KPMG

上海睿威律师事务所

Overview of Draft Personal Information Protection Law in China

KPMG Cybersecurity

—

November 10, 2020

Introduction

On October 21, 2020, the website of the National People's Congress (www.npc.gov.cn) published the full text of the Personal Information Protection Law of the People 's Republic of China (Draft) (hereinafter referred to as "draft PIPL") and solicited public opinions.

As the first special law on personal information protection in China, the draft Personal Information Protection Law will have significant impact on the activities of organizations and individuals dealing with personal information. The draft PIPL focuses on "personal information processing activities", clarifies the scope of application, the definition of personal information and sensitive personal information, the legal basis of personal information processing and the basic requirements of notice and consent. It also clarifies the obligations of the personal information processor and proposes requirements for the handling of personal information by state agencies.

From the perspective of compliance of general business organizations, this article would like to summarize the key points of personal information protection proposed in the draft Personal Information Protection Law and explore the effective path for enterprises to implement personal information protection activities so as to turn challenges into opportunities in the digital era.

Table of contents

Overview

> The formulation of a personal information protection law is an objective requirement to further strengthen the legal protection of personal information protection, a practical need to maintain a good cyber ecology, and an important measure to promote the healthy development of the digital economy.
>
> - Law Committee, National People's Congress

Scope of application

- Personal information processing activities conducted within China
- Certain processing activities conducted outside of China, of domestic natural persons' personal information

Personal information processor

- Organizations and individuals who independently decide the purpose and method of processing personal information.
- "Special" processors: joint processing, entrust and entrusted processing, third parties, etc.

Legal basis of personal information processing

- Obtain personal consent; or
- Signing or performing contracts, performing legal duties or obligations, responding to emergencies, implementing news reports and public opinion supervision for public interests, and other circumstances stipulated by laws and administrative regulations.

Protection obligations of personal information processors

- Protection from organization & people, policy & procedure, and technology enabled etc.
- Responding and addressing individual's applications for the exercise of rights.
- Pre-event risk assessment and regular post-event audit.

Personal information cross-border transfer

- Critical Infrastructure Information Operator (CIIO) and personal information processors who reach the number prescribed by the State Cyberspace Administration shall store the personal information collected and generated within the territory of the People's Republic of China.
- Pre-event risk assessment and separate consent.

Legal liability

- Ordering rectification, confiscating illegal gains, fines for organizations and people, recording in the credit profiles and compensating for losses.
- The maximum fine is not more than 50 million yuan or not more than 5% of its turnover of the previous year.

Scope of application

Scope of Application

The provisions on the scope of application in the draft PIPL are different from those in the Cybersecurity Law of the People's Republic of China (hereinafter referred to as "CSL") and the Data Security Law of the People's Republic of China (draft). Similar practice noted as European Union General Data Protection Regulation (hereinafter referred to as "EU GDPR") in extraterritorial application. Key definition reflects the data nature of "personal information", focuses where "personal information processing activities" occurs, and pays less attention to the geographic nature of "personal information processors", and stipulates that "activities carried out in processing the personal information of natural persons within the territory of the People's Republic of China" or eligible "activities carried out outside the territory of the People's Republic of China to process the personal information of natural persons within the territory of the People's Republic of China" are applicable to this law. ***(Article 3)***

Personal Information and Sensitive Personal Information

Compared with the PRC Civil Code and CSL, the draft PIPL made minor updates to the definition of "personal information" which is now more similar as EU GDPR, that is "various kinds of information related to identified or identifiable natural persons." And it clarifies that the information processed anonymously does not belong to "personal information". ***(Article 4)***

The draft PIPL separately provides the definition and protection requirements of "sensitive personal information" (formerly referred as "personal sensitive information") in "Chapter 2 Rules for Processing Personal Information, Section 2 Rules for Processing Sensitive Personal Information". "Sensitive Personal Information" is defined as "Personal Information that may lead to discrimination or serious harm to personal or property safety once disclosed or illegally used". Minor adjustments are also noted if compared with existing laws, regulations and national standards, which include, from "harm" to "serious harm", excluding "infringement of reputation", adding Sensitive Personal Information examples like "races", "ethnicity" that similar as EU GDPR. ***(Article 29)***

It is worth noting that, in addition to definition provided for "Personal Information" and "Sensitive Personal Information", the draft PIPL includes requirements "managing personal information by hierarchical classification" in "Chapter V Obligations of Personal Information Processors". However, currently in the draft PIPL, there is no classification standards indicated. In practice, it is recommended to consider sector specific data classification standards and requirements to further classify, manage and protect Personal Information being processed. ***(Article 50)***

Scope of application (Cont'd)

Personal Information Processor

The draft PIPL puts forward the concept of "personal information processor" in the domestic system for the first time, as the primary subject that bears personal information protection obligations. Essentially, the "personal information processor" defined in draft PIPL is more like "personal information controller" (Data Controller) mentioned in GB/T 35273-2020 and EU GDPR, who has the right to make independent decisions on personal information processing activities. ***(Article 69)***

In practice, organizations may act as different types of Personal Information Processors at the same time due to different processing activities, such as joint processing, entrust (and entrusted) processing, and even generally referred to as "Third Party". Special types of personal information processors undertake specific protection obligations under corresponding processing scenarios, such as:

- **Jointly processing**: Where personal information processors jointly processing personal information infringe upon personal information rights and interests, they shall bear joint and several liabilities in accordance with the law. ***(Article 21)***

- **Entrust (and entrusted) processing**: the entrusting party assumes the obligation of supervision, the entrusted party shall deal with it according to the agreement and return or delete the personal information after the completion of the contract or the termination of the entrustment relationship. Without the consent of the personal information processor, the entrusted party shall not re-entrust others to process personal information. ***(Article 22)***

- **"Third Party"**: Considering the complexity and possible scenarios of the entire cycle of personal information processing activities, the draft PIPL also sets out basic requirements on the rights and obligations of the "Third Party" involved in personal information processing activities. As the recipient of personal information, "Third Party" shall process personal information within a limited scope, and shall not use technology or other means to re-identify individuals based on the anonymized information obtained. ***(Article 24)***

Any personal information processor outside the territory of the People's Republic of China shall establish a special agency or designate a representative within the territory of the People's Republic of China to be responsible for relevant matters of personal information protection, and submit the name and contact information of relevant agency or the representative to the department performing duties of personal information protection. ***(Article 52)***

Legal basis of personal information processing

Legal basis

Based on Article 41 of the Cyber Security Law, the draft PIPL has extended the legal basis for processing personal information to a certain extent. In addition to "obtaining personal consent", if the processing of personal information meets one of the following circumstances, it can also be used as a legal basis for processing personal information ***(Article 13)***:

- ✓ Where it is necessary for the conclusion or performance of a contract to which the individual concerned is a party;
- ✓ Where it is necessary for the performance of statutory duties or statutory obligations;
- ✓ Where it is necessary for coping with public health emergencies or for the protection of the life, health and property safety of a natural person;
- ✓ Where processing personal information within a reasonable scope is to carry out such activities as news reporting and supervision by public opinions for the public interest;
- ✓ Other circumstances provided by laws and administrative regulations.

Principles

The draft PIPL reiterated a number of basic principles of personal information processing, which is highly consistent with existing international laws and best practices in relation to personal information protection, generally including lawfulness and fairness, transparency, purpose limitation, minimum necessary, accuracy and integrity, security and accountability, etc. ***(Article 5, 6, 7, 8 and 9)***

Notice and Consent

With legal basis, the draft PIPL further discusses the notice and consent requirements for the processing of personal information in different scenarios. Normally, the handling of personal information should be properly notified in accordance with applicable requirements and the individual's consent should be obtained. Individuals have the right to know and make decisions about the processing of their personal information, and have the right to withdraw or refuse. ***(Article 14, 16, 17, 18 and 44)***

Besides, the draft PIPL further clarifies certain exception scenarios, including:

Legal basis of personal information processing (Cont'd)

Notice exempted

- General provisions noted in Article 19, "a personal information processor may not notify the individual of the matters provided for in laws and administrative regulations where confidentiality shall be kept or it is not necessary to notify the individual of the matters provided for in the preceding article."

Special notice

- **Emergency**: Article 19 "In case of emergency, when it is unable to timely inform the individual to protect the life, health and property safety of natural persons, the personal information processor shall inform the individual in time after elimination of emergency."
- **Merge or split**: Article 23 "Where a personal information processor needs to transfer personal information due to merger, division or other reasons, it shall inform the individual of the identity and contact information of the recipient."

Special consent

- **Processing children's personal information**: Article 15 "If a personal information processor knows or should know that the personal information it processes is the personal information of a minor below the age of 14, it shall obtain the consent of the minor's guardian."

Separate consent

- **Providing a third party with the personal information it processes**: Article 24 "Where a personal information processor provides a third party with the personal information it processes, it shall inform the individual of the identity and contact information of the third party, purpose and method of processing and type of personal information, and shall obtain his/her separate consent."
- **Publicizing the personal information it processes**: Article 26 "A personal information processor shall not publicize the personal information it processes, unless the individual's consent is obtained, or it is otherwise required by laws and administrative regulations."
- **Processing of sensitive personal information**: Article 30 "Where the processing of sensitive personal information of an individual is subject to the individual's consent, the personal information processor shall obtain the individual's consent. Where laws and administrative regulations provide that the processing of sensitive personal information shall be subject to written consent, such provisions shall prevail. shall inform the individual of the necessity of processing sensitive personal information and the impacts on the individual."
- **Providing personal information of an individual to a party outside the territory of the People's Republic of China**: Article 39 "it shall inform the individual of such matters as the identity of the overseas recipient, contact information, purpose and method of processing, type of personal information and the way for the individual to exercise the rights prescribed herein against the overseas recipient, and shall obtain the individual's separate consent."

As for the detailed guidelines of notice and consent, it is recommended to refer to Personal Information Security Specification GB / T 35273-2020 and the Personal Information Notification and Consent Guide (Exposure Draft).

Protection obligation of personal information processor

The draft PIPL specifies requirements for personal information protection from organization and people, policy and procedure, as well as technology. Within the comprehensive personal information protection framework, the following domains are highlighted:

- **Appointment of person in charge of personal information protection; *(Article 51)***
- Training and awareness for personal information processing personnel; ***(Article 50)***
- Formulation and implementation of the overall internal management policies and procedures for personal information protection; ***(Article 50)***
- Managing personal information by hierarchical classification***; (Article 50)***
- Managing the access rights to process personal information; ***(Article 50)***
- Managing the retention period of the processed personal information; ***(Article 20)***
- **Mechanism for accepting and processing applications for exercising personal rights by individuals; *(Article 49)***
- Third party security management of personal information processing; ***(Article 22, 24)***
- Emergency response and notification of personal information incidents; ***(Article 50)***
- Personal information security technical protection (such as encryption, de-identification, etc.); ***(Article 50)***
- **Assessing the risks of personal information processing activities beforehand; *(Article 54)*** and
- Periodical audit etc. ***(Article 53)***

In practice, it is recommended that personal information protection management within the organization shall be planned and implemented in a systematic and consistent way. Detail requirements can always refer to the series of national standards, including but not limited to Guidelines for personal information security engineering (Exposure Draft), Security Impact Assessment Guide of Personal Information (Exposure Draft), Guide for De-Identifying Personal Information GB/T 37964-2019, Personal Information Security Specification GB/T 35273-2020, etc.

Where the quantity of personal information processed by a processor reaches that specified by the State Cyberspace Administration, the processor shall designate a person in charge of personal information protection to be responsible for supervising the processing of personal information and the adopted protection measures. ***(Article 51)***

The rights that individuals can exercise mainly including access and copy, correct and update, withdraw and delete, and requesting the personal information processor to explain. ***(Article 45, 46, 47, 48, 49)***

The requirements for pre-risk assessment of personal information processing activities are applicable to quite a few scenarios such as processing sensitive personal information, providing cross-border personal information, making use of personal information to make automatic decision, and providing personal information to "Third Party". The typical assessment scenarios listed overlaps those in the national standard for personal information security impact assessment, and detail assessment requirements can also refer to the standard. The risk assessment report and processing record shall be kept for at least three years. ***(Article 54)***

Requirements highly relevant to digitalization

Personal information cross-border transfer

The draft PIPL sets a separate chapter "Chapter III Rules for Cross-border Provision of Personal Information", to provide the preconditions and controls personal information cross-border transfer. In addition to the critical information infrastructure operators mentioned in the CSL, the draft PIPL further extends the scope of local storage of personal information to "personal information processors whose processing of personal information reaches the number prescribed by the State Cyberspace Administration.", which might have significant impact on sectors which are involving in processing large volume of personal information, such as online shopping, hotel services etc.. At present, there is no clear "prescribed amount" set though in the draft PIPL. ***(Article 38, 39, 40)***

In addition, personal information cross-border transfer is one of the scenarios mentioned that requires "separate consent" and risk assessment beforehand. ***(Article 39, 54)***

Image capturing and personal identification in public places

In view of the increasing application of acquisition and recognition technologies in public places, the draft PIPL specifies image capturing and personal identification equipment installed in public places shall be necessary for maintaining public security, comply with relevant provisions of the State, and conspicuous prompting signs shall be installed. Personal images and personal identity feature information collected can only be used for the purpose of maintaining public security, and can not be publicized or provided to others, unless the individual's separate consent is obtained, or it is otherwise required by laws and administrative regulations. ***(Article 27)***

Requirements highly relevant to digitalization (Cont'd)

Processing disclosed personal information

The draft PIPL also sets requirements on processing of legally disclosed personal information. Such processing shall conform to the purposes for which such personal information is disclosed; where such processing is beyond the reasonable scope relating to the purposes, the personal information processor shall inform the individual concerned and obtain his/her consent in accordance with this Law. Where the purposes for which personal information is disclosed are not clear, the personal information processor shall process the disclosed personal information in a reasonable and prudent manner; where such personal information is used to engage in the activities that have great impact on the individual concerned, the personal information processor shall inform the individual and obtain his/her consent in accordance with this Law. ***(Article 28)***

Automatic decision-making

The draft PIPL defines an automatic decision-making as "an activity in which personal information is used to automatically analyze and evaluate a person's behavior habits, hobbies or economic, health or credit status through computer programs and make decisions." ***(Article 69)***

The Personal Information Security Specification GB/T 35273-2020 has preliminarily clarified the relevant requirements when adopting automatic decision-making mechanisms in information systems. The Personal Information Security Specification GB/T 35273-2020 mainly requests that personal information processors should provide individuals with channels to raise complaints against the results of automatic decision-making and support manual review of the results of automatic decision-making.

The draft PIPL adds that if an individual believes that automatic decision-making has a significant impact on his/her rights and interests, he/she has the right to require the personal information processor to provide explanation, and to reject the decision made by the personal information processor only through automatic decision-making. In addition, where business marketing and information push are carried out through automatic decision-making, options not based on his/her personal characteristics shall be provided at the same time. ***(Article 25)***

Making use of personal information to make automatic decisions shall assess the risks of personal information processing activities in advance and keep a record of the processing as well. ***(Article 54)***

Compliance and legal liability

Competent Authority

The draft PIPL specifies that at the central level, the State Cyberspace Administration is responsible for coordinating the protection of personal information and relevant supervision and administration work; and relevant departments under the State Council are responsible for protecting, supervising and administering personal information within the scope of their respective duties in accordance with the provisions of this Law and relevant laws and administrative regulations. And at the local level, the duties of relevant departments of local people's governments at or above the county level in protecting, supervising and administering personal information shall be determined in accordance with relevant provisions of the State. ***(Article 56, 57, 58)***

To fulfill the responsibility of personal information protection, an effective mechanism should be established to receive and handle complaints and reports on illegal personal information processing activities. ***(Article 61)***

When departments performing duties of personal information protection perform duties in accordance with the law, the personal information processor shall provide assistance and cooperation, and shall not refuse or obstruct such performance. ***(Article 59, 60)***

Legal Liability

Slightly different from the China Cybersecurity Law, the draft PIPL does not specify specific responsibilities for violating certain clauses. Possible consequences of violations include ordering rectification, confiscating its illegal gains, fines for organizations and people, being recorded in the credit profile and compensation for losses. The capped amount of fines for serious violations has been significantly increased compared with other laws like CSL, which is now set as not more than 50 million yuan or not more than 5% of the previous year's turnover, while the "coverage" of turnover is not yet quite clear. ***(Article 62, 63, 65)***

In addition, similar clauses regarding liability for compensation as EU GDPR, that the draft PIPL also mentions if the personal information processor can prove that it is not at fault, its liability may be mitigated or exempted. ***(Article 65)***

Laws, regulations and national standards related to personal information protection (selected)

2020

- Civil Code of the People's Republic of China (to enact from January 1st, 2021)
- Data Security Law of the People's Republic of China (Draft)
- Personal Information Protection Law of the People's Republic of China (Draft)
- Personal Information Security Specification GB/T 35273-2020
- Cyber-data Process Security Specification (Exposure Draft)
- Guideline for Personal Information Notice and Consent(Exposure Draft)
- Specification on Collection Personal Information with Mobile Internet Applications(Apps) (Exposure Draft)
- Cybersecurity Standard Practice Guide - Guidelines for Personal Information Security Protection of Mobile Internet Applications (APP) (TC260-PG-20203A)(Exposure Draft)
- Cybersecurity Standard Practice Guide - Assessment Guidelines for Collecting and Using Personal Information of Mobile Internet Applications (APP) (TC260-PG-20202A)

2019

- Interpretation of the Supreme People's Court and the Supreme People's Procuratorate on Several Issues Concerning the Application of Law in the Handling of Criminal Cases Involving Illegal Use of Information Networks and Assistance in Criminal Activities Committed through Information Networks
- Announcement of Launching Special Crackdown Against Illegal Collection and Use of Personal Information by Apps
- Guide to the Self-Assessment of Illegal Collection and Use of Personal Information by Apps
- Identification Method for the Behaviour of APP to Collect and Use Personal Information Illegally
- Provisions on Children's Online Privacy Protection
- Administrative Measures on Data Security (Exposure Draft)
- Measures for Security Assessment for Cross-border Transfer of Personal Information (Exposure Draft)
- Guideline for Internet Personal Information Security Protection
- Guide for De-Identifying Personal Information GB/T 37964-2019
- Guidelines for Personal Information Security Engineering (Exposure Draft)
- Cybersecurity Practice Guide - Necessary Information Specification for Basic Business Functions of Mobile Internet Applications (TC260-PG-20191A)

2018

- E-commerce Law of the People's Republic of China
- Security Impact Assessment Guide of Personal Information (Exposure Draft)

2017

- Cybersecurity Law of the People's Republic of China
- Interpretation of Several Issues regarding Application of Law to Criminal Cases of Infringement of Citizen's Personal Information Handled by the Supreme People's Court and the Supreme People's Procuratorate
- Measures for the Security Assessment of Personal Information and Important Data to be Transmitted Abroad (Exposure Draft)
- Guidelines for Data Cross-Border Transfer Security Assessment (Exposure Draft)

Before 2017

- Law of the People's Republic of China on the Protection of Rights and Interests of Consumers
- Amendment to the Criminal Law of the People's Republic of China (7)
- Amendment to the Criminal Law of the People's Republic of China (9)
- Decision on Strengthening Network Information Protection
- Provisions on Protecting the Personal Information of Telecommunications and Internet Users

Recommendation on next actions

In terms of the overall legislative process, the Personal Information Protection Law was included in the legislative plan of the 13th National People's Congress of the People's Republic of China in 2018, and passed by the 44th Chairman's Meeting of the 13th National People's Congress of the People's Republic of China in 2019. The formulation of the Personal Information Protection Law was clearly included in the 2020 Legislative Work Plan of the Standing Committee of the National People's Congress. The official release of the draft of this protection law indicates that the progress of relevant legislation is proceeding in an orderly manner as planned, and thus it is suggested to keep closely monitoring of the process and changes to adapt the compliance strategies of the organization in a timely manner.

According to the list of current domestic laws, regulations and national standards related to personal information protection shared, it is quite clear that currently the implementation of the personal information protection activities is not impossible and unfounded. On the contrary, the current relatively complex compliance landscape brings greater challenges on how companies can effectively manage personal information protection risks during the "uncertain" period, especially how to consider personal information protection in the process of digital transformation and the application of new technologies such as big data, so as to ensure business development and expansion.

To better manage the overall compliance risk of enterprises and ensure the security of personal information, it is recommended that immediate actions should be taken to proactively manage and protect personal information:

01

Health check and roadmap plan

Conduct as-is assessment, considering digital transformation and data strategy, to develop strategy plan and implementation roadmap for personal information protection within the organization.

02

Achieve quick-wins for key risk areas

Quick remediation in high-risk domains, usually including establishment of governance and operating models, revision of legal documents, establishment of emergency response and data subject right fulfilment mechanism, and training and awareness etc.

03

Phased approach to roll-out

Take phased approach to roll out the systematic protection and management of personal information in different business units, and implement with technology to enable the automation of control process.

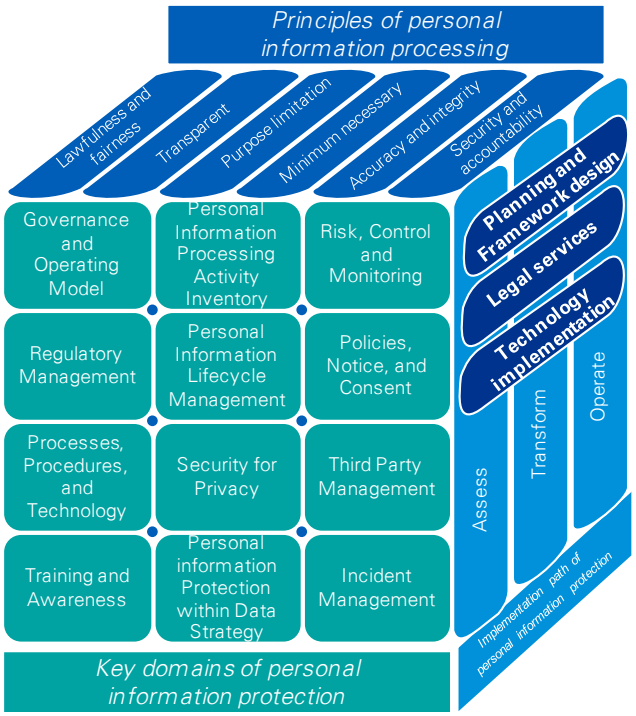
04

Continuous improvement and enhancement

Continuously improve and enhance the overall framework, process and technical measures to ensure its consistency and effectiveness with the evolving internal and external environments.

KPMG personal information protection framework and services

KPMG's personal information protection management framework and services are dedicated to solving customers' real business and technical threats, and assisting companies to gradually improve. KPMG's personal information management maturity model not only targets the general personal information protection requirements of various industries, but also meets the industry-specific personal information protection requirements applicable to enterprises, such as Personal Financial Information Protection Technical Specification JR/T0171-2020, Financial data security—Guidelines for data security classification JR/T 0197-2020, etc. which is customized to assist enterprises in current situation assessment and goal planning, refine the construction and improvement action plan of each component, and promote personal information protection in an orderly and comprehensive way.



Global collaborated cybersecurity and legal professionals

Rich experience for personal information protection assess, planning and implementation

Active Player in China's Cyber Ecosystem


Shift
Pg Dn
End

Contact us

Henry Shek
KPMG China
Cybersecurity Advisory
Partner
Tel: +852 2143 8799
henry.shek@kpmg.com

Richard Zhang
KPMG China
Cybersecurity Advisory
Partner
Tel: +86 (21) 2212 3637
richard.zhang@kpmg.com

Brian Cheung
KPMG China
Cybersecurity Advisory
Director
Tel: +852 2847 5062
brian.cheung@kpmg.com

Quin Huang
KPMG China
Cybersecurity Advisory
Director
Tel: +86 (21) 2212 2355
quin.huang@kpmg.com

Danny Hao
KPMG China
Cybersecurity Advisory
Director
Tel: +86 (10) 8508 5498
danny.hao@kpmg.com

Rocky Wu
上海睿威律师事务所
Data and IP protection
Partner
Tel: +86 (21) 5203 1587
rocky.wu@kpmglegal.com.cn