中倫律師事務所
ZHONG LUN LAW FIRM

# New Era Is Coming: How China's *Personal Information Protection Law* Will Impact International NGO's Data Management

***Hengka (Henry) JI***

***Jiannan ZHU***

The rapid technology evolvement, coupled with a growing awareness of data sovereignty and national security concern, has urged many countries to pass laws and regulations regarding data management and protection. Personal information, also known as personal data or personally identifiable information, is a significant part of this data protection legislation regime.

China is also at the forefront of this drive. The Standing Committee of the National People's Congress of the People's Republic of China ("the **PRC**") has recently passed the *Personal Information Protection Law* ("**PIPL**"), which will take effect on ***November 1, 2021***. The main legislative purposes of the PIPL are to further regulate data activities, promote the reasonable use and protect rights regarding personal information.

Alongside the *PRC Cybersecurity Law* ("**CSL**") and the *PRC Data Security Law* ("**DSL**"), the PIPL constitutes another important pillar, advancing China's ambitious goal of establishing a holistic regulatory framework for the governance of cybersecurity and data protection. Once taking effect, the PIPL will cast significant impacts on the data compliance practices of international non-governmental organizations ("**INGO"**) as well as multinational enterprises to the extent they collect, transfer, process or use the personal information of individuals within China.

In this article, we aim to briefly introduce and illustrate the burning issues and significant aspects in the PIPL which will most likely impact to a great extent INGOs' international cooperation and operations in China (in particular, the INGOs in health, education and trade/industry research sectors which heavily involve processing sensitive personal information) following the release of the *Law on Administration of Activities of Overseas Nongovernmental Organizations in the Mainland of China* ("**INGO Law**") effective from 2017. Understanding PIPL will be crucial for INGOs to take appropriate actions and ensure compliance within the proper legal context in the new era of data management.

## I. DEFINITIONS OF PERSONAL INFORMATION, SENSITIVE PERSONAL INFORMATION, PROCESSING AND PROCESSOR

Under the PIPL, **Personal Information** is defined to encompass all kinds of information related to identified or identifiable natural persons recorded by electronic or other means. As an exception to the PIPL, information processed anonymously will be excluded.

The PIPL introduces the concept of **Sensitive Personal Information** for the first time, referring to the personal information that is likely to result in damage to the personal dignity of any natural person *or* damage to his/her personal or property safety if it is disclosed or illegally used.

**Processing of Personal Information** shall include, but not limited to, the collection,

storage, use, processing, transmission, provision, disclosure, and deletion of personal information.

The concept of **Personal Information Processor** is also clarified in the PIPL and is referred to as any organization or individual that independently determines the purpose and method of the processing of personal information.

## II. COVERED SCOPE UNDER THE PIPL

Theoretically, the PIPL would be applicable to any processing of personal information of natural persons within the territory of the PRC. Any organization or individual conducting personal information processing activities within the territory of the PRC will be covered by the PIPL.

Besides activities to be conducted within the PRC, the PIPL exerts certain exterritorial jurisdiction over personal information processing activities that take place outside the PRC if the purpose is to analyze or assess the activities of individuals in the PRC. ***INGOs subject to this exterritorial jurisdiction of the PIPL are required to establish a dedicated entity or appoint a representative in China to handle matters in relation to the protection of personal information they collect, and to file the information of the entity or the representative with competent government authorities.*** INGOs or individuals are likely to be put on a "blacklist" that would restrict or prohibit them from receiving personal information from the PRC if they infringe the personal information rights and interests of Chinese citizens or harm the national security or public interest of China.

## III. IMPLICATIONS FOR CROSS-BORDER DATA TRANSFER

Under the PIPL, cross-border transmission of personal information shall fulfill the pre-condition that the personal information processor must prove and demonstrate a solid reason (business or other reasonable needs) for such transmission outside the territory of the PRC. Otherwise, the personal information will not be allowed to be transferred overseas.

In comparison to the previous rules, the PIPL enhances the informed consent requirements for cross-border data transfer. In other words, the PIPL requires that when a personal information processor provides personal information outside the PRC, it shall inform the data owners of the name of the overseas recipient, the recipient's contact information, purpose for the processing, processing method, and types of personal information to be processed, as well as the means and procedures for the data owners to exercise the rights provided under the PIPL. In that case, separate consent from data owner shall be obtained.

Furthermore, the PIPL requires that a personal information processor must ensure that all personal information transferred out of the PRC shall be provided a level of protection at least on par with the standards under the PIPL. Since data/information protection legislation varies in different jurisdictions, and some do not have relevant legislation at all, the requirements in PIPL may increase some INGOs' compliance obligations.

## IV. WATCH-OUT FOR SENSITIVE PERSONAL INFORMATION

Sensitive personal information may include information such as biometric identification, religious belief, identity, medical health, financial accounts and

whereabouts and tracks, as well as the personal information of minors under the age of 14.

Due to its sensitive nature, the processing of sensitive personal information shall meet specific transparency requirements regarding the necessity of the processing concerned as well as the impact of such processing on one's personal rights and interests. The processor shall obtain separate consent and conduct personal information protection impact assessments. In practice, we would recommend INGOs which involve personal information classification to take more stringent measures concerning sensitive personal information protection and incorporate verifiable separate consent settings.

## V. PROCESSOR'S LEGAL OBLIGATIONS

The PIPL puts forward a regulatory framework that imposes substantial obligations and responsibilities on all personal information processors, including:

(1) Formulating internal management systems and operating procedures.

(2) Implementing classified management of personal information.

(3) Taking proper technical security measures such as encryption and de-identification.

(4) Reasonably determining the authorizations for personal information and providing regular security education and training for relevant staff.

(5) Formulating and implementing emergency response plans for personal information security incidents.

(6) Conducting regular compliance audits.

(7) Adopting other measures stipulated by laws and regulations.

## VI. LEGAL LIABILITY FOR NON-COMPLIANCE

Violations under the PIPL would lead to severe legal consequences. ***Administrative sanctions include penalties of up to RMB 50 million, cessation of operation for rectification, or revocation of operating permits or registration certificates***. The person in charge may be held liable for 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 stipulated period of time.

The PIPL also imposes tortious liability on processors infringing upon the rights and interests of individuals' personal information. Furthermore, the PIPL imposes the burden of proof on the defendant (personal information processor) in a civil action to facilitate damage claims. Moreover, it should be noted that criminal liability may be attached under the PIPL in some cases.

## VII.PRACTICAL RECOMMENDATIONS

Based on our firsthand experiences, the following measures are recommended for consideration by the relevant INGOs with operations or projects in China:

(1) Manage personal information by its nature and hierarchy.

(2) Provide necessary legal training to relevant managers, advisers, employees or consultant regarding the detailed implementation rules to be promulgated by the competent Chinese authority in near future.

(3) Optimize the collection process of personal information of employees.

(4) Conduct self-assessment in terms of collected personal information.

(5) Establish more robust compliance system for the protection of personal information from global and local perspectives.

(6) Make amendments to organization's personal information policy.

(7) Formulate proper security incident response plan and carry out drills thereof (if necessary).

**IN CONCLUSION**, the PIPL is the first comprehensive national law governing how organizations and individuals shall process the personal information of individuals in the territory of the PRC. Due to its broad scope, the PIPL will significantly impact almost every INGO operating in China, and INGOs are recommended to conduct a rigorous assessment on its data privacy policy and internal procedures to fully comply with the PIPL. Furthermore, from the European Union's General Data Protection Regulation to China's PIPL, the world is progressively stepping into the new era of data protection. It is critical for INGOs with operations in multiple jurisdictions to establish an aligned and effective compliance system and closely monitor legislative updates in the fields of data protection and cybersecurity law in China or other jurisdictions where they have presence.