, a two-step test shall be made to identify if an information is personal information or not. Firstly, we must see if there is an "identified" or "identifiable" natural person or not. If it is, then we shall see if such information is "in relation to" such a natural person or not. The first test will be more important. In practice, it is relatively easy to judge if a natural person is "identified". But it is more difficult to judge if a natural person is "identifiable". Theoretically speaking, any information even those only very remotely related to a natural person can be used to identify a natural person jointly with other information, so long as adequate quantity of information can be collected, which renders almost everyone to be "identifiable". But in the real world, given the nature, size and business of the information processor, various facts shall be considered to judge if a natural personal constitutes an "identifiable natural person" to a certain processor and it is difficult to establish a one-fit-all standard. For example, a giant online shopping company may have more opportunities, a stronger incentive and more technical tools than a small size ordinary trading company to collect various information to identify a natural person thus renders a particular natural person more likely to be "identifiable" to the online shopping company than to the trading company.

Also, the concept of "personal information" shall be carefully distinguished from the concept of "right to privacy" under the Civil Code. They are not concepts inclusive to each other but have some overlapping parts. According to Article 1032 of the Civil Code, "privacy" means the tranquility of a natural person's private life and private space, private activities, private information that a natural person does not wish to be known to other persons. Therefore, the concept of "privacy" is not limited to the dimension of "information". Behaviors like sneak shot or unlawful open of private mail are infringements to "privacy" but not necessarily related to personal information. And Section 3 of Article 1034 of the Civil Code states that "privacy information" among "personal information" shall be regulated as a "right to privacy" and if there is no relevant regulation, then regulations regarding protection of personal information shall apply.

III. Safe Harbor: Anonymization

As mentioned above, one core value of the PIPL is to balance the "protection" and "utilization" of personal information. When a piece of information has been processed to a form which can no longer be used to identify a particular natural person, then the possibility of any damages to be caused upon the natural person due to a leak or unlawful use of such information would become relatively remote. And under such a circumstance, the "utilization" shall be prioritized over the "protection". This is why the PIPL expressly excludes anonymized personal information from the scope of "personal information" which renders the processing of anonymized personal information no longer need to be regulated by the PIPL (but such kind of processing may otherwise be regulated by Data Security Law).

What does "anonymization" mean under the PIPL? Article 73 of the PIPL defines "anonymization" as "a process whereby personal information are processed such that a specific natural person cannot be identified and that the personal information cannot be restored". And the Article 73 also defines a similar concept "de-identification" as "a process whereby personal information are processed such that a specific natural person cannot be identified without the help of additional information" which is similar to the concept of "pseudonymization" under GDPR. The key different between "anonymization" and "de-identification" is when a personal information is "de-identified", it can still identify a specific natural person if combined with addition information while in the case of "anonymization", personal information can no longer be used to identify specific natural person with or without additional information.

Introduction of "anonymization" provides a safe harbor for personal information processing. But in practice, it is hard to achieve a complete "anonymization". Firstly, under many circumstance like electronic commerce or

behavioural advertisement, anonymization will not be a possible option for the processor since identifying a specific natural person is the key value or function of such application. Secondly, a complete "anonymization" is technically difficult to achieve. Theoretically speaking, so long as the processor can collect enough information, any anonymized personal information can be restored to identify specific natural person. Thus, in the practice, like the concept of "identifiable", it may be necessary to establish a case-by-case approach with regard to the judgement of "anonymization".

IV. Lawful Collection of Personal Information

The concept of "process" under the PIPL has covered all aspects of processing personal information including collection, storage, utilize, transfer and provision. But there is no doubt that lawful collection of personal information is the condition to lawful processing of personal information.

Before the enactment of the PIPL, "consent" is the only ground for a lawful collection of personal information. For example, Article 41 of the Cybersecurity Law states that the network operator shall collect and use personal information in accordance with the principle of lawfulness, fairness and necessity. Publish the policies regarding the collection and utilization of personal information, expressly state the purposes, methods and scope for collection and utilization of personal information **and obtain the consent by the natural person.** Article 1035 of the Civil Code states that collection of personal information **shall be consented** by the natural person, unless the laws and regulations provide otherwise.

Unlike previous legislations, Article 13 of the PIPL provides a few scenarios that personal information may be processed without obtaining consent. Namely, where the processing of personal information is necessary for the conclusion or performance of a contract to which the relevant natural person is a party or is necessary to carry out human resource management, or where processing of personal information is necessary for the performance of statutory duties or obligations, or where processing of personal information is necessary to respond to public health emergency, to protect life, health and property safety of natural person in an emergency, or where processing of person information for the purpose of news report and public opinion supervision, or process disclosed personal information within a reasonable scope. While keeping "consent" as the most fundamental ground for lawful processing, the PIPL does provides more flexibilities in secure a lawful ground for processing personal information.

However, exempt of "consent" does not at the same time exempt the obligation of "inform". Article 17 of the PIPL requires that before processing personal information, a processor shall inform, in truthful, accurate and complete manner, the name and contact information of the personal information processor, purpose, method, categories and storage duration of processing, natural person's right to their personal information and procedures to exercise them. Such obligation to inform will not be exempted merely because "consent" is not required.

And if the processor decide to rely on "consent" as the ground for lawful processing, the processor shall ensure that the consent is an "informed, volunteer and express" consent. In practice, some companies only set out a very outlined privacy policy without much detailed information. Such an approach may face compliance risk under the PIPL since an outlined policy will make the natural person's consent nat to be an "informed" one. And under some special circumstances, a "separate consent" is required addition to a general one. Such circumstances include providing persona information to a third party, disclose personal information, process sensitive personal information and transfer personal information to overseas areas. But the PIPL does not clearly address what kind of consent will amount to a "separate consent". Generally, the processor can obtain a separate consent by preparing and providing a separate personal information statement or to make relevant content in a general personal information statement conspicuous.

The processor shall bear in their mind that the obligation of "inform and consent" may sometimes be a big burden. Especially, when a processor is collecting personal information from another processor. When the processor collects directly from a natural person, it is relatively easy to inform and obtain consent from such person, but when collecting personal information from another processor, it is difficult to obtain an informed consent from relevant natural person. Under such a circumstance, the processor shall carefully check the origin, collection procedures and scope of authorization to avoid compliance risks.

V. Cross-border Transfer of Personal Information

Cross-border transfer of personal information is a hot topic during the legislative process of the PIPL. Before the PIPL, the public comment version of the *Measures for the Security Assessment of Cross-border Transfer of Personal Information* requires a universal security assessment on any cross-border transfer of personal information which raised a great concern especially in the multinational enterprises. Under the context of globalization, more and more cross-border transfer of personal information occurs in the daily business activities. We have been hearing from multinational enterprises that they are quite confused if transfer of personal information for pure employment management purpose (transferring employees' personal information to their overseas headquarter) shall also be subject to such security assessment.

The PIPL now provides a clearer approach to the cross-border transfer of personal information. According to the Article 40 of the PIPL, critical information infrastructure operator (CIIO) and personal information processor that processes personal information up to a certain volume shall store the personal information collected and generated within in the territory of PRC in mainland China and if the personal information are genuinely necessary to be transferred overseas, the processor shall pass the security assessment conducted by the national cybersecurity authority. And for cross-border transfer of personal information under other circumstances, Article 38 of the PIPL states that the personal information processor shall either obtain personal information protection certification by professional institutes or enter into a contract with the overseas recipient according to the standard contract formulated by the national cybersecurity authority.

However, the PIPL is not clear about under what circumstance that the processor shall obtain personal information protection certification and under what circumstance entering into the standard contract will suffice. But it is very likely that a standard contract will be enough for transfer of personal information between a group of companies merely for the purpose of internal management..

As to the security assessment for cross-border transfer of personal information, on 29 October 2021, the Cyberspace Administration of China (CAC) has released the draft of the *Measures for the Security Assessment for Cross-border Transfer of Data*. The Measures regulates the security assessment not only for cross-transfer of "personal information" but also covers the cross-border transfer of "data" under the Data Security Law. The Measures requires that when a processor who has processed personal information up to one million natural person wishes to transfer personal information overseas, or more than 100 thousands natural persons' personal information has been accumulatively transferred overseas or more than 10 thousands natural persons' sensitive personal information has been accumulatively transferred overseas, then a security assessment must be conducted and passed. The Measures also provides a framework for such security assessment but still leave much space for further regulations. At the time of completion of this article, the Measures is still in the process of gathering public comments.

VI. Wrap-up

Further to the key points that have been discussed hereunder, there are a few other points in the PIPL worth paying attention to, such like natural persons' rights to personal information, the burden of proof in personal information disputes and processing sensitive personal information. The PIPL sets up the framework on protection and utilization of personal information but still leaves much space for further implementation rules and interpretation.

For inquiries, questions or comments, please contact us at info_china@ohebashi.com or suny@hanlinglaw.com