The Coming PIPL: Have you prepared?

By Xun Yang | Yuwei Xia

Tomorrow, 1 November 2021, the Personal Information Protection Law ("**PIPL**") will come into effect. This would be the first piece of comprehensive legislation on personal information protection. Since tomorrow, all kinds of personal information, electronic or paper-based data, employee data, consumer data or otherwise, will be subject to the same personal data protection rules and breach of these rules will result in civil, administrative and even criminal liabilities.

PIPL is not drafted from scratch. Rather, it reflects the personal information practice since the effectiveness of the Cyber Security Law in 2017. It also addresses a number of issues in the personal information protection regime which have long been controversial. It is determined to be milestone legislation on personal information protections.

Tomorrow, those business operators which handle personal information during their course of business are facing stricter rules on personal information protections. Have you prepared for such stricter rules?

1. Highlights of PIPL

PIPL sets out comprehensive rules on full-circle protections of personal information, including collection, storage, usage, process, transmission, provision, disclosure, etc., which are collectively defined as "handling" under the PIPL. In particular, PIPL strengthens the personal information protections from the following aspects.

如果您需要本出版物的中文本，
请联系:

Publication@llinkslaw. com

For more Llinks publications,
please contact:

Publication@llinkslaw.com

(1) Extraterritorial Effect

PIPL introduces an extraterritorial effect that personal information handling activities outside of China, concerning interest of China, would be subject to PIPL.

According to Article 3 of the PIPL, the handling of personal information outside of China will be subject to PIPL if either (i) personal information is handled for the purpose of providing products or services to persons residing in China or (ii) personal information is handled to analyze or to assess persons residing in China.

In order to enforce PIPL against those foreign companies, PIPL requires that those foreign companies subject to PIPL establish representative offices or appoint officers taking charge of personal information protection matters. The contact information of such offices or officers must be filed with the government.

Additionally, PIPL proposes the measures to sanction foreign companies which violate PIPL. According to Article 42 of PIPL, if a foreign company handles personal information in a manner prejudicing to personal interest of a Chinese citizen, to public interest in China or to national security of China, it may be included in a blacklist to which the provision of personal information will be banned. Consequently, Chinese individuals or entities will not be allowed to provide personal information to those entities on the blacklist.

(2) Full-circle Protections of Personal Information

PIPL sets out full comprehensive rules on collection, storage, processing, and disposal of personal information and introduces stricter rules on protection of sensitive data.

Firstly, PIPL sets out a series of legal grounds where personal information can be handled. In addition to "notification and consent" which has been long been considered the necessary legal ground for handling personal information, PIPL, for the first time on the national law level, broadens the grounds for handling personal information, including, among others, the circumstances where it is necessary to perform contractual obligations or to perform statutory obligations. Please note that even in circumstance where consents are not required for handling personal information, notification of the scope, purpose, and manner of handling personal information is still required.

Secondly, PIPL sets out detailed requirements for notification and consent. In particular, separate consents are required to be obtained from relevant individuals when: (a) handling sensitive personal information; (b) provision of personal information; (c) public disclosure of personal information; or (d) export of personal information. However, how a “separate consent” requirement is implemented remains to be seen.

Thirdly, PIPL sets out rules on transfer of personal information. PIPL divides personal information transfers into four scenarios: (1) joint handling of personal information, (2) provision of personal information, (3) entrusted handling of personal information, and (4) personal information transfers in a business transfer context. PIPL imposes different requirements, such as notification, separate consents, etc. on personal information transfers in different scenarios in order to ensure the security levels of personal information protections will not be prejudiced because of the transfers.

(3) Export of Personal Information

PIPL sets out strict rules on export of personal information. In line with the Cyber Security Law, operators of critical information infrastructure are, in principle, required to store personal information in China except for necessity where government risk assessment is required. PIPL also requires those companies which handle personal information at an amount reaching a certain threshold to follow the same rule. According to the draft Data Export Security Assessment Measure published on 29 Oct. 2021 for public consultation, such threshold could be (i) export by data handler which handles personal information about 1 million individuals or above; or (ii) export of personal information accumulatively about 100 thousand or above or export of sensitive personal information accumulatively about 10 thousand or above.

Moreover, for other export of personal information, one of the following grounds must be met: (a) passing the security assessment by Cyberspace Administration of China ("**CAC**"); (b) obtaining certification of data security by a professional body recognized by the CAC; (c) entering into an agreement with the overseas recipient with provisions governing the rights and obligations of the parties based on a template contract to be released by the CAC; or (d) other requirements as provided by relevant laws and regulations. Additionally, an internal risk assessment is required before exporting personal information.

(4) Individuals' Rights

Similar to GDPR, PIPL grants relevant individuals the right to control the personal information relating to them. These rights include the right to know what personal information has been collected or processed, the right to have a copy of the personal information being collected or process, the right to update or correct the personal information, and the right to withdraw consents to handling personal information. Additionally, PIPL for the first time introduces the concept of "portability," and requires that if relevant individuals request that their personal information be transfer to a third party, to the extent conditions imposed by CAC are satisfied, such request be respected. It remains unclear what CAC's conditions would be.

(5) Legal consequence: Increased Penalty and Civil Liability

PIPL imposes increased penalties for violating PIPL, including an administrative fine of up to RMB 50 million or 5% of the violator's turnover in the preceding year, confiscation of illegal gains, cessation of

operation for rectification, or revocation of operating permits or business licenses. Additionally, the person-in-charge or other directly liable individuals may also be held liable and subject to a fine up to RMB 1 million. Such individuals may further be restricted from serving as a director, supervisor, senior management or personal information protection officer for a certain period of time.

Infringement of personal information, causing damages to relevant individuals, will result in civil liabilities. What's important, PIPL shifts the burden of proof of "fault" on the defendant personal information handlers to facilitate the establishment of a personal information infringement claims. According to Article 69 of PIPL, in case of personal information infringement, if the party which handles personal information fails to prove its innocence, it will be presumed to be faulty.

2. Challenges and Solutions

In facing the strict personal information protection rules, how should a company be compliant? A lot of concerns have been raised since the publication of PIPL.

There is no grace period for enforcing PIPL. PIPL will start to be enforced tomorrow. This means that all companies which handle personal information would need to comply with PIPL from tomorrow (if they haven't done so). Would this be challenging?

Some people concern that onerous personal information protection requirements may cause difficulties to business operations. Some people concern that who and which position will be appointed to take charge of personal information protections and thus to report to the government. Some people concern that PIPL will impede exports of personal information. Some people concern the ''reversal of burden of proof" in civil cases will encourage individuals to bring actions against those which handle their personal information.

What are the immediate action companies should take in facing these challenges?

Our top suggestion is to establish an internal data governance to protect personal information. A suite of managerial rules on personal information protection is not only a legal requirement for all companies which handle personal information; but also facilitate to form a defense in case of any personal information incident occurs. Under PIPL, the burden of proof of no-fault is shifted to the party which handles personal information. In case of a personal information incident, a good way to prove the innocent is to demonstrate a well prepared and implemented managerial rules, plus well-trained staff. Moreover, a well-prepared internal policy on personal information protections show companies' respect to the laws and, if there is a minor or technical violation on personal information protection matter, the law enforcement body will likely impose light or even no penalty on those companies during the initial period of time after the effectiveness of PIPL.

Secondly, companies may consider re-streaming their business processes per PIPL requirements. PIPL imposes quite strict conditions on collection, process, transfer of personal information. In particular, the

handling of sensitive personal information, the sharing of personal information, collection of bio-recognition information requires separate consents. Additionally, PIPL sets out onerous requirement on data export, making transfer of personal information out of China more difficult. As such, business operators may need to consider re-design their business process, leaving room to seek informed consents from individuals, and relocating regional IT hubs to China, retaining more sensitive data within the territory of China.

Thirdly, companies would need to perform internal audits on a periodic basis to ensure their compliance with PIPL and other regulations on personal information. The auditing process will help companies be better compliant; and, more importantly, a report from the audits will help establish a prima facie evidence to prove the companies' no-fault during a personal information incident to avoid civil liabilities.

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

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