

A Guide to China's Personal Information Protection Law

By David Pan | Xun Yang
Nigel Zhu | Susan Deng | Jianqi Yang | Emily Hu

In strengthening personal information protection, China has been issuing laws and regulations at a fast pace. Followed by the *Cybersecurity Law*, the *Civil Code* and the *Data Security Law*, an overarching law which sets forth a basic framework for personal information protection has long been anticipated. After three drafts and deliberation, China passed the *Personal Information Protection Law* (hereinafter referred to as the “PIPL”) on August 20, 2021, which will be effective on November 1, 2021.

Highlights of the PIPL:

- 1) Adds “employment” as a legal basis for personal information processing.
- 2) “Separate consent” must be obtained for processing of sensitive personal information.
- 3) Right to portability for personal information subjects.
- 4) Clarifies handling of personal information of the deceased.
- 5) Changes “infrastructural Internet platform services providers” in previous drafts to “important Internet platform services providers”, and imposes special corresponding obligations.
- 6) Adds “removal from APP store” as a penalty on non-compliant APPs.
- 7) Increases amount of fines and adds individual person liability.
- 8) Introduces rules of consumer public interest lawsuits.

For more Llinks publications,
please contact:

Publication@llinkslaw.com

1. Definition of “Personal Information”

Under the PIPL, “personal information” refers to “information that is recorded by electronic or other means and is related to any identified or identifiable natural person”. It expands the scope of personal information by adopting the “relevance” standard, rather than the traditional “identifiability” standard. Information will be considered as “personal information” if (1) such information can be used to identify a certain person, or (2) such information is related to a particular identified/identifiable person.

In judicial practice, MAC (Medial Access Control) address is recognized by the court as a type of personal information because the MAC address, if combined with other information, can lead to a specific phone number; also, a court ruled that “friend list” is personal information in another case because “friend list” both identifies and relates to a natural person. With the fast evolvement of data technology, companies can gather and aggregate more and more personal information from multiple sources, and companies will continuously enhance their identification capabilities. In this context, though some information processed by companies is not deemed as personal information previously, it will become related to an identifiable natural person, i.e. personal information protectable by the PIPL. In other words, the scope of personal information will keep expanding. It is advisable for companies to keep this in mind when identifying personal information, and fulfill relevant personal information protection obligations accordingly.

2. Legal Basis of Personal Information Processing

The PIPL takes consent as the principal basis for lawful personal information processing, and adds other legal grounds for processing:

- 1) Execution of a contract to which the personal information subject is a party, or implementation of human resource management in accordance with lawful labor manuals and collective labor contracts;
- 2) Fulfillment of legal responsibilities or obligations;
- 3) Response to public health emergencies, or for the purpose of protecting natural persons’ health and safety or property in emergencies;
- 4) Processing personal information in news reporting or public sentiment monitoring in the public interest within a reasonable scope;
- 5) Use of publicly-available information within a reasonable scope.

Thanks to this breakthrough provision, companies may consider reasonably relying on legal grounds other than consent. For example, companies can quote “1) to process employees’ personal information without their consent”, provided that the processing can be justified as necessary for human resource management. To avoid any risk, companies shall follow the principle of necessity and adopt a restrictive definition of “necessary for human resources management”.

In terms of processing of personal information that has been made public, because the definitions of “public” and the scope of “reasonableness” remain unanswered by the PIPL, companies are advised to take caution in relying on 5) for processing personal information made public.

3. Processing of Sensitive Personal Information

Sensitive personal information refers to personal information that is likely to result in damage to one's dignity or personal or property safety once disclosed or illegally used, including information of biometric identification, religious belief, specific identity, medical health, financial account and whereabouts and tracks, as well as any of personal information of minors under the age of 14. In terms of processing sensitive personal information, the PIPL calls for a "separate consent".

According to a draft of national standards *Information Security Technology – Guidelines for Personal Information Notices and Consent*, to obtain a valid "separate consent", a personal information processor* must (1) inform the individuals of the purpose, method, scope of the personal information, and the storage time and the security measures in a form of "enhanced notification" and (2) obtain explicit consent of the individuals (take the initiative to make affirmations). The "enhanced notification" should disclose relevant information in a way that the individuals cannot bypass (such as "pop-up" window), so that personal information subjects must make a decision before moving on to next webpage.

【Note: The concept of "personal information processor" under the PIPL is similar to the data controller under the GDPR.】

Importantly, considering the broad use of facial recognition technology, the PIPL imposes a strict restriction on the processing of facial information. Except for the purpose of public security solely, when a personal information processor installs and uses image capture and face recognition devices in public places, it must obtain separate consent from individuals (or their guardians in case of minors). In certain offline scenarios, it could be quite hard, if not impossible, to obtain separate consent from personal information subjects. It remains to be seen how this rule will be enforced.

4. Prohibition on Big Data-enabled Price Discrimination

In recent crackdowns against *APP's infringement on user rights*, regulatory authorities found that some APPs have violated the principle of necessity by collecting personal information irrelevant to the services they provided. In response, the PIPL specifically regulates the "necessity" of personal information processing, requiring that the processing of personal information must be directly related to the purpose of processing and must be conducted in a way that causes minimum impact on personal information subjects' rights. Meanwhile, personal information must be collected within the smallest scope required for achieving the processing purpose. It can be reasonably predicted that after the PIPL comes into effect, regulatory authorities will focus the "necessity" of APPs' personal information collection with references to the *Provisions on the Scope of Necessary Personal Information for Common Types of Mobile Internet Applications*.

Excessive personal information is very often collected for big data analysis and user profiling, which enables differentiated treatment (including price discrimination) on consumers. The PIPL explicitly prohibits this

practice. According to Article 42 of the PIPL, companies shall conduct a personal information protection impact assessment before they implement any new automated decision-making. Article 24 of the PIPL additionally requires that companies may not offer unreasonable differential treatment of individuals in terms of price or other trading conditions. Besides, companies should provide individuals with convenient methods to opt-out of automated decision-making. In addition to the PIPL, the Cyberspace Affairs Committee (“CAC”) will also publish special regulations on recommendation algorithm which requires transparency of automated decision-making.

5. Cross-border Transfer of Personal Information

The PIPL provides a detailed framework for cross-border personal information transfers, and the requirements differ depending on the type of personal information processors. In summary:

- 1) CIIOs and entities processing personal information the amount of which exceeds the threshold prescribed by the authority are required to locally store personal information collected in China and conduct government-led data cross-border transfer review before they can export personal information out of China;
- 2) All other personal information processors must choose to (i) go through the data cross-border transfer assessment mentioned above, (ii) complete personal information protection certification conducted by a specialized institution, or (iii) conclude a standard contract (which is to be formulated by the CAC) with the overseas recipient, in order to legally export personal information.

In addition, companies should meet the following requirements before providing any personal information:

- 1) fulfilling the obligation of notice to the personal information subjects;
- 2) obtaining separate consent;
- 3) conducting a risk assessment prior to the transmission;
- 4) taking measures to ensure the processing of personal information by the recipient meets the standards provided by the PIPL.

Notably, without the approval of the competent authority, companies in China shall not provide personal information stored within China to any foreign judicial or law enforcement authorities.

6. Individual Rights

Individuals’ rights set out in the PIPL are similar to data subjects’ rights under GDPR. Specifically, individuals will have the right to (1) know the processing activities, and decide whether to give consent to, restrict, or object to that processing; (2) access and receive a copy of the personal information processed; (3) correct inaccurate or incomplete personal information; (4) delete personal information under certain circumstances; and (5) withdraw consent. These personal information rights extend beyond an individual’s death and can be exerted by close relatives of the deceased, except as otherwise arranged by the deceased prior to his or her death.

Moreover, the PIPL grants to individuals the right to portability -- the ability to obtain and reuse their personal information across different service providers. According to Article 45 of the PIPL, where individuals request the transfer of their personal information to designated personal information processors, and where the conditions specified by the CAC are met, the previous processor must offer a means for the transfer.

Such mechanism for individuals' personal information rights raises the compliance bar for the type, format and structure of personal information held by companies and will have a direct impact on the product design and business process related to personal information handling.

7. Penalties

The PIPL provides for harsh punishments on personal information violations. The PIPL introduces progressive sanctions on infringing APPs, which is "Reprimand Notice → Ordered rectification → Removal from APP store". Such approach is consistent with previous law enforcement in cracking down on non-compliant APPs.

Compared with the *Cybersecurity Law*, the PIPL significantly raises penalties. Specifically, in severe cases, a violator may be fined up to RMB 50 million, or 5% of its revenue of the preceding fiscal year. In addition to a fine up to RMB 1 million, the responsible persons may be prohibited from serving as directors, supervisors, senior managers and personal information protection officers. If any illegal processing of personal information constitutes a criminal offence, administrative regulators will hand over the case to public security organs.

8. Personal Information Related Litigation

In order to protect individuals' personal information, the PIPL introduces a public interest litigation mechanism. For violations of the rights of a large number of people, procuratorates, consumer rights organizations, and other competent organizations may bring a class action against the entity on behalf of the victims. It is worth noting that in addition to civil damages, the infringer may need to bear administrative and criminal responsibility.

Moreover, considering that individuals often lack the capability to provide sufficient evidence to prove losses suffered, the PIPL puts the burden of proof on personal information processors. Personal information processors who fail to prove their innocence for the damages caused will be held liable. As such, it is advisable for companies to preemptively gather compelling evidence which can prove that they have fulfilled personal information protection obligations and have adopted strict security measures.

Imposing stricter curbs on personal information processing, the PIPL will significantly affect companies that engage in personal information processing in China. Accordingly, personal information processors may want to conduct due diligence to thoroughly understand what sorts and volume of personal information which they collect and how the personal information is used, stored, processed, transferred and disclosed, and most significantly, to take steps to remediate gaps.

If you would like to know more information about the subjects covered in this publication, please contact:



David Pan
+86 21 3135 8701
david.pan@llinkslaw.com



Xun Yang
+86 21 3135 8799
xun.yang@llinkslaw.com

SHANGHAI

19F, ONE LUJIAZUI
68 Yin Cheng Road Middle
Shanghai 200120 P.R.China
T: +86 21 3135 8666
F: +86 21 3135 8600

BEIJING

4F, China Resources Building
8 Jianguomenbei Avenue
Beijing 100005 P.R.China
T: +86 10 8519 2266
F: +86 10 8519 2929

SHENZHEN

18F, China Resources Tower
2666 Keyuan South Road, Nanshan District
Shenzhen 518063 P.R.China
T: +86 755 3391 7666
F: +86 755 3391 7668

HONG KONG

Room 3201, 32/F, Alexandra House
18 Chater Road
Central, Hong Kong
T: +852 2592 1978
F: +852 2868 0883

LONDON

1/F, 3 More London Riverside
London SE1 2RE
United Kingdom
T: +44 (0)20 3283 4337
D: +44 (0)20 3283 4323



www.llinkslaw.com



Wechat: LlinksLaw

WE LINK LOCAL LEGAL INTELLIGENCE WITH THE WORLD

This publication represents only the opinions of the authors and should not in any way be considered as legal opinions or advice given by Llinks. We expressly disclaim any liability for the consequences of action or non-action based on this publication. All rights reserved.

© Llinks Law Offices 2021