Impact of 2nd Draft of PI Law and Data Law on Multinational Financial Institutions

By Xun Yang | Jianqi Yang

In April 2021, the *Standing Committee of the National People's Congress* announced the release of the *2nd draft of the Personal Information Protection Law* (the "**PI Law**") and *the 2nd draft of the Data Security Law* (the "**Data Law**") for public consultations. The release of the two drafts indicates a further step toward the establishment of a comprehensive data protection system in China and will have significant impact on multinational financial institutions.

1. Data Exportation

The 2nd draft of the PI Law and of the Data Law largely retain the data exportation system adopted by the 1st draft of these laws that normal data exportations will be subject to risk assessment to be performed by data exporters but exports of large amounts of personal data or of important data will be subject to risk assessment to be organized by the government panels. However, the 2nd draft of these laws propose the following changes to further strengthen data export controls.

In relation to the export of personal information, the PI Law requires that exporters enter into data export agreements with personal information recipients according to a template agreement which the *Cyberspace Administration of China* ("**CAC**") will compose. This requirement is even stricter than that set out in the draft *Risk Assessment Measure for Personal Information Export* which CAC released in 2019, which set out mandatory contents to be included in the data export agreements. The requirement to use government template may require a change in the customary data sharing practice. Currently, most multinational financial institutions have the need to integrate and process personal information (including

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

both employee data and customer data) on a global basis. Usually, entities in different jurisdictions within the same financial institution group enter into data sharing addendums which are drafted based on GDPR requirements and then adapted by local laws in various jurisdictions including China. However, the requirement to use government template suggests the necessity to change the current practice because data sharing addendum adapted from GDPR may not be compliant. As such, an additional data export agreement according to the government form may be necessary.

In relation to export of important data, the Data Law expands the scope of application of government-organized risk assessment. In addition to the export of important data by operators of critical information infrastructure (**"CII"**) under the *PRC Cyber Security Law*, the Data Law requires that export of important data by all network operators be subject to risk assessment performed by CAC or the relevant regulators. Some financial data, such as aggregated customer transactional data covering multiple provinces, are likely considered important data according to the *Financial Data Security --- Data Security Classification Guidance*. The export of these data by securities firms, fund managers, wealth management companies, or other financial institutions will need to undergo a risk assessment performed under the supervisions of CSRC or CBIRC, as the case maybe.

2. Extraterritorial Effect

The 1st draft PI Law has introduced the extraterritorial effect of personal information protection. The 2nd draft further strengthens such effect. Moreover, the Data Law also established extraterritorial protections of important data by taking reference to the PI Law.

The PI Law and the Data Law now have a wide extraterritorial jurisdiction. Any collection, processing, or disposal of data, either personal information or important data, will be subject to the PI Law and/or the Data Law as far as these data are about individuals in China or otherwise relevant to the public interest of China, regardless of whether a Chinese company or a foreign company collects, processes or disposes such data, or of whether such data are collected, processed, or disposed inside or outside of China. As such, when the headquarters or regional hubs of multinational financial institutions collect, process, or dispose data collected or generated in China, they need to comply with the PI Law and the Data Law, in addition to the laws in the jurisdictions where such headquarters and regional hubs are located.

Additionally, the PI Law proposes the measures to sanction companies which violate the PI Law. According to Article 42 of the PI Law, if a foreign company collects, processes, or disposes personal information about individuals in China in violation of the PI Law, it may be included in a blacklist to which the provision of personal information will be banned. In other words, if a headquarter or regional hub of a financial institution violates the PI law, its Chinese affiliates will be prohibited from continuing supplying personal information to it, thus causing operational interruptions.

Moreover, in observation of the "data sovereignty" principle, the disclosure of data to foreign government agencies will be subject to an approval requirement. Under both the PI Law and the Data Law, if a company

is ordered by a foreign government agency to disclose personal information about individuals in China or important data concerning Chinese public interest, such company must not disclose such personal information or important data unless the disclosure is approved by the relevant regulator of the PRC government. For example, if SEC compels the disclosure of certain business data of a Chinese company or personal information about the beneficiary owner of a Chinese company, the securities firm in China which possesses such data or information can follow the disclosure order only if the disclosure has been approved by CSRC. This may put multinational financial institutions in a dilemma where, on one side, they are compelled by a foreign government agency to disclose certain data and, on the other, they are prohibited from the disclosure by the PRC government.

3. Collection of Personal Information from Public Sources

The 2nd draft of the PI Law adds a scenario where collection and use of personal information does not require individual consents, that is the collection and use of personal information from public sources within a reasonable scope. This provision permits the collection and use of publicly available personal information without individuals' consents and, for the same time, requires that the collection and use be refrained within a reasonable scope.

Neither the PI Law nor other law or regulation further defines the "reasonable scope." It is generally understood that if the purpose of collection or use of personal information is reasonably foreseeable or expected, then such collection or use is likely be considered within the reasonable scope. Financial institutions may collect a wide range of information from public sources for research and market intelligence purposes, including personal information. This "public sources" exception to consent requirement gives financial institution more flexibility to utilize publicly available personal information.

4. Big Data

The PI Law and the Data Law encourage the development and application of big data technology.

From a policy aspect, the Data Law encourages the development of big data technology and business innovations by using big data. This indicates, big data will have an increasingly wide application in a great variety of business sectors, including the financial business sector. Sourcing and using big data from third party data providers may become customary in the financial business.

The PI Law confirms that use of anonymous data or big data generated from personal information with respect to which consents have been withdrawn. Further to the first draft of the PI Law which confirms the legality of the processing of personal information before consents to such processing are withdrawn, the 2nd draft of the PI Law further confirms that the effect of the personal information processing occurred before the consents are withdrawn. In other words, if a financial institution generates big data or anonymized data by processing customers' personal information based on customers' consents, it can further develop and use such big data or anonymized data even if such customer consents are withdrawn.

Therefore, it would be advisable for financial institutions to promptly anonymize personal information they collect before any individual could withdraw the consent to secure the flexibility to continue using the data.

5. Strengthening Cyber Security Protections

The PI Law and the Data Law propose rules on strengthening cyber security protections.

From the system aspect, the Data Law includes a requirement that data processing follow the multi-level protection schedule. Under the multi-level protection scheme which the public security department introduced in 2007, network operators are required to classify their systems according to the criticalness of the system and the sensitivities of the data stored thereon and then to apply different security measures to their systems corresponding to the relevant security levels. The inclusion in the Data Law the requirement to follow multi-level protection scheme means that the multi-level protection scheme will become a legal requirement applicable to all data processors. Therefore, financial institutions need to comply with not only the security measures imposed by the regulators but also the multi-level protection scheme enacted by the public security department.

From the data aspect, the Data Law provides that the government will establish a data classification protection system, under which important data will be specified and subject to “emphasized” (additional) protections. This provision suggests that the government will be responsible for determining the categories and scope of important data and the data possessors will be responsible to apply security measures to protect the important data according to the legal requirement. As such, financial institutions will be required to identify important data in their possessions according to categories and scope determined by the government and apply security measures accordingly.

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