Professional Perspective

China Personal Information Protection Law (PIPL) FAQs

Ken (Jianmin) Dai and Jet (Zhisong) Deng, Dentons

Bloomberg Law

China Personal Information Protection Law (PIPL) FAQs

Contributed by Ken (Jianmin) Dai and Jet (Zhisong) Deng, Dentons

Q1. What is the PIPL?

China's Personal Information Protection Law (PIPL), adopted on Aug. 20, 2021, at the 30th Session of the Standing Committee of the 13th national People's Congress, is the first national-level law comprehensively regulating issues in relation to personal information protection.

> **Comment:** The text of the PIPL is available in Mandarin and English.

Q2. When did the PIPL take effect?

The PIPL entered into force as of Nov. 1, 2021.

Q3. What is personal information (PI)?

Personal information is defined as any kind of information, electronically or otherwise recorded, related to an identified or identifiable natural person within the People's Republic of China (PRC). PI excludes anonymized information that cannot be used to identify a specific natural person and is not reversible after anonymization. PIPL Art. 4.

Q4. What does the processing (or handling) of PI mean?

Processing (sometimes translated as "handling") includes the collection, storage, use, alteration, transmission, provision, disclosure, deletion, etc. of PI. PIPL Art. 4.

Q5. What is the territorial scope of the PIPL?

The PIPL applies to PI processing activities within the PRC. Similar to the General Data Protection Regulation (GDPR), the PIPL has extra-territorial reach. Any processing of PI outside China will also trigger PIPL's application where one of the following circumstances occurs:

- The purpose of the processing is to provide products or services to natural persons located within the PRC.
- The processing is for analyzing or assessing the behaviors of natural persons located within the PRC.
- Other circumstances provided by laws and regulations.

PIPL Art. 3.

Q6. What processing activity is exempt from the PIPL?

Natural persons' processing of PI for the purposes of personal or family affairs is exempt from the law. PIPL Art. 72.

Q7. Does the PIPL apply to the PI of deceased individuals?

Yes. The next of kin of a deceased individual, for the sake of legal and legitimate interests, may access, copy, correct, or delete the relevant PI of the deceased individual, unless otherwise prescribed by the decedent before death. PIPL Art. 49.

Q8. What is sensitive personal information (SPI)?

The PIPL defines SPI as PI that, if disclosed or illegally used, may cause harm to the security or dignity of natural persons. SPI includes information on biometric characteristics, religious beliefs, specific identity, medical health, financial accounts, individual location tracking, etc. Moreover, any PI of a minor under the age of 14 is regarded as SPI. PIPL Art. 28.

> **Comment:** While PIPL does not define "specific identity," given other regulations and national standards, "specific identity" may include race, ethnic group, sexual orientation, and special social identities like union membership.

Q9. Is SPI treated differently from PI?

Yes. Processing SPI requires a specific purpose, sufficient necessity, and stricter protective measures. Separate consent is also required, and written consent may be needed if provided by other laws and regulations. PIPL Art. 29.

In addition, PI handlers must inform individuals of the necessity of processing SPI and the impact of processing SPI on their rights and interests. PIPL Art. 30.

In the case of a minor, the parent or other guardian's separate consent must be obtained before processing. PIPL Art. 31.

Q10. What rights do individuals (i.e., data subjects) have?

Unless laws or administrative regulations stipulate otherwise, the PIPL grants individuals the right to know about, decide on, limit use of, or object to the use of their PI. PIPL Art. 44. The PIPL also grants individuals the right to access and copy their PI subject to certain exceptions, as well as the right to correct or supplement their PI if incorrect or incomplete. PIPL Art. 45; PIPL Art. 46.

Handlers must proactively delete—or alternatively individuals may request handlers to delete—PI where: (1) the processing is no longer necessary for the stated purpose; (2) the handler is no longer providing a product or service, or the retention period has expired; (3) individuals have revoked consent; (4) the processing would violate specific laws, regulations, or agreements; or (5) other laws or regulations so provide. PIPL Art. 47.

The PIPL also creates a right to data portability, provided any transfer to a new handler satisfies the conditions prescribed by the relevant enforcement authorities. PIPL Art. 45.

Q11. What data protection principles must PI handlers follow?

In their processing of PI, handlers must abide by all of the following principles:

- Lawfulness, fairness, necessity, and good faith. PIPL Art. 5.
- Purpose limitation and data minimization. PIPL Art. 6.
- Openness and transparency. PIPL Art. 7.
- Accuracy and completeness. PIPL Art. 8.
- Security and accountability. PIPL Art. 9.
- Limited data retention. PIPL Art. 19.

Q12. What are the legal bases for processing PI?

PIPL provides several legal bases for processing PI:

- Obtaining individuals' consent.
- Where necessary for the performance of a contract to which the individual concerned is a party, or for the implementation of human resources management.
- Where necessary for the performance of statutory responsibilities or obligations.
- Where necessary for responding to a public health emergency or protecting the life, health, or property of individuals in cases of emergency.
- For purposes of news reporting and other activities in the public interest.
- For purposes of processing PI already disclosed by the individuals themselves or otherwise lawfully disclosed.
- Where otherwise permitted by laws and regulations.

PIPL Art. 13.

Comment: Unlike the GDPR, the PIPL does not include "legitimate interest" as a legal basis for processing PI.

Q13. What constitutes valid consent?

Where consent serves as the legal basis for processing PI, an individual's consent must be given freely, voluntarily, and explicitly on a fully informed basis. If the purposes or means of processing change, or if the categories of PI change, new consent must be obtained from the individual regarding the change. PIPL Art. 14.

Q14. What is separate consent?

The PIPL requires handlers to secure "separate consent" under certain circumstances, without giving a definition or an explanation of what "separate consent" means.

Comment: In practice, separate consent should be independent of the means used to secure initial consent, such as through the use of a pop-up window or a separate and distinct check box.

Q15. Under what circumstances is separate consent required?

Separate consent is required in the following circumstances:

- When transferring PI to another PI handler. PIPL Art. 23.
- When otherwise disclosing PI. PIPL Art. 25.
- When processing PI collected by public surveillance devices for purposes other than public security. PIPL Art. 26.
- When processing SPI. PIPL Art. 29.
- When transferring PI outside the PRC. PIPL Art. 39.

Q16. Are there any specific requirements for advertising?

To the extent PI is used to advertise by means of automated decision-making, the PIPL requires handlers to provide individuals with the option not to target ads based on individuals' characteristics or to provide a method to reject such advertising. PIPL Art. 24.

Comment: Because the PIPL does not include "legitimate interest" as a legal basis for processing, it appears that handlers must rely on consent for any use of PI for advertising purposes.

Q17. What constitutes automated decision-making?

Automated decision-making refers to the use of computer programs to automatically analyze or assess individuals' behaviors, habits, interests, or hobbies, or individuals' financial, health, or credit status, etc. PIPL Art. 73.

Q18. What rules apply to automated decision-making?

Handlers that use PI in automated decision-making must ensure the transparency, fairness, and justice of the automated results. Handlers are prohibited from engaging in unreasonable differential treatment of individuals based on automated decision-making. PIPL Art. 24.

If the use of automated decision-making significantly affects the rights and interests of an individual, the individual can require the handler to explain its use of such decision-making, and can prohibit the handler from making decisions based solely on its use. PIPL Art. 24.

Q19. What is a PI handler?

A "PI handler" refers to organizations and individuals that independently determine the purposes and means of processing PI.

Comment: A PI handler is akin to a "data controller" under the GDPR.

Q20. What are the principal duties of a PI handler?

The PIPL imposes the following obligations on PI handlers.

- Adopt and implement a privacy program that categorizes and manages PI in accordance with laws and regulations, incorporates appropriate security measures, prevents leaks and unauthorized disclosures, educates employees and staff on PI handling practices, and includes an incident response plan. PIPL Art. 51.
- Appoint a data protection officer (DPO) if the handler processes PI that meets a yet-to-be specified threshold established by the relevant enforcement authorities. Handlers must also disclose the DPO's name and contact information to those authorities. PIPL Art. 52.
- Appoint a local representative or entity to be responsible for data protection practices if the handler operates outside the PRC and falls within the extra-territorial reach of the PIPL. The handler must disclose the name and contact information of that representative or entity to the relevant enforcement authorities. PIPL Art. 53.
- Conduct regular compliance audits of data protection practices. PIPL Art. 54.
- Prepare PI protection impact assessments (PIPIAs) when (1) handling SPI; (2) using PI to conduct automated decision-making; (3) disclosing PI to "entrusted parties" (i.e., data processors), other handlers, or third parties; (4) transferring PI abroad; or (5) engaging in any other handling activities that significantly affect individuals. PIPL Art. 55.
- Immediately adopt remedial measures and notify the relevant enforcement authorities as well as affected individuals in the wake of an actual or potential cybersecurity incident (i.e., "leak, distortion, or loss"). Notification of affected individuals is not necessary if the remedial measures effectively mitigate harm to the individuals. PIPL Art. 57.

  Comments: The duty to notify is triggered even in cases of *potential* incidents. How to assess whether an incident "might have occurred" remains unclear at the time of this writing.

  Handlers providing internet platform services have additional obligations outlined in PIPL Art. 58. See Q23.

Q21. What is an entrusted party and what are the main obligations?

An "entrusted party" is akin to a "data processor" under the GDPR. When a PI handler entrusts the processing of PI to another entity pursuant to a contract, the entrusted party must process the PI as agreed, and may not subcontract the processing without the PI handler's consent. An entrusted party does not determine the purposes and means of the processing, and it may not process PI beyond the purposes and means set forth in the contract. PIPL Art. 21.

An entrusted party shall take necessary measures to safeguard the security of the PI it processes and assist the PI handlers in fulfilling their obligations. PIPL Art. 59.

Q22. Are there special requirements for processing the PI of minors?

Yes. Rules concerning minors include:

- PI of a minor under 14 years of age constitutes SPI. PIPL Art. 28.
- As such, a handler processing the PI of those under 14 must prepare a PI protection impact assessment (PIPIA). PIPL Art. 55.
- Handlers processing the PI of minors under 14 must obtain the consent of the parent or guardian. PIPL Art. 31.
- Handlers processing the PI of minors under 14 must adopt "special processing rules." PIPL Art. 31.

  Comment: While PIPL offers no guidance as to what "special processing rules" should address, it may be helpful to refer to the Provisions on the Cyber Protection of Children's Personal Information issued in 2019.

Q23. Are there special requirements for internet giants?

Yes. PI handlers providing "important" internet platform services with a large number of users and complex types of business have extra obligations outlined in PIPL Art. 58, including:

- Establishing a PI protection compliance program overseen by an independent supervisory body comprised mainly of outsiders.
- Formulating platform rules under the principles of openness, fairness, and justice, and clarifying standards for the handling of PI by intra-platform product or service providers.
- Terminating service to any product or service provider that seriously violates the laws and regulations on PI handling.
- Regularly preparing and releasing "social responsibility reports" on PI protection.

Comment: These requirements appear to target Big Tech, but the specific threshold or standard to identify such platforms remains unclear at the time of this writing.

Q24. Does the PIPL include data localization requirements?

Yes. The PIPL provides several scenarios that require PI handlers to store the PI they process within the PRC as follows.

- PI processed by state agencies. PIPL Art. 36.
- PI collected or generated within the PRC by critical information infrastructure operators (CIIOs). PIPL Art. 40.
- PI collected or generated within the PRC by PI handlers who have processed PI reaching a yet-to-be specified threshold established by the relevant enforcement authorities. PIPL Art. 40.

Q25. Can PI be transferred outside China? Are there any conditions?

Yes. In general, a handler may transfer PI outside the PRC, but only after:

- Obtaining separate informed consent from the individuals whose PI is to be transferred (PIPL Art. 39);
- Conducting and documenting a PI protection impact assessment (PIPIA) (PIPL Art. 55); and
- Satisfying one of the following conditions from PIPL Art. 38:

  1. Pass a security assessment to be developed by government cybersecurity authorities.
  2. Obtain a PI protection certification conducted by a specialized body to be identified by government cybersecurity authorities.
  3. Agree, along with the data importer, to the terms of a standard contract to be drafted by government cybersecurity authorities.
  4. Abide by other conditions prescribed in law or regulation or by the government cybersecurity authorities.

Handlers must adopt measures to ensure that overseas recipients adopt a level of PI protection equivalent to the standard set out by the PIPL (PIPL Art. 38).

Comment: Notably, no PI handler may provide PI stored within the PRC to foreign judicial or law enforcement authorities without the approval of competent PRC authorities (PIPL Art. 41).

Q26. Is there a whitelist or blacklist regarding the cross-border transfer of PI?

Not yet, but where overseas organizations or individuals engage in activities that harm the PI rights and interests of Chinese citizens or harm state security or public interests, those organizations may be placed on a blacklist and therefore restricted or prohibited from receiving PI from the PRC. PIPL Art. 42.

Q27. Under what circumstances is a personal information protection impact assessment (PIPIA) required?

PI handlers must conduct and document a PIPIA in advance of any of the following situations:

- Processing SPI.
- Using PI to conduct automated decision-making.
- Disclosing PI to entrusted parties (i.e., data processors), other handlers, or third parties.
- Transferring PI abroad.
- Engaging in any other handling activities that significantly affect individuals' rights. PIPL Art. 55.

PIPIA records must be kept for at least three years. PIPL Art. 56.

Q28. What must be included in a PIPIA?

According to PIPL Art. 56, a PIPIA report must state all of the following:

- Whether the purposes or means of the processing of PI are lawful, legitimate, and necessary.
- The impact on individuals' rights and interests, as well as any security risks.
- Whether the protective measures adopted are legal, effective, and appropriate to the degree of risk.

Q29. Does the PIPL mandate any record-keeping obligations?

Yes. PI handlers must maintain PIPIA reports and "handling status records" for at least three years. PIPL Art. 56.

> **Comment:** While there is no record-keeping obligation regarding PIPL compliance generally, it would be advisable to maintain security assessments and other documentation related to cross-border transfers of PI. Moreover, to the extent a handler relies on consent as the basis for processing PI, it would be advisable to maintain documentation of that consent.

Q30. Who enforces the PIPL?

Certain cybersecurity authorities, as well as the relevant departments under the State Council—for example, the Ministry of Public Security, the State Administration for Market Regulation, the Ministry of Science and Technology—are authorized to enforce the PIPL.

With regard to minor violations, any of the above may impose fines of not more than CNY 1 million (about $157,000), but if the matter is serious, only provincial or higher-level authorities may impose fines of up to CNY 50 million (about $8 million) or 5% of annual revenue. PIPL Art. 66.

Q31. What penalties might be imposed in the case of a violation?

In the case of a minor violation, authorities may impose:

- An order requiring correction, confiscation of illegal gains, or provisional suspension or termination of improper practices.
- A fine of up to CNY 1 million against wrongdoers who refuse to correct their behaviors.
- A fine of between CNY 10,000 and CNY 100,000 against a directly responsible person. PIPL Art. 66.

In the case of a serious violation, provincial or higher-level authorities may impose::

- An order requiring correction, confiscation of illegal gains, suspension or closure of the relevant business, or revocation of the business license.
- A fine of up to CNY 50 million or 5% of the turnover in the previous year.
- A fine of between CNY 100,000 and CNY 1 million against a directly responsible person.

- A prohibition against directly responsible persons from holding senior management positions and roles for a certain period. PIPL Art. 66.

In both cases, such illegal acts will be included in credit records and be publicly disclosed. PIPL Art. 67.

Q32. What remedies are available to individuals (i.e., data subjects) and others for violations of the PIPL?

Any organization or individual has the right to file a complaint with the relevant enforcement authorities about a PI handler's unlawful practices. PIPL Art. 65.

Where PI handlers reject individuals' requests to exercise their rights, individuals may file a lawsuit in court. PIPL Art. 50.

Where illegal processing of PI harms the rights and interests of individuals, the procuratorates, consumer organizations prescribed by the law, and other organizations designated by the relevant enforcement authorities may bring an action before a court. PIPL Art. 70.

Q33. Who bears the burden of proof in a lawsuit?

Where the handling of PI infringes upon individual rights and causes harm, the PIPL appears to require the PI handler to prove it is not at fault. PIPL Art. 69. Damages may be awarded based on the losses suffered by the individual or the gains made by the PI handler. PIPL Art. 69.