The Asset Management Industry
SERVING INDIVIDUAL INVESTORS
INVESTMENT COMPANY INSTITUTE

MEMO# 33738

August 27, 2021

China Promulgates Its First Personal Data Protection Law

[33738]

August 27, 2021

TO: ICI Global Members
Global Regulated Funds Committee
Global Regulated Funds Committee - Asia SUBJECTS: International/Global
Operations RE: China Promulgates Its First Personal Data Protection Law
On 20 August 2021, the Standing Committee of the National People's Congress (NPC), China's top legislative authority, adopted the Personal Information Protection Law of the People's Republic of China[1] (PIPL), the first law specifically regulating the protection of personal data in China. The PIPL will take effect on 1 November 2021.

The PIPL lays out a comprehensive set of rules governing how personal information is collected, used, processed, shared and transferred in China. It is modeled, in part, on omnibus data protection regimes adopted in other jurisdictions, notably the EU General Data Protection Regulation (GDPR). The PIPL, together with the Cybersecurity Law of the People's Republic of China[2] (Cybersecurity Law) and the Data Security Law of the People's Republic of China[3] (DSL), provides the fundamental framework of laws governing data protection, cybersecurity, and data security in China. The PIPL and the DSL, which comes into effect on 1 September 2021, will have substantive implications for foreign asset managers in their handling of personal data of individuals in China.

This memo provides a brief overview of the key provisions of the PIPL.

1. Scope of Application and Extraterritorial Effect

a. Scope of Data

"Personal information" refers to any information related to an identified or identifiable individual recorded whether electronically or through other means, but does not include anonymized information. The processing of personal information includes, but is not limited to, the collection, storage, use, processing, transmission, provision, disclosure, and deletion of personal information (PIPL, Chapter 1, Article 4).

Within the universe of "personal information" is a special category called "sensitive personal information" which is defined as personal information that, if leaked or illegally used, could lead to injury of a person's character and dignity, or harm to the personal or

property safety of an individual. Sensitive personal information includes information relating to race, ethnicity, religious beliefs, individual biometric features, medical health, financial accounts, individual location tracking, and personal information of a minor under the age of 14 (PIPL, Chapter 2, Article 28). The PIPL stipulates enhanced measures for protection of sensitive personal information (see sections 2 and 3 below).

b. Territorial Scope

The PIPL applies to entities and individuals processing personal information (information processors) within the territory of China. It further extends the territorial scope to overseas information processors who handle personal information of individuals in China for the purpose of offering products or services to or analyzing and assessing the behavior of such individuals (PIPL, Chapter 1, Article 3). An overseas information processor is required to establish a dedicated entity or appoint a representative in China whose functions are to handle matters related to the protection of personal information collected and file with the relevant authorities such entity's or representative's details, including the name and contact information (PIPL, Chapter 5, Article 53).

2. Personal Information Processing Framework

Information processors are required to have a legal basis to support the processing of personal information. Consent from data subjects remains the primary legal basis for lawful processing, with certain exceptions provided in the PIPL. Processing of personal information without consent is allowed if the processing is necessary for conclusion or performance of a contract to which the data subject is a party, or for human resources purposes (PIPL, Chapter 2, Article 13). Moreover, information processors must obtain separate consent from data subjects in case of: (i) processing of sensitive personal information, (ii) sharing or disclosure of personal information, or (iii) transferring of personal information outside China (PIPL, Chapter 2, Articles 23, 25, 29; and Chapter 3, Article 39).

Prior to processing personal information, information processors must clearly inform data subjects of the purpose and methods of the data processing, categories of processed personal information, retention period, and procedures for data subjects to exercise their individual rights under the PIPL (PIPL, Chapter 2, Article 17). The retention period of personal information should be the minimum period necessary to fulfill the purpose of data processing (PIPL, Chapter 2, Article 19). With respect to the processing of sensitive personal information, information processors should additionally inform data subjects of the necessity of processing such sensitive personal information and the impact thereof on the data subjects' rights and interests (PIPL, Chapter 2, Article 30).

The PIPL also explicitly requires information processors to establish mechanisms for receiving and responding to data requests from data subjects. (PIPL, Chapter 4, Article 50).

3. Governance and Control Requirements

The PIPL outlines the compliance control and personal information security protection that an information processor must implement. Information processors should regularly conduct audits to assess that the processing of personal information is in compliance with relevant laws and regulations (PIPL, Chapter 5, Article 54). Information processors must first perform a risk assessment before: (i) sensitive personal information is processed, (ii) personal information is used in automated decision-making, or (iii) personal information is transferred outside China (PIPL, Chapter 5, Article 55). Records of these processing

activities and the risk assessments should be kept for at least three years (PIPL, Chapter 5, Article 56).

4. Cross-border Data Transfer of Personal Information

Under certain circumstances, personal data processed in China is not allowed to leave the country without having passed a security assessment by the Cyberspace Administration of China (CAC). First, the operators of critical information infrastructures (CIIs)[4] must store personal information inside China. Secondly, an information processor that handles personal information, the volume of which reaches the "threshold" prescribed by the CAC (the threshold is not defined in the PIPL), is not allowed to transfer any personal information it handles outside China (PIPL, Chapter 3, Article 40).

All other information processors that do not fall under either of the above categories may transfer personal information outside China if any of the following conditions are satisfied (PIPL, Chapter 3, Article 38):

- the information processor has passed a security assessment by the CAC;
- the information processor has obtained a certification of personal information protection from a professional institution in accordance with the rules of the CAC;
- a contract has been signed with the overseas recipient in accordance with a standard contract formulated by the CAC (the full text of the standard contract has not yet been published).

As mentioned in section 2, the PIPL requires information processors to obtain the consent of data subjects where their personal information is to be transferred outside China (PIPL, Chapter 3, Article 39). Further, according to provisions under the DSL, the PIPL prohibits information processors from providing personal information stored in China to foreign law enforcement agencies or other foreign judicial authorities without prior approval from the Chinese government (PIPL, Chapter 3, Article 41).

5. Penalties

Where there is a non-compliance with the PIPL, including any unlawful processing of personal information or failure to perform any PIPL obligations, the competent authorities may order a correction, confiscate unlawful income, and issue a warning. In case of a serious violation, an information processor may be subject to a fine of up to RMB 50 million or 5% of its annual revenue for the prior fiscal year (PIPL, Chapter 7, Article 66).

6. Next Steps

The promulgation of the DSL and the PIPL marks the beginning of a new era of data privacy and cybersecurity protection in China. Foreign asset managers may wish to start the groundwork in preparation for the new regime. This could include reviewing governance structures and systems covering all aspects of data handling, understanding the types and uses of data collected and the processing cycle, and identifying potential areas for further evaluation or enhancement.

ICI Global will continue to monitor and keep members appraised of the relevant developments.

Alexa Lam
Chief Executive Officer, Asia Pacific

ICI Global

Irene Leung
Regional Lead, Member Relations and Research, Asia Pacific
ICI Global

Lisa Cheng
Research Analyst
ICI Global

endnotes

[1] See Personal Information Protection Law of the People's Republic of China, available (in Chinese only) at: http://www.npc.gov.cn/npc/c30834/202108/a8c4e3672c74491a80b53a172bb753fe.shtml.

[2] The Cybersecurity Law, effective since 1 June 2017, is the first law addressing cybersecurity issues in China. See Cybersecurity Law of the People's Republic of China, available (in Chinese only) at: http://www.cac.gov.cn/2016-11/07/c_1119867116.htm.

[3] The Data Security Law, to be effective on 1 September 2021, regulates all types of data processing and data security administration activities carried out within the territory of China. See Data Security Law of the People's Republic of China, available (in Chinese only) at: http://www.npc.gov.cn/npc/c30834/202106/7c9af12f51334a73b56d7938f99a788a.shtml. See also ICI Memorandum 33734, available at: https://www.ici.org/memo33734.

[4] CIIs are defined as information infrastructure in the industries of public communication and information service, energy, transportation, water resources, finance, public service, e-government, national defense and military affairs and other important network facilities and information systems, the disruption, disfunction and data leakage of which may endanger national security, civil livelihood and public interest. Under the Cybersecurity Law, personal information and other important data collected by CII operators must be stored locally in China. A CII operator should pass a security assessment by the CAC before any cross-border data transfer. As stipulated in the recently published Regulations for the Security Protection of Critical Information Infrastructure, industry regulators will formulate CII identification standards for the relevant industry and identify CIIs based on such standards. See Regulations for the Security Protection of Critical Information Infrastructure, available (in Chinese only) at: http://www.gov.cn/zhengce/content/2021-08/17/content_5631671.htm.