Cooley

China's New National Privacy Law: The PIPL

November 30, 2021

As the world continues to work from home in the wake of COVID-19, and companies lean on online technologies to conduct their businesses and service their customers, the People's Republic of China (home to the most online users in the world), is one of the latest countries to pass a new omnibus privacy law. Effective November 1, 2021, despite numerous yet-to-be-defined elements, the Personal Information Protection Law (PIPL)[1] is China's first comprehensive law designed to regulate online data and protect personal information.

China's Data Security Law went into effect earlier this year, on September 1, 2021, and applies to a wide range of data processing activities including, but not limited to, processing personal information. With extraterritorial scope and severe fines and penalties, these laws are set to impose an increasingly complex and comprehensive legal framework for processing personal information when doing business in China.

The PIPL is enforced and administered by the Cyberspace Administration of China and relevant state and local government departments. The law draws from the European Union's General Data Protection Regulation (GDPR), with heavy penalties up to the greater of 5% of the previous year's revenue (possibly global) or $7.7 million. The PIPL consists of more than 70 articles spanning eight chapters. (Read the full, unofficial translation of the text.) Our takeaways and a summary of key provisions of the law are below.

Our take

Given the broad scope, extraterritorial application and potential for substantial fines, organizations or individuals should assess their PIPL compliance obligations if they process personal information within China, for the purpose of providing products or services for individuals within China, or to analyze or evaluate the behavior of individuals within China. These obligations could include:

- Adjusting public-facing documentation such as privacy policies, data subject rights request procedures, and other user interfaces and user experiences (such as sign-up flows).
- Implementing the forthcoming standard contractual clauses in contracts involving personal information that is transferred outside China.
- Implementing consent mechanisms, including multiple layers of consent for certain processing activities or transfers (e.g., transferring personal information outside of China or to another personal information processor).
- Adding PIPL data breach notification requirements to incident response plans.
- Assessing the need to localize data in China and the impact that might have on global operations.

Data mapping and other exercises related to compliance with the GDPR, California Consumer Privacy Act (CCPA) and other regulations likely can be repurposed to make PIPL compliance less onerous, although some customization will be needed. Overall, PIPL compliance efforts likely will remain a work in progress, given the uncertainty posed by interpretations and enforcement of the lengthy new law, and pending implementing rules and regulations. As with the CCPA and GDPR, clients should continue to monitor amendments to the PIPL, its implementing regulations and relevant enforcement actions, and adjust their practices accordingly. Cooley's global team of privacy experts is working with many clients who do business in China to assess PIPL compliance obligations. Reach out to any of the contacts listed below to discuss your PIPL questions.

Who must comply with the PIPL?

Like the GDPR, the PIPL is intended to impose extraterritorial jurisdiction, and arguably covers any company or individual that processes the personal information of individuals in China (regardless of the individual's nationality or residency).[2] Additionally, the PIPL requires personal information processors (also known as personal information handlers, or 个人信息处理者) located outside of China to establish dedicated entities or

appoint individual representatives in charge of personal information within China.[3] Such organizations or representatives do not need to have any employment relationship or be affiliated with the foreign processor. Furthermore, and similar to the data protection officer concept in the GDPR, personal information processors processing a certain threshold of personal information (although the threshold remains undefined to date) are required to designate and publish the contact information of an individual in charge of processing and protecting personal information.[4]

Does the PIPL differentiate between 'controllers' and 'processors' of personal information?

In a designation that is sure to cause some confusion, under the PIPL, "personal information processors" are akin to "controllers" and "entrusted parties" are like "processors" under the GDPR. Personal information processors assume liability and compliance requirements in the PIPL. Meanwhile, joint personal information processors must enter into an agreement that designates the specific rights and obligations for each personal information processor and indicates that joint personal information processors are jointly liable.[5]

Additionally, if the processing of personal information is performed by an entrusted party (e.g., a processor under the GDPR) on behalf of a personal information processor, the parties must enter into an agreement that specifically designates the purpose, duration, method, categories, protection, rights and duties of processing of personal information.[6] In practice, the data processing agreement should include the following based on the requirements in the PIPL[7]:

- A prohibition against the entrusted party processing personal information outside the agreement.
- Terms requiring the entrusted party to return or delete personal information upon completion, revocation or expiration of the agreement.
- Provisions requiring the entrusted party to obtain the personal information processor's consent before allowing a sub-processor to process personal information.

What type of data is covered under the PIPL?

The PIPL defines personal information like the CCPA and GDPR do, as:

… various kinds of information related to identified or identifiable natural persons recorded by electronic or other means, excluding the anonymized information.[8]
The PIPL also follows the CCPA and GDPR by deeming anonymized information as nonpersonal and outside the scope of the law. However, the definition of anonymization is strict and may be hard to meet:

Anonymization refers to a process in which the personal information is processed so that it is impossible to identify a certain natural person and unable to be reversed.[9]
Like the CCPA (as modified by the California Privacy Rights Act (CPRA)) and the GDPR, the PIPL ambiguously defines "sensitive personal information":

Sensitive personal information refers to the personal information that can easily lead to the infringement of the personal dignity of natural persons or the harm of personal or property safety once leaked or illegally used, including such information as biometrics, religious belief, specific identities, medical health, financial accounts, and whereabouts, and the personal information of minors under the age of 14.[10]
Sensitive personal information is subject to additional requirements for processing such as:

- Identifying a specific purpose and sufficient necessity for the processing.
- Providing notice to the individual of the impact that the processing will have on the individual's rights and interests.
- Requiring the use of "strict protective measures" (still undefined).
- Conducting a privacy impact assessment and creating a record of processing.
- Obtaining separate individual consent for the processing (and possibly **written consent** where required by yet-to-be-published regulations).

The PIPL also instructs the Cyberspace Administration of China to formulate special personal information protection rules and standards for sensitive personal information processing.[11]

What are the legal bases available for data processing under the PIPL?

Under the PIPL, personal information processors may only process personal information where:

1. Consent of the individual has been obtained, which must be informed, voluntary and explicit (at thresholds not yet defined), subject to the following:[12]
    a. If the purpose, method or categories for processing information changes, new consent must be obtained.
    b. Individuals must have the ability to withdraw consent by "convenient means" (not yet defined).
    c. The provision of products or services can't be conditioned on the basis of consent, unless the information being collected is necessary for providing the products or services (which appears to reflect the concept of "freely given" consent under the GDPR).
    d. Parental/guardian consent is necessary if the processing involves personal information of a minor below the age of 14.[13]
2. It is necessary for the conclusion or performance of a contract to which the individual is a party, or to implement human resources management in accordance with labor rules and regulations formulated and collective contracts concluded according to law.
3. It is necessary for the fulfillment of statutory duties or obligations.
4. It is necessary for coping with public health emergencies or for the protection of an individual's life, health or property.
5. Such acts as news reporting and supervision by public opinions are carried out for the public interest, and the processing of personal information is within a reasonable scope.
6. The personal information has already been disclosed by the individual, or other legally disclosed personal information is processed within a reasonable scope in accordance with the provisions of this law.
7. Other circumstances exist as provided by Chinese laws and regulations.

Notably, the PIPL indicates that individual consent is the default legal basis for processing unless one of the other legal bases applies. Also noteworthy is the absence of a "legitimate interest" processing basis as is available under the GDPR, which has been used by many EU data controllers as a more flexible means of establishing a legal basis for processing. However, it is still possible that Chinese authorities could expand the available legal processing bases via regulation.

What types of notice are required under the PIPL?

Privacy notice

Before the processing of personal information, a personal information processor must truthfully, accurately and completely inform individuals in an "eye-catching manner with clear and understandable language" that includes:[14]

- The name and contact method of the personal information processor.
- The purpose and method of processing personal information, and the type and retention period of processed personal information.
- Methods and procedures for individuals to exercise the rights provided under the PIPL.
- Other items about which laws or administrative regulations provide shall be notified.

Additionally, individuals must be notified of any changes to these key data processing elements.

Notice for consent purposes

Where the legal basis for processing of personal information is consent, personal information processors must provide robust notice, in clear and easy-to-understand language, before processing personal information.[15]

Notice of personal information transfers for business transactions

Where a personal information processor transfers personal information during a business transaction, the processor must inform individuals of the name and contact information of the recipient. The PIPL also requires new consent to be obtained if the recipient changes the purpose or method of processing personal information.[16]

Notice for transfers of personal information to another personal information processor

If a personal information processor transfers personal information to another personal information processor, the processor must:

- Notify the individual of the name and contact information of the new personal information processor.
- Notify the individual of the purpose and method of processing, as well as the type of personal information being processed by the new personal information processor.
- Obtain separate consent for this new processing.

The new personal information processor must also adhere to the original scope of the method, purpose and type of personal information communicated to the individual, or obtain new consent.[17]

What individual rights does the PIPL provide?

The PIPL creates specific rights for individuals with respect to the processing of their personal information, including the right to[18]:

- Know, decide on, and limit or object to processing personal information by others.
- Access and copy (including transfer) their information from personal information processors.
- Request correction or completion of their personal information.
- Request deletion in certain circumstances or withdraw consent.

Personal information processors must establish a convenient, but undefined, mechanism for individuals to exercise these rights.[19] Notably, relatives of a deceased natural person may – for their own lawful and legitimate interests – access, copy, correct and delete the personal information of the deceased.[20]

Does the PIPL require data privacy impact assessments?

Personal information processors and controllers must conduct and keep for three years personal information protection impact assessments (PIPIAs) for certain personal information processing, including:

1. Processing sensitive personal information.
2. Using personal information to make automated decisions.
3. Entrusting others to process or otherwise share or disclose personal information.
4. Transferring personal information overseas.
5. Other processing activities that significantly impact an individual's rights and interests.[21]

PIPIAs must include a determination of[22]:

- Whether the purpose and method of processing personal information are legitimate, justifiable and necessary.
- The impact on individuals' rights and interests, and the security risks.
- Whether the security protection measures taken are legitimate, effective and appropriate to the degree of risks.

Does the PIPL (or other Chinese data protection laws)

impose data localization requirements and/or restrict cross-border data transfers?

In addition to providing notice of the transfer to relevant individuals and obtaining consent,[23] personal information processors must conduct an ex-ante impact assessment of personal data protection and record processing circumstances,[24] and meet one of the following conditions before transferring personal information outside of China:[25]

- Pass a security assessment organized by the Cyberspace Administration of China.[26]
- Obtain a certification issued by the organization as authorized by Cyberspace Administration of China.
- Sign a cross-border data transfer agreement with the overseas data receiver(s) according to the standard contract formulated by the Cyberspace Administration of China, specifying the rights and obligations of both parties.
- Satisfy another mechanism that may be provided for by other laws and regulations.

Additionally, the PIPL requires critical information infrastructure operators (CIIOs)[27] or the personal information processors handling large amounts of personal information (at thresholds that have yet to be defined) to store personal information locally within China.[28] Such CIIOs or large volume processors can **only** transfer personal information overseas when such a transfer is necessary **and** they pass an official security assessment.[29]

Without elaboration, the PIPL requires personal information processors to take necessary measures to ensure that the processing of personal information by overseas recipients meets the personal information protection standards stipulated under the PIPL.[30]

Personal information processors must also obtain individual consent for the cross-border transfers after informing individuals of:

1. The contact information of the overseas recipient of their personal information.
2. The purposes, method and type of personal information being transferred overseas.
3. The procedures for exercising their rights under the PIPL regarding that data.[31]

What are the potential penalties for failing to comply with the PIPL?

PIPL penalties are graduated depending on the severity of noncompliance, ranging from a warning and order to cure violations, to an order suspending services or revocation of operating permits or business licenses, to the confiscation of illegal gains, to significant administrative fines. Company employees also may be held personally liable and face fines or be banned from serving as directors, supervisors, officers or persons-in-charge of personal information protection matters for the relevant entities.

Companies and/or their employees may even face criminal liability in serious cases.[32] For instance, any person who illegally obtains, sells or supplies to third parties more than 500 pieces of information that can affect citizens' personal and financial safety (such as lodging information, communication records, health and physical information, transaction information, etc.) in violation of the PIPL may be sentenced to up to three years of detention.[33]

Notes

1. This blog post was based on an unofficial English translation of the PIPL.
2. Article 3.
3. Article 53.
4. Article 52.
5. Article 20.
6. Article 21.
7. *Id.*

8. Article 4.
9. Article 73(IV).
10. Article 28.
11. Article 28, Article 29, Article 30, Article 31, Article 32, Article 55.
12. Article 14.
13. Article 31.
14. Article 17.
15. Article 14.
16. Article 22.
17. Article 23.
18. Chapter IV: Rights of Individuals in Activities of Processing Personal Information.
19. Article 50.
20. Article 49.
21. Article 55.
22. Article 56.
23. Article 39.
24. Article 55.
25. Article 38.
26. The Cyberspace Administration of China released a draft Security Review Measures for Cross-Border Data Transfer for public comment on October 29, 2021. While still a draft, it adds clarity with respect to when security reviews would be required, review criteria and procedures, key terms of data transfer agreements (although draft standard contractual clauses were conspicuously absent), and review frequency.
27. Per both the Cybersecurity Law and the Regulation on Protection of Security of Critical Information Infrastructure, “critical information infrastructure” is defined as important network facilities, information systems, etc. in important industries and fields such as public communications and information services, energy, transportation, water, finance, public services, electronic government affairs and national defense technologies, and others which, in the event of damage thereto, loss of function thereof or leak of data therefrom, could seriously jeopardize national security, national economy and people’s livelihoods, or the public interest.
28. Article 40.
29. *Id.*
30. Article 38.
31. Article 39.
32. Article 71.
33. Article 253a of the People’s Republic of China Criminal Law and Article 5.4 of the 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 of Infringing on Citizens’ Personal Information.

Key Contacts

Allison Nostdahl New York	anostdahl@cooley.com +1 212 479 6774

Zixiang Liu Shanghai	zliu@cooley.com +86 21 6030 0685