DEACONS
的近律師行

Corporate Commercial Client Alert

China Trade & Investment

4 October 2021

How to Transfer Personal Information out of China under the Personal Information Protection Law

Edwarde Webre and Joyce Mu

The *Personal Information Protection Law* (the "PIPL") will take effect on 1 November 2021. It follows the fundamental rules on protecting personal information under the *Cybersecurity Law and Civil Code* of the People's Republic of China (PRC).

We highlight below the key points in the PIPL on processing personal information within China, and outbound transfer of personal information, which may impact businesses whether they are operating in or outside the PRC.

1. Definitions

Among others, the PIPL defines the following terms:

Personal Information is all kinds of information related to the identified or identifiable natural persons that is recorded by electronic or other means, excluding the information processed anonymously ("PI"). Note that the PI is distinguished from the Privacy defined under the Civil Code as "a natural person's private life peace, as well as private space, private activities and private information that do not want to be known by others". For instance, the name and contact number of a natural person are PI but not Privacy.

Processing of Personal Information includes the collection, storage, use, transform, transmission, provision, publication and deletion etc. of Personal Information.

Personal Information Processor refers to an organisation or individual that independently determines the purpose and method of the processing in the processing of personal information ("Processor"). The PI Processor is essentially a "PI Controller". Actually the concept of "PI Controller" has been used in the judicial practice, and it is defined as "an organisation or individual capable of deciding the purpose and method of the PI processing" in the recommended national standard "Information security technology - Personal information security specification" (GB/T 35273-2020, effective as of 1 October 2020).

2. Basic Rules for Personal Information Processing

- **Application and Extra-Territoriality**

  The PIPL is applicable to the processing of PI inside the PRC. The PIPL also has extraterritorial application where the processing of the PI is related to the provision of services or products to individuals in China or analysing or evaluating the activities of individuals in China.

  There is currently no specific requirement of targeting the PRC. The PIPL may consequently be applicable to a foreign company receiving online orders from the PRC individuals on non-Chinese websites that are not specifically targeting PRC nationals. It is expected that the scope of extraterritorial application will be clarified.

- **Minimum scope and storage term**

  The PIPL requires the processing of PI shall be for a definite and reasonable purpose, be directly related to the purpose of processing and shall be conducted in a way that minimises the impact on personal rights and interests. The collection of PI shall be limited to the minimum scope for achieving the purpose of processing and

excessive collection of PI is not allowed. The retention period of PI shall be the minimum period necessary for achieving the purpose of processing, unless otherwise stipulated by laws or administrative regulations.

- **Voluntary and express consent**

  The PIPL follows the principle of "inform & consent" in the Cybersecurity Law, and requires the processing of PI to be subject to the voluntary and express consent of the individual made upon the receipt of sufficient information.

  Separate consent is required in certain situations, including when personal information will be disclosed to a third party, disclosed publicly or transferred to a party outside of PRC. The specific nature of separate consent may be clarified in the future, but it is expected that a separate unbundled and opt-in consent will be required.

- **Withdrawal of consent**

  An individual shall have the right to withdraw his/her consent, and the Processor shall not refuse to provide products or services solely on the ground that the individual does not give consent or withdraws his/her consent, unless the processing of PI is necessary for providing products or services to that individual.

- **Sensitive PI processing**

  Sensitive PI refers to the PI that is likely to result in damage to the personal dignity of any natural person or damage to his or her personal or property safety once disclosed or illegally used, including such information as biometric identification, religious belief, specific identity, medical health, financial account and whereabouts and tracks, as well as the PI of minors under the age of 14.

  The PIPL imposes more onerous responsibilities regarding the processing of Sensitive PI. Only for a specific purpose and sufficient necessity, and strict protection measures have been taken, may a Processor process Sensitive PI. A previous consent given in relation to non-sensitive personal information will not suffice and a standalone consent specific for the process of Sensitive PI shall be obtained. Further, the individual should be informed of the necessity and impact on his/her personal interests resulting from processing his/her Sensitive PI, except for the circumstances that may be exempted from informing the individual according to the PIPL.

- **Exemption to consent**

  On the other hand, the PIPL provides the below five circumstances under which PI could be legally processed without the individual's consent, which substantially extends the scope of circumstances where the Processing of PI is permitted:

  1) where it is necessary for concluding or performing a contract to which the individual concerned is a party or for the implementation of human resources management in accordance with the labour rules and regulations legally formulated and the collective contract legally concluded (note that this must be supported by a contractual relationship and sufficient evidence showing the necessity);

  2) where it is necessary for performing statutory duties or statutory obligations;

  3) where it is necessary for responding to a public health emergency or for protecting the life, health and property safety of a natural person;

  4) where such acts as news reporting and supervision by public opinions are carried out for the public interest, and the Processing of PI is within reasonable scope;

  5) where it is necessary to process the PI disclosed by the individual concerned or other PI that has been legally disclosed within a reasonable scope in accordance with the PIPL; or

  6) other circumstances provided by laws or administrative regulations.

- **Person in Charge**

  Similar to the Cybersecurity Law and the Data Security Law, a person in charge of PI protection ("Person in Charge") shall be designated by the Processor when the volume/quantity of PI reaches a threshold (not known yet) specified by the Cyberspace Administration of China (CAC). The Personal in Charge shall be responsible for supervising the activities of processing PI and the adopted PI protection measures. The Processor shall make public the contact details of the Person in Charge, and file the name and contact details of the Person in Charge

with competent government authority. Obviously there would be certain overlap among the duties of the person in charge under the Cybersecurity Law, the Data Security Law and the PIPL, and these laws do not prohibit a person from holding the post of different types of personal in charge simultaneously. It is yet to see if a third party (as opposed to an employee of the Processor) could be engaged as the Person in Charge.

3. Transfer of Personal Information out of the PRC

Pursuant to the PIPL, a Processor may only transfer PI to a recipient outside the PRC when any of the following conditions is met:

1) the Processor has passed the security assessment organised by the CAC;

2) the Processor has been certified by a recognised institution in respect of the protection of personal information as required by the CAC;

3) the Process has entered into a contract with the overseas recipient, in a standard form formulated by the CAC, specifying the rights and obligations of each party; or

4) other conditions required by the law, administrative regulations or the CAC.

Note that the Processor shall take necessary measures to ensure that the activities of processing PI by the overseas recipient meet the standards for protection of PI as prescribed in the PIPL. However, it is yet to see what specific measures/activities the Processors shall take to satisfy the CAC.

The use of the standard form contract would appear to be the easiest method of obtaining clearance. However, the standard form contract has not yet been issued.

In addition, the Processor shall inform each data subject the followings and obtain a standalone consent for cross-border transfer:

a) name, contact details, purpose of processing, and method of processing of the overseas recipient;

b) type of PI to be transferred; and

c) method and procedure for the data subject to exercise his/her legal rights stipulated in the PIPL against the overseas recipient.

Note that the critical information infrastructure operators (CIIO) and the Processors whose volume/quantity of PI reaches a threshold (not known yet) prescribed by CAC shall store within the PRC the PI collected and generated onshore. However, when there is actual need to transfer PI overseas, the cross-border transfer shall first pass the security assessment organised by the CAC. On a related note, the Measures on Security Assessment for Cross-border Transfer of Personal Information made on basis of the Cybersecurity Law has not yet been not finalised. The last draft issued in June 2019 states that the cross-border transfer of personal information shall not be allowed if it is identified by the security assessment that such cross-border transfer may affect national security or damage public interest, or that it is difficult to effectively protect the safety of personal information. Nonetheless, as consistent with the Data Security Law, the PIPL prohibits the Processor from providing the PI stored within the PRC to foreign judicial or law enforcement authorities without approval of competent regulator. This prohibition may put multinationals or PRC parties in a dilemma during offshore lawsuits. It is yet to see what the procedures and timeframe would be on applying for such approval.

With respect to official requests made directly to PRC authorities by foreign judicial or law enforcement authorities, the PRC competent authorities shall handle the cross-border provision of PI in accordance with the applicable law as well as the international treaties and agreement concluded or acceded to by the PRC, or under the principles of equity and mutual benefit.

A foreign entity processing PI offshore may be required to establish an office onshore or designate an agent in the PRC to deal with authorities on PI protection related issues. A registration with the authorities will be required.

4. Legal Consequences

The PIPL provides heavy penalty against a violating party. In particular, the cap of penalty is increased to RMB50 million (or 5% of the turnover in the preceding year) against serious violation by a Processor, in addition to the administrative penalties following the Cybersecurity Law, such as rectification, confiscation of illegal gains, warnings,

penalties under RMB 1 million against the person directly in charge and other directly liable persons, business suspension, business halt for rectification, and the revocation of relevant permit or business license.

Apart from the administrative penalties, the PIPL also provides civil compensation for the infringement of PI, to the extent of the losses caused to the individuals concerned or the benefits obtained by the Processor.

As for the offshore entities or individuals which PI processing activities jeopardize the PRC's national security or public interests or PRC nationals' rights and interests, the CAC may put such offshore entities or individuals in a blacklist, and restrict/prohibit them from being provided with PI.

5. Conclusion

As the first piece of specific legislation, the PIPL is a symbol that the protection of PI in China is stepping into a new stage. In the era of information, this topic is receiving much needed public attention. With the continuous improvement of laws and regulations, enterprises may in the future be confronted with stricter data privacy compliance requirements than ever. We may also expect to see headlines of big data breach fines imposed by the PRC authorities, following the suit of the US and EU.

Deacons will pay close attention to the status of legislation on personal information protection in China, and provide updates that may impact your business. For tailored measures and practical advices to manage risks in personal information processing, please contact us.

Want to know more?

Cynthia Chung
Partner
cynthia.chung@deacons.com
+852 2825 9297

Machiuanna Chu
Partner
machiuanna.chu@deacons.com
+852 2825 9630

Edwarde Webre
Partner
edwarde.webre@deacons.com
+852 2825 9730

Elsie Chan
Partner
elsie.chan@deacons.com
+852 2825 9604

Helen Liao
Partner
helen.liao@deacons.com
+852 2825 9779

Stefano Mariani
Partner
stefano.mariani@deacons.com
+852 2825 9314