China Personal Information Protection Law: Compliance Guidance for Foreign Banks and Companies (II)

July 19, 2022

In the previous article, based on our experiences in relevant mattes, we discussed how multinational companies and financial institutions should balance costs and compliance in five aspects under the China Personal Information Protection Law (PIPL). This article will continue to discuss this topic about the costs and compliance balance under PIPL from other perspectives.

This article will introduce how multinational companies are advised to refine their compliance system under the PIPL from the following four aspects:

1. **Building channels to protect the rights of data subjects;**
2. **Supervision and control on third-party data processors;**
3. **Personal information collected by the critical information infrastructure operators (the "CIIO") shall be saved within the territory of the PRC;**
4. **Assessing the compliance of cross-border data flow.**

1. Building channels to protect the rights of data subjects

Chapter 4 of the PIPL provides the data subjects with rights to know, to decide, to consult and duplicate, to transfer, to supplement and correct, to delete, to explain and other rights in relation to their personal information. When conducting data compliance reviews, multinational companies are advised to build up a convenient and complete mechanism to protect the rights of data subjects. The following aspects need to be aware of:

(1) Focusing on the protection of data subjects' rights to know based on the principle of "notification-consent"

The right to know is an important right of data subjects, but the PIPL has not provided detailed protection measures for it. We suggest that multinational companies could refer to the provisions of GDPR when carrying out compliance work, and provide corresponding protection of the right to know to data subjects. For example, companies shall reply to data subjects' requests for the right to know within a reasonable period of time and provide information in the way requested by data subjects. The company shall provide information in a concise and easy-to-understand

Key contact

Leo (Liang) Zhou
Senior Partner
Guangzhou
D +86 20 3810 2725
liang.zhou@dentons.cn

manner while free of charge, and may verify the identification of the data subject before providing the information if necessary.

(2) Building a classified and graded data protection system

According to Article 5 of Regulations for the Administration of Network Data Security (Exposure Draft), China establishes a classified and graded data protection system. Multinational companies could refer to the state classification standards to classify and grade their internal network data. The data can be divided into general data, important data and core data. Different protection measures can be adopted for different classification of data so as to improve the efficiency and pertinence of data protection.

Generally, data should be classified by referring to the state classification standards and the industry classification standards. If the industry does not have such standards, data could also be classified from the perspective of business management.

(3) Providing convenient ways for data subjects to refuse

According to Article 44 of PIPL, an individual has the right to restrict or refuse others to process his/her personal information; according to Article 47 of PIPL, an individual has the right to withdraw the consent he/she has given and has the right to request the processor to delete the personal information which has been collected or processed. When processing personal information, multinational companies shall protect the right of data subjects to refuse and provide convenient and feasible methods for data subjects to quit.

In a project of explicit consent for the processing of personal images and personal identification data that we reviewed and revised, the company provides two options of "Yes" and "No" for employees to choose. Besides, in the website privacy policy project of another multinational company that we participated, the multinational company provides two options of “Unsubscribe” and “Opt-out” for its employees, and employees can choose to refuse to receive some or all of the notifications sent by the website at any time by setting their own preferences on the website or by directly exiting.

2. Supervision and control on third-party data processors

In a project we advised where a bank in the North America collected personal information of Chinese clients for account-opening, we combined practical experience with regulations in PIPL, and gave the suggestion that either in a way that (1) the bank entrusts a third party to process the collected data, or (2) the third party collects and processes the data before providing the data to the bank, the collecting party shall inform the clients of the recipient’s related information and supervise the personal information processing activities by the third party.

(1) Prudently selecting third party processor and making sure its data processing capability meets standards specified in PIPL

When selecting a third-party data processor, the multinational companies are advised to make prudent selection and conduct due diligence on the third-party data processor so as to make sure that its data processing capability can meet the requirements of PIPL and ensure the security of data processing. According to Article 38 of PIPL, if multinational companies selects a foreign third party processor, they shall pass security assessment or personal information protection certification, and enter into a contract with the overseas third party in accordance with the model contract developed by the national cyberspace administration.

(2) Obligation to inform data subjects

In practice, if a company entrusts a third party to process personal information, it shall obtain prior consent of data subjects before supervising and controlling the third party. Article 24 of PIPL does not compulsorily require the client to inform the data subject of the name, contact information, purpose, method of processing and the type of personal information to be processed by the third party, nor to obtain the individuals' exclusive consent. However, as a way of processing personal information, the third party entrusted by the company constitute changes to the processor, which triggers the requirement under Article 17 (2) of the PIPL. We suggest that the company shall inform the data subject of the changes to the information in relation to personal information processing, such as the name of the third party, processing purpose, method, type and storage period.

(3) Conducting personal information protection impact assessment before providing data

In accordance with Article 55 of PIPL, if a company entrusts a third party to process personal information or provides a third party with personal information, it shall conduct a personal information protection impact assessment in advance, record processing results and save such records for three years. In practice, the legal department, compliance department or information security department of the company may take the lead in the assessment work. They could decide to conduct the assessment work by themselves or hire an external independent third party to undertake the assessment work based on the actual situation of the company.

(4) Signing a data processing contract with unambiguous rights and obligations

When entrusting a third party with the processing of personal information, the company shall sign a data processing contract with the third party. In order to better control and supervise the information processing by the third party, the entrusting party shall, in the contract, expressly define the rights and obligations of both parties, limit the methods and contents of the third party's processing of the information, particularly define the liabilities of each party, and establish a supervision method for the entrusting party.

3. Personal information collected by the CIIO shall be saved within the territory of the PRC

Article 40 of the PIPL provides that the critical information infrastructure operators ("CIIO") shall save the personal information they collect within the territory of the PRC. As the main participants of cross-border data activities, multinational companies, if they are one of the CIIOs, need to actively comply with the various requirements on data storage under the PIPL when carrying out cross-border data compliance.

(1) Localized storage principle

According to Security Protection Regulations for Critical Information Infrastructure, CIIO refers to the important network facilities and information systems in important industries and fields such as public telecommunications, information services, energy, transportation, water conservancy, finance, public services, e-government and national defense science, technology and industry, as well as other important network facilities and information systems which, in case of destruction, loss of function or leak of data, may result in serious damage to national security, the national economy and the people's livelihood and public interests. Whether a multinational company is a CIIO is subject to the determination of the competent authorities and supervisory authorities of the aforesaid important industries and sectors.

(2) Main methods of localized storage

All domestic or foreign companies shall use servers located in China to collect and save personal information and data related to critical area. For example, Apple Inc. has migrated its iCloud data to Guizhou Cloud Big Data and all data collected on servers located in China, and Tesla has set up a data center in China to save all data generated from the vehicles sold in mainland China. As representatives of the critical information infrastructure operators, automobile data security and communication data security take the lead to be localized in practice, and may lead to the data compliance in relation to local storage in other industries.

4. Assessing the compliance of cross-border data flow

Digital economy is playing an increasingly important role in modern society. If a company only focuses on data localization, it will limit the effective and orderly flow of data and the globalization development of the multinational companies. Multinational companies is advised to always be aware of the compliance requirements in the cross-border data flow, so as to make sure the data flow complies with national regulations and declines business risks caused by violations.

(1) Assess the legality of cross-border data related activities under PRC law

We used to participate in a project regarding the collection of personal information of Chinese clients by a Hong Kong bank. The bank inquired

how such collection would be censored under PRC law. We analyzed the legality of the collection of domestic client information, collection of domestic client information through official websites and apps, obtaining domestic client's credit information, and cross-border data transfer under PRC law, and provided a legal basis for the bank's references and advised the bank on what can and cannot be done. The legality of cross-border data- related activities shall not be assessed solely based on specific laws. Such activities shall be placed within the broad framework of PRC information security laws and regulations, and the legal risks of each activity shall be analyzed individually, so as to ensure the legality of the data activities of multinational companies in China.

(2) Cross-border data flows need to be assessed for the risk of overlapping jurisdictions

Multinational companies not only need to pay attention to the relevant laws and regulations within China, but also need to be aware of any legislative developments regarding data storage and cross-border data transmission in the destination country. For example, the data exported to the EU shall comply with the relevant rules of the GDPR. The data exported to the United States shall pay attention to the Cloud Act and other relative regulations of the USA, so as to facilitate effective data transmission.

We will continue to share more insights in our final article on how multinational companies balance cost and compliance under the PIPL.
