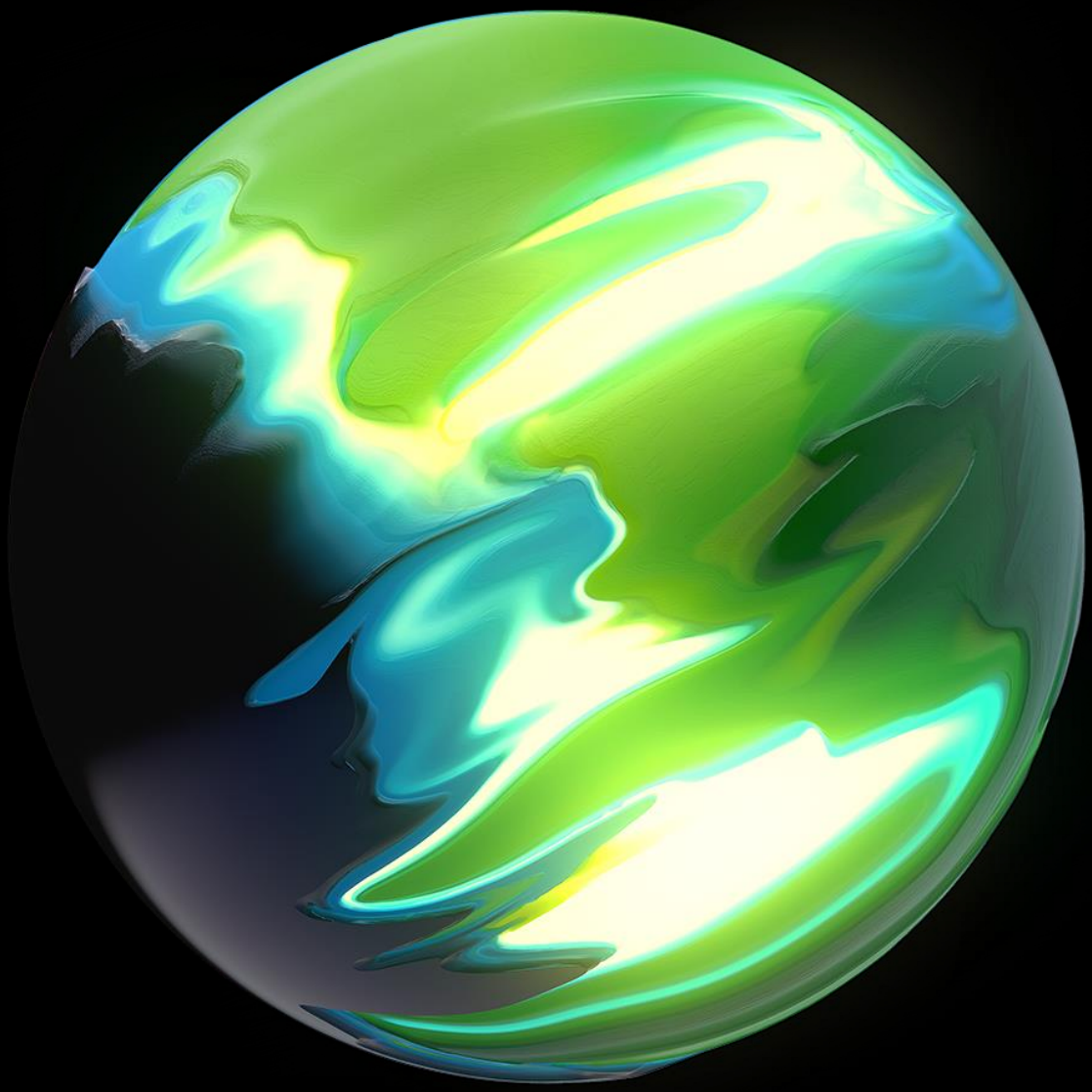
Deloitte.

德勤



China draft Personal Information Protection Law (PIPL) General introduction and impact analysis

May 2021

MAKING AN IMPACT THAT MATTERS since 1845

Introduction of the draft Personal Information Protection Law (PIPL)

Background of Draft PIPL

As data privacy is getting prioritized worldwide, many countries have started to frame relevant laws and regulations in recent years on personal information protection. PIPL is the **new data privacy law** in China, targeted at **personal information protection** and **addressing the problems with personal data leakage**. The PIPL is applicable to **organizations and individuals who process personally identifiable information (PII)** in China. This includes organizations and individuals that are **located outside of China** but processing, analyzing or accessing **PII of individuals in China**. The first draft was submitted to the National People's Congress of the People's Republic of China for review in early October 2020. Below is the enactment timeline of the law anticipated before the end of 2021:

**There is currently no official announcement about the official enactment date of this law. However, by taking reference to the panel discussion of the IAPP's Global Privacy Summit Online 2021, the finalization of the laws is likely to happen before the end of 2021. (Source: https://iapp.org/news/a/china-india-could-finalize-privacy-legislation-by-years-end/?mkt_tok=MTM4LUVaTS0wNDIAAAF8miTR9UoAz2HuPVZjOHhUB50ER7qemVXxHS_nLOjfY_INnqbK8m7ImtVaFFeT1LHSYnWpjVvfjYh_IIw1g0wnQx8U2BQxJy05AHZqWZZUiv83)*

How PIPL impacts your organization

- **Data subjects are given more rights** over the use of their own data. They can request to edit, remove, restrict the use of their data, or withdraw consent given previously.
- **More stringent requirements** on data sharing and data transfer, which your organization and any third party joint data controllers may need to pass data related assessments.
- **Penalties and fines** on organizations for data breaches. Including increased fines (up to 50 million RMB), revenue confiscation (up to 5% annual revenue) and business cessation.
- **Mandatory security controls** to be applied when storing and processing the PII, and **training** to be provided to responsible personnel who handles the PII.
- **Mandatory data localization** when the amount of PII exceed the threshold set by the Cybersecurity Administration of China (CAC).

Are you and your employees, systems, business partners ready to support these changes?

Definitions of Information

Personally Identifiable Information (PII)
All kinds of information relating to **identified or identifiable natural persons** which is recorded by electronic or other means, excluding any anonymized information. PII includes Critical Information Infrastructure (CII) and Sensitive Information (SI).

Critical Information Infrastructure (CII)
information which will result in **serious damage** to state security, the national economy and the people's livelihood and public interest if it is destroyed, loses functions or encounters data leakage.

Sensitive Information (SI)
Information that, once leaked or illegally used, may lead to **personal discrimination or material harm** to personal or property security, including race, ethnicity, religious beliefs, individual biometric features, medical health, financial accounts, individual location tracking and other information.

Outline of the Draft PIPL

CHAPTER

I **General Provisions**
Article 1 – 12 *Key takeaway: Purpose and definitions*

II **Chapter II. Rules on Processing of Personal Information**
Article 13 – 37 Key takeaway: lawful collection and processing of PII

III **Rules on Cross-Border Provision of Personal Information**
Article 38 – 43 *Key takeaway: The **preconditions and controls** for transferring PII abroad*

IV **Rights of Individuals in processing of Personal Information**
Article 44 – 49 *Key takeaway: Individuals' **rights over their own PII** and to **give or withdraw consent** over the use of their PII.*

V **Obligations of Personal Information Processors**
Article 50 – 55 *Key takeaway: A set of requirements for PII processors to **protect the data collected**.*

VI **Authorities Fulfilling Personal Information Protection Duties and Responsibilities**
Article 56 – 61 *Key takeaway: Responsibilities of CAC and related departments.*

VII **Legal Liability**
Article 62 – 67 *Key takeaway: **Penalties and fines** for violation of the regulatory requirements stated in this law*

VIII **Supplementary Provisions**
Article 68 – 70 *Key takeaway: Definitions and official enactment date (to be determined)*

Key highlights and our interpretation of the draft PIPL

Key Highlights of the Law

Category	Article No. & Content	What You Need to Do	Impact and Penalty
Obtain Consent of Individuals for Data Handling	**Article 24:** **Notifications** to, and **explicit consent** from the data subjects when **third parties** are involved in the PII processing.	All **matters related to PII processing activities**, including the identity and contact details of data recipients must be **provided to data subjects**. **Consent must be obtained** prior any PII processing.	When PII rights and interests are infringed, PII handlers need to **compensate the individuals** for: • the loss the individuals suffered • the benefit obtained by the PII handler(s) **Lawsuit filed to a People's** if the infringement involves many individuals. Below impacts and penalties will be resulted if PII processors fail to comply to the requirements stipulated in this law: • **Confiscate unlawful income** • Issue warning • A **fine of up to 50,000,000 RMB** or 5% annual revenue • **Suspension** of related business activities • **Cessation of business** for rectification • **Cancellation** of professional **licenses or business permits.** • **Additional fine** of max. 1,000,000 RMB if correction is refused
Organizational Governance	**Article 50:** PII processors to **adopt security measures** to **prevent unauthorized access** and **protect the PII** from data leakage, theft, distortion of deletion.	PII processors should **adopt security measures to protect the PII collected** (e.g. applying data encryption, providing security training and education to employees).	
	Article 51 & 52: PII processors (both in or outside of China) to **appoint responsible persons for supervision** of PII processing and protection activities.	PII processors should **appoint responsible person(s) for supervising the data activities** on PII and security measures adopted for protecting PII,	
Rights of Individuals	**Article 44, 45, 46 & 48:** Data subjects' rights **access or correct the PII**, and to **know, decide or request for the explanation** of the processing of their PII.	Individuals can **decide whether organizations can process** their PII and to what extent, or to make changes, or delete the PII collected.	
Cross Border Data Transfer (CBDT)	**Article 39:** **Notifications** to, and **explicit consent** from the data subjects when their PII needs to be **transferred outside of People's Republic of China.**	**Notify the individual on the CBDT arrangement,** ways to exercise their rights, and obtain consent.	
	Article 40: When CIIOs and PII processors process PII exceeding the amount set by CAC, they should **pass a security assessment** if they need to provide PII to any party outside the People's Republic of China.	CIIOs and PII Processors who meet data volume threshold (to be determined) set by CAC shall **pass the security assessment before cross-border data transfer can take place.**	
Data Localization	**Article 40** – When CIIOs and PII processors process PII exceeding the amount set by CAC, they should **store personal information collected and produced in the People's Republic of China domestically**.	CIIOs and PII Processors who meet data volume threshold* set by CAC shall **store all PII collected and generated within Mainland China.**	

*Note: Data volume threshold is not yet determined, but following the Measures for the Assessment of Personal Information and Important Data Exit Security (draft for comment) released in 2017 April, the data volume threshold was set to be 500,000 data subjects or 1,000 GB.)

PIPL implications to organizations from data life cycle perspective

Do you meet the mandatory requirements set in the draft PIPL to store or process PII?
Although the enactment date of draft PIPL is still undetermined, and some regulations are subject to further revisions, organizations should consider below potential impact in order to prepare for the change in regulatory requirements.
By taking reference of the grace period given when the China Cybersecurity Law was enacted (i.e. 19 months), organizations have **approximately one and a half year to comply** to the requirements stated in the PIPL once enacted.

Below are some mandatory requirements from the draft PIPL which **you should consider when you process personal data in the Cloud**.

Data Life Cycle Stages	Mandatory PIPL Requirements
Data Subject Notification	**Inform the data** subjects for below data activities: • The **purpose and method** of collecting / processing the data subjects' PII • The **rights of data subjects** that they could request to: inquire, access, edit, delete, restrict or refuse, withdraw consent, etc. • The **transfer of data subjects' PII** to Cloud Service Providers, any third parties processing the PII on behalf of the organization, or recipients outside of the country (i.e. Cross-border data transfer).
Right to Use & Disclose	Before collecting and processing data subjects' PII, the rights to use their PII must be granted (i.e. **consent obtained from the data subjects**): • **Transferring data subject's PII** to Cloud Service Providers, any third parties processing the PII on behalf of the organization, or recipients outside of the country (i.e. Cross-border data transfer). • **Processing of PII of data subjects** (e.g. analytics, internal data related assessments, potential job opportunities, etc.)
Data Collection	• Ensure **secure channel** in collecting and uploading (e.g. to Cloud) the PII • If images or videos are to be taken from data subjects, the image collection or **personal identity recognition equipment shall be installed in public venues**
Data Usage	• **Apply security protection measures** such as encryption and de-identification to protect the PII stored in the Cloud from unauthorized access, data leakage of theft, distortion or deletion. • **Appointing person-in-charge to supervise and monitor** the data protection measures and process and provide training to the responsible staff • **Data localization of PII collected** if the amount of PII processed exceeded the threshold set by the CAC
Data Sharing / Transfer	To **transfer / share the data subjects' PII** to Cloud hosted **outside of the country**, organization must meet at least one of the following: • **Pass the security assessment organized by CAC** (including any third parties that are processing the data on behalf of the company) and file an application for approval if the transfer is for international judicial assistance or administrative law enforcement assistance. • **Undergo Personal Information Protection Certification** conducted by a professional agency according to the requirements of the Cyberspace Administration of China. • **Conclude a contract with the foreign receiving party**, agreeing on both sides' rights and obligations, and supervising their PII processing to ensure that the PII standards provided by PIPL are met.
Data Disposal / Retention	• Delete the PII of data subjects **upon their request** (e.g. data subjects ask to withdraw consent for transferring / sharing data overseas or have their data removed from the company). • Delete the PII of data subjects **when the agreed retention period has expired** or the **processing purpose has been achieved**. • **Cease processing** the PII of data subjects if it is **technically difficult to delete** such PII.

Are you ready to fulfill all the above mandatory requirements in the given timeframe?

How Deloitte can help

Our Success Stories

Our Deloitte Cyber professional team has the experience and knowledge to get you prepared for the major transition in handling data privacy related issues. Below are some **recent successful stories of PIPL-specific and other data privacy law challenges**, which may also apply to you:

Conduct digital and privacy assessments under business resilience, covering the obligations and readiness for the enactment of PIPL

Find the ideal method and implement the strategy for you to access global client data in a secure compliant protocol under all these increasingly stringent data privacy laws (e.g. Cyber Security Law (CSL), PIPL)

Help you **understand and realize your top technology risks** to ensure **business continuity and resilience** of operations in China

Provide recommendations and support remediation of any related **data privacy law gaps** across business operations

Establish data privacy awareness and training program to raise staff awareness and ensure ongoing alignment to regulatory and policy requirements

Are you facing similar challenges?

Our Extended Service Offerings

Governance & Compliance	• Impact analysis of PIPL requirements and advisory on local / global security standards to meet regulatory requirements. • Define the suitable and practical PIPL compliance management framework.
Gap Assessment	• Perform gap analysis and benchmarking against peers. • Governance setup & tool implementation, including data & process discovery, process automation / enhancement.
Data Privacy & Protection	• Perform security & privacy risk analysis of your organization's and your desired (Cloud) IT architecture. • Develop appropriate data privacy & security solutions to protect PII
Technology & Digital	• Data discovery, mapping, and inventories; privacy-by-design advice and application; online and e-Privacy; digital asset risk assessment and management
DPO as a Service	• DPO as a service to support clients in becoming and staying compliant with data privacy laws and related regulations. • Perform real-time security analytics with our global cyber threat intelligence insight to provide 24x7 Managed Security Services (MSS).
Cloud and Infrastructure Security	Wide range of innovative, end-to-end Cyber + Cloud capabilities tailored to our your environments while enabling significant and secure digital transformation: • Cloud governance and compliance • Cloud infrastructure security • Cloud security management • Cloud security strategy and planning

Why Deloitte?

Strength in Numbers

What sets Deloitte Cyber apart from the competition is the know-how. Deloitte has the experience in dealing with many of the **world's toughest cyber and privacy issues**, helping clients solve our **most complex business challenges**. It's our team that doesn't quit—it's our experience you can depend on, it's our commitment that we stand behind. **Why trust anyone else**?

17,000+
cyber and risk practitioners worldwide

125+
offices across APAC and Global

26+
years providing cyber and privacy risk services

30+
Cyber Intelligence Centre

Contact us @ Deloitte data & privacy

Brad Lin
Director, Risk Advisory
Tel: +852 2109 5353
Email: bradlin@deloitte.com.hk

Hatty Siu
Associate Director, Risk Advisory
Tel: +852 2852 5898
Email: hattysiu@deloitte.com.hk

Flarey Ying
Senior Consultant, Risk Advisory
Tel: +852 2258 6034
Email: fying@deloitte.com.hk

Vivien Peng
Senior Consultant, Risk Advisory
Tel: +852 2109 5238
Email: vivipeng@deloitte.com.hk

Designed by CoRe Creative Services. RITM0707909