Published on *The National Law Review* https://natlawreview.com

China Issues Draft of Personal Information Protection Law

Article By:

Hunton Andrews Kurth's Privacy and Cybersecurity

On October 21, 2020, China issued a draft of Personal Information Protection Law ("Draft PIPL") for public comments. The Draft PIPL marks the introduction of a comprehensive system for the protection of personal information in China.

China's Cybersecurity Law, Data Security Law (draft) and Draft PIPL constitute three fundamental laws on cybersecurity and data protection. The Draft PIPL contains provisions relating to issues presented by new technology and applications and leaves some issues open for future legislation or non-binding guidelines.

The Draft PIPL consists of eight chapters and 70 articles, covering topics such as: (1) personal information processing, (2) the cross-border transfer of personal information, (3) the rights of data subjects in relation to data processing, (4) obligations of data processors, (5) the authority in charge of personal information and (6) legal liabilities.

Personal information refers to the various types of information recorded in electrical or other formats related to identified and identifiable individuals. The definition includes information that can identify data subjects as well as information that is related to the data subjects.

Summarized below are some key provisions of the Draft PIPL.

Departments Exercising Personal Information Protection

The Departments responsible for personal information protection ("Departments") include the Cyberspace Administration of China ("CAC"), the relevant department of the State Council and the relevant department of local government at the level of county or above.

Scope of Application

The Draft PIPL could be applicable outside of China to the extent necessary for the purpose of protecting the interests of data subjects in China. In cases where the purpose of data processing outside of China is to provide products or services to individuals in China or to analyze and make assessments about the behavior of individuals in China, these data processing activities would be governed by the Draft PIPL.

In addition, data processors located outside of China but governed by the Draft PIPL shall establish entities or appoint representatives in charge of personal information protection. The name of the entity or name and contact information of the representative shall be filed with the relevant Department.

The Draft PIPL would not apply to an individual processing his or her own data or family's data.

Seven Principles for Data Processing

The Draft PIPL stipulates seven data protection principles, including legality, explicit purpose, minimum necessity, transparency, accuracy, accountability and data security. This is the first time accuracy is contemplated with respect to personal information processing.

Consent and Exceptions for Consent

Under the Draft PIPL, the processing of personal information is not limited only to where consent is obtained, as provided by Cybersecurity Law. Under the PIPL, a data processor may process personal data based on: (1) consent of the data subject; (2) the necessity of executing or performing a contract; (3) the necessity of performing a legal obligation or legal duty; (4) a response to an emergent public health event or the necessity of protecting the safety of an individual's life and property; or (5) the publication of news and the supervision by public opinion for the public interest within reasonable scope.

A data processor shall not refuse to provide products or services on the grounds that an individual does not give consent to the processing of his or her personal information or withdraws his or her consent, except where the processing of personal information is essential for providing the products or services.

Joint Data Processing and Data Processing by Entrustment

If data processors process personal information together, the co-processors shall bear joint liability in cases of infringement of personal interests.

Where a data processor entrusts a third party to process personal information, both parties shall execute an agreement that includes the purpose of data processing, the processing mode, the types of personal information processed, protection measures and both parties' rights and liabilities. In these cases, the data processor must supervise the data processing activities. The Draft PIPL does not list specific supervision methods. After completion of performance of the contract or termination of entrustment, personal information shall be returned or deleted.

Provision of Personal Information to a Third Party

Where providing personal information to a third party, a data processor shall inform the data subject of the identity and contact information of the third party, the purpose of data processing, the processing mode and the type of personal information covered, as well as obtain separate consent from the data subject.

Automated Decision-Making

With respect to automated decision-making, data processors shall ensure the transparency of the decision and fairness of the result. In the event that data subjects consider the automated decision-making to have a significant impact on their interests, the data subjects are entitled to request that the data processor provide an explanation, and the data subject may refuse to permit the processor to make a decision solely by automated means. If the data processor adopts automated decision-making to conduct marketing and push messages, the data subject also may choose to have the processor not conduct marketing and push messages that target the personal characteristics of an individual.

Sensitive Personal Information

The Draft PIPL stipulates more restrictions on the processing of sensitive personal information. Sensitive personal information is defined as information that once leaked or abused may cause damage to personal reputation or seriously endanger personal and property safety, and includes race, nationality, religion, biometric information, health, financial account, personal whereabouts and other information. Only if the personal data processor has a specific purpose and sufficient necessity and obtains separate consent or written consent from the data subjects is processing sensitive personal information allowed.

The data processor shall also inform the data subject of the necessity of processing sensitive personal sensitive information and the impact on the data subject.

Personal Image Collected by the Equipment Installed in Public

A personal image and personally identifiable information collected by an image acquisition and personal identification device installed in public may only be used for the purpose of maintaining public security and may not be disclosed or provided to others unless consent is obtained from the individual or otherwise provided by relevant laws and regulations.

Disclosed Information

With respect to disclosed personal information, data processing must conform to the purposes for which the personal information is disclosed. In cases of data processing that exceeds the reasonable scope of that purpose, data processors must inform the data subjects and obtain consent before processing.

Where the purpose is not clear when personal information is disclosed, data processors must process the personal information in a reasonable and prudent way. In the event processing the disclosed personal information may have a substantial impact on data subjects, data processors shall inform data subjects and obtain consent.

Cross-Border Transfer of Personal Information

The Draft PIPL provides three methods for cross-border transfers of personal information. In general, cross-border transfers of personal information shall be certified by recognized institutions, or the data processor shall execute a cross-border transfer agreement with the recipient located outside of China and ensure that the processing meets the protection standard provided under the Draft PIPL. Where the data processor is categorized as a critical information infrastructure (“CII”) operator or the volume of data processed by the data processor exceeds the level stipulated by the CAC, the cross-

border transfer of personal information must pass a security assessment conducted by the CAC.

In cases of cross-border transfer of personal information, the data processor shall inform the data subjects of the identity and contact information of the overseas receiving party, the purpose of data processing, the processing mode, the type of personal information to be processed and the way data subjects can exercise their rights provided under the Draft PIPL, as well as obtain separate consent from the data subjects.

In terms of cross-border transfer of personal information for the purpose of providing international judicial assistance and law enforcement assistance, the transfer shall be approved by a competent authority.

Under the Draft PIPL, if an entity or individual infringes the personal information interests of Chinese citizens or if any nation or region adopts unreasonable measures towards China with respect to personal information protection, the CAC may take certain countermeasures against the nation or region.

Localization

In addition to the approval requirement for cross-border transfer of personal information applied to CII operators and the data processors that process data exceeding a specified volume, these data processors must store personal information in China.

Rights of the Data Subjects with Respect to Data Processing

Data subjects have the right to know, right to decide on, and right to limit or object to the processing of their personal information by others. Data subjects also have the right to access and copy their personal information from data processors and the right to request that data processors correct or complete their personal information. Under certain circumstances, data subjects have the right to request deletion of their personal information, the right to withdraw consent and the right to request that the data processor explains the processing rules.

The data processor shall establish the mechanism for the data subject to exercise his or her rights.

Obligations of Data Processor

The Draft PIPL provides the obligations of data processors with respect to data processing in an independent chapter. The obligations include establishing internal administrative policies and operating procedures, implementing the classified and hierarchical administration of personal information, making reasonable determinations regarding permission for data processing, conducting regular trainings and education, establishing and implementing contingency plans, adopting technical security measures and conducting regular audits of personal information processing activities.

Data Protection Officer

Where the volume of personal information processed reaches the level identified by the CAC, the data processor shall appoint a data protection officer (“DPO”) responsible for personal information processing. The name and contact information of the DPO shall be made public and filed with the relevant Department.

Advanced Risk Assessment

The data processor shall make a risk assessment in advance of processing sensitive personal information, the cross-border transfer of personal information, performance of automated decision-making on personal information, personal information being processed by a third party, providing personal information to a third party and disclosing personal information. The assessment report and disposal conditions shall be kept for three years.

Data Breach

In the event of a data breach, the data processor shall take remedial measures immediately and notify the relevant Department and data subjects. The Draft PIPL provides specific content to be included in the notification. Nonetheless, the Draft PIPL provides one exception to notification of data subjects. If the measures taken by the data processor could effectively avoid damages caused by the disclosure of personal information, it is not necessary for the data processor to notify the data subjects unless the relevant Department determines the disclosure may result in damage.

Legal Liabilities

The Draft PIPL enlarges the range of penalties beyond those provided in the Cybersecurity Law. In addition to rectification, confiscation of illegal gains, warnings, penalties under 1 million RMB, business suspensions, business halts for rectification, and the revocation of relevant permits or business licenses under Cybersecurity Law, the Draft PIPL also stipulates that in serious cases, data processors also are subject to fines under 50 million RMB or under 5% of the prior year's revenue.

National Law Review, Volume X, Number 301