What does the new draft Personal Information Protection Law mean to International Financial Institutions?

By Xun Yang | Jianqi Yang

This briefing will focus the discussion on the following issues:

- extraterritorial jurisdiction
- Engaged processing
- Date export
- Compelled disclosure to foreign government agencies

China has recently issued the draft *Personal Information Protection Law* (the "***PI Law***"), which, if adopted, will be the first comprehensive high-level legislation on personal information protections in China. It details the rules for collection, storage, processing, and disposal of personal information, clarifies a number of controversial issues such as security assessment for data exportation, and sets out comprehensive requirements in relation to establishing internal policies for data management. Thus, the PI Law forms a solid base for further legislations on personal information protection matters.

The PI Law influences all business sectors. In particular, it would likely affect significantly the data practice of international financial institutions which already have business operations in China or are expanding their business operations into China.

Extraterritorial Jurisdiction

Different from the *Cyber Security Law* effective in 2017 which regulates constructions, operations, maintenance, and utilizations of networks in the territory of PRC, the PI Law has explicit exterritorial effect. International financial institutions which do not have presence in China would still be subject to the PI Law in terms of collections and utilization of personal information of people residing in China.

For more Llinks publications, please contact:

Publication@llinkslaw.com

According to Article 3 of the PI Law, the PI Law regulates the collection, storage, utilization, processing, transmission, provision or disclosure (collectively "***handling***") outside of China of personal information about people residing in the territory of China if either of the following conditions are met: (i) the purpose of the handling is to provide goods and services to people in the territory of China; (ii) the purpose of the handling is to analyze or evaluate behaviors of people within the territory of China; and (iii) any other situation provided for by laws and regulations. China has a huge financial service market, which attracts those international financial institutions to invest in. Meanwhile, the financial service sector has not been fully opened to foreign investment. As a result, many foreign financial institutions select to stay offshore whilst studying the China market or servicing Chinese customers by sending staff to travel to China or otherwise remotely. During the course of such remote business operations, foreign financial institutions inevitably collect and analyze personal information generated in China, which include customer identities, financial information, family structures, contact information, etc. If the PI Law is finally adopted, the handling of personal information by these foreign financial institutions will be subject to the PI Law. Consequently, foreign financial institutions will be required to follow the data protection requirements under the PI Law. A violation to the data protection requirements under the PI Law may result in the foreign financial institution being included in a blacklist and in a ban on cross-border transfers of personal information to it.

It may be a big challenge, for those financial institutions which have already developed and implemented robust data protection policies in practice, to follow the PI Law when handling the personal information. However, the PI Law does increase the administrative cost by imposing a "local presence" requirement on those foreign financial institutions which collect or use personal information concerning people residing in China. The requirement is that, according to Article 52 of the PI Law, a foreign financial institution establish a dedicated department or appoint a representative in China to take charge of data protection matters. The data protection department and the data protection person must be filed with the government. The PI Law does not set out the criteria for such department or person. However, with respect to data protection persons working for foreign securities and fund business, the China Securities and Regulatory Commission (***CSRC***) may require that they maintain securities professional qualifications. This will increase administrative burdens on foreign financial institutions.

Engaged Processing

Generally speaking, the PI Law permits the outsourced processing of personal information. Consequently, financial institutions can outsource to third party service providers IT or business functions concerning personal information.

The PI Law distinguishes outsource of personal information processing from transfer of personal information due to business disposal or otherwise; and impose less burden on outsourcing arrangement. According to Article 22 of the PI Law, a personal information controller is allowed to engage a third party service provider to process personal information in its possession provided that (i) the personal information controller enters into an agreement with the service provider to define the purpose of and method for the processing, the nature and categories of personal information to be processed, as well as the required security measures to protect

personal information; (ii) the personal information controller supervises the personal information processing activities; (iii) the service provider only processes personal information within the scope of consents which relevant data subjects grant; and (iv) the service provider returns to the personal information controller or otherwise destroys personal information upon the completion of the processing. A personal information controller is not required to seek data subjects' separate consents to the outsourced processing; nor is it required to disclose the identity of the service provider. Consequently, a personal information controller can decide whether to enter into an outsourcing arrangement involving process of personal information after its collection of personal information.

At the early stage when international financial institutions enter into the Chinese market, they tend to outsource their administrative functions, IT functions, and certain ancillary business functions (e.g., with respect to mutual fund business, the TA and FA functions) to manage the costs and retain the flexibility. Such outsourcing arrangement will more or less involve process of personal information. The PI Law does not impose any requirement to seek individuals' separate consents or to disclose service providers' identities, and thus facilitates outsourcing arrangements.

Nevertheless, in order to control the data breach risks arising from outsourcing arrangements, it would be important to enter into service agreements with service providers pursuant to legal requirements under the PI Law and to include all necessary clauses, such as the scope and restriction of the outsourced services, auditing right, confidentiality, destruction of information, prohibition on further subcontracting, etc. A well drafted service agreement will help mitigate data breaching risks arising from outsourcing arrangement and be a good defence when authorities perform regular inspections on outsourcing activities involving personal information.

Data Exportation

The PI Law releases the concern that all data exports require security assessment organized by the government. As a result, foreign financial institutions would have a greater flexibility to integrate on their global platform the data generated from their business operations in China.

Restrictions on data exportation have long been a controversial topic in China. The Cyber Security Law sets out the principle that personal information and important data which critical information infrastructure (***CII***) operators collect or generate in China must be kept in China and that, if they are necessarily to be exported outside of China, a security assessment procedure according to relevant regulations would be required. In order words, the Cyber Security Law only restricts the export of personal information and important data which CII operators generate or collect in China. However, the Cyberspace Administration of China (***CAC***), the key regulator on cyber security matters in China, issued a draft *Administrative Measure for Export of Personal Information and Important Data* in 2017, which was later replaced by the draft *Administrative Measure for Data Security* and the draft *Administrative Measure for Security Review of Export of Personal Information*, of which both were released in 2019. All these draft measures expanded the scope of personal information exports where security assessment is required. Under these draft measures, all exports of personal information require security assessment regardless of whether they are collected or generated by CII operators or of the

materiality of the personal information. These measures also require government approvals for the security assessment before exports can be implemented. Such a wide scope of application of the security assessment requirement triggers concerns that the security assessments will incur a significant administrative cost and that the delay in government approvals for the security assessments will delay the exporting process.

The PI Law relieves the concerns by narrowing down the scope of applications of the security assessment requirement. According to Articles 38 and 40 of the PI Law, an export of personal information by a CII operator or an export of personal information reaching a volume threshold to be stipulated by CAC must undergo a security assessment procedure organized by CAC. With respect to all other circumstances relating to exports of personal information, the exporter may select to undergo, or not to undergo, the security assessment procedure on its own discretion. If a security assessment is not selected, the exporter will be responsible for entering into an agreement with the offshore personal information receiver to procure that the receiver meet the personal information protection standard imposed by the PI Law. On this regard, the data transfer agreement will be critically important to ensure the compliant because the exporter is responsible for the behaviors of the data receiver.

The PI Law helps clarify the requirements on data exports and relieve the concerns of multinational corporations, including in particular international financial institutions. International financial institutions usually desire to have extensive data integration, i.e., to process, analyze, and store information about customers and staff on global platform, which enables them to apply their operational strategies, investment models, and risk control tools consistently. The reduction in the scope of application of the security assessment requirement renders international financial institutions greater flexibilities to export and integrate data globally.

Note that the PI Law does not exclude the possibility that relevant industrial regulators may impose other conditions on data export. For example, CSRC restricts the export of client identity data and transactional data. These restrictions will still apply despite of the PI Law.

Compelled Disclosure to Foreign Government Agencies

The PI Law prohibits the disclosure to foreign government agencies of personal information collected in China. This prohibition may confront international financial institutions with the dilemma that, whilst they may be compelled to disclose personal information to foreign government agencies, they are prohibited from the disclosure by the China government.

According to Article 41 of the PI Law, unless otherwise provided for under international conventions or bilateral treaties to which China is a party, the disclosure of personal information to foreign government agencies for judicial assistance or administrative enforcement is required to be approved by the China government. This requirement is consistent with that under the *PRC Securities Law* effective in March 2020 where disclosure to foreign law enforcement agencies of files and materials relating to securities business is prohibited unless such disclosure is made via a cooperative mechanism established between China and foreign governments (e.g., the

MOU between CSRC and US SEC) or otherwise approved by CSRC or other government agencies in China. These requirements mean that the China government would have full control over the information to be disclosed to foreign government agencies.

However, the prohibition on disclosure contradicts to some foreign authorities' positions. For example, the US congress passed the CLOUD Act in 2018, pursuant to which the US government has the power to compel companies to disclose to it personal information or other data in the possession of not only those companies but also their subsidiaries overseas even if the local laws where these subsidiaries are located prohibit these subsidiaries from doing so. Consequently, when US government orders a US financial institution to disclose certain personal information in the possession of its subsidiary in China and the China government disapproves such disclosure, the financial institution will (i) violate the US law, if it selects not to disclose such personal information as US government orders; or (ii) violate the China law, if it selects to follow the order of the US government.

It may be too early to assess the practical impact of this prohibition on international financial institutions, or to suggest a resolution. However, a well-developed information firewall between a foreign financial institution and its subsidiaries in China as well as a well-designed managerial policy may help segregate data generated in China from those under direct or indirect control of the foreign financial institution and thus reduce the practicability to compel the disclosure of data in the possession of such Chinese subsidiary.

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
16F/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
27F, Henley Building
5 Queen's Road Central
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