PPIL vs. GDPR
A comparison

Effective dates

PIPL: November 1 2021

GDPR: May 25, 2018

The latest data protection regulation (and one with potentially the greatest reach) is China's Personal Information Protection Law.

If you conduct business in China it deserves your attention, as the consequences for failing to comply include high penalties and even government blacklisting and restriction of activities.

Let's compare China's PIPL with the EU's GDPR, looking for key points to keep in mind to help you comply.

bysafeonline.com

Scope

PIPL: Besides regulating organizations' and individuals' handling of personal data belonging to natural persons within the jurisdiction of China, Article 3 of the law extends the territorial scope beyond the borders of China. Data processing activities established outside of China are covered, if one of the following circumstances is present:

- The purpose is to provide products or services to natural persons inside China's border
- Conducting analysis or assessment of activities of natural persons inside the borders
- Other circumstances provided in laws or administrative regulations.

GDPR: Protects persons in the EU (regardless of nationality) and regulates organizations established in the EU, as well as organizations located outside the EU if the organization:

- Offers goods or services to, or monitors the behavior of data subjects located in the EU.
- Has a website that is accessible to anyone living in or visiting the EU.

Key takeaway: If you offer your services to, or your website is accessible to Chinese citizens/anyone living in or visiting the EU, you should be prepared to comply with their respective regulations.

Tip: Use DataMapper to find and track all sensitive data about your customers, or search a specific name or list of names (e.g., lists from a region/country).

Fines

PIPL: Up to 5% of a company's annual revenue of the previous year or CNY 50 million (about €6.7 million).

GDPR: Up to €20 million or 4 percent of worldwide turnover for the preceding financial year, whichever is higher.

Did you know? PIPL's upper limit for fines is for "grave" violations (an undefined term). Chinese authorities may also: suspend offending business activities, stop business activities, cancel administrative and business licenses, or place offending organizations on a blacklist that restricts them from collecting personal data.

Types of personal data protected

PIPL: All kinds of information recorded by electronic or other means, related to identified or identifiable natural persons.

GDPR: Any information related to an identified or identifiable natural person.

Both regulations: Have a broad definition of personal data but exclude anonymized data. Chinese and European authorities will likely take a broad approach when interpreting what constitutes personal information in practice.

Sensitive data defined

PIPL: Personal information that, once disclosed or illegally used, may easily cause grave harm to the dignity, personal, or property security of natural persons, including information on biometric characteristics, religious beliefs, specially designated status, medical health, financial accounts, individual location tracking, etc., as well as the personal information of minors under the age of 14.

GDPR: Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.

Key point of difference: PIPL has an open list that describes sensitive data that "may easily cause grave harm", while the GDPR has a closed list that focuses on specific categories, allowing the PIPL to consider some data as sensitive that the GDPR may not.

Where do you store sensitive data?

DataMapper quickly identifies high-risk data. It uses advanced AI and machine learning algorithms find and track all the data your team stores whether it is saved on users' desktops, buried in email folders, or stored in the company cloud. Sensitive data is automatically sorted by risk level and you can monitor it from one dashboard.

Consent requirements and legal basis

PIPL: The most common legal basis is consent, which must be informed, voluntary and explicit. (Art. 13 lists other legal bases).

GDPR: Consent must be freely given, specific, informed, an unambiguous indication of the data subject's wishes. (Art. 6 lists other legal bases).

Point of difference: The PIPL does not recognize "legitimate interests pursued by the controller" as a legal basis for personal information processing. This and other aspects of the PIPL put extra emphasis on always obtaining consent.

Privacy notice requirements

PIPL: Businesses must provide consumers with a comprehensive description of their online and offline practices regarding collection, use, disclosure, and sale of personal information and data rights.

GDPR: Organizations are required to provide a variety of information to data subjects prior to the processing of their personal data, whether or not personal data is collected directly from data subjects.

All privacy notices must be:

- Concise
- Easily accessible
- Easy-to-understand
- In clear and plain language

Tip: Track your data processing procedures, then outline them in a simple privacy policy that lets your customers know they can trust you.

Processing principles

PIPL: Legality, Appropriateness, Necessity and Good Faith, Clear and Reasonable Purpose, Openness and Transparency, Quality Assurance (including accuracy and security)

GDPR: Lawfulness and Necessity, Purpose Limitation, Collection Limitation, Openness and Transparency, Accuracy, Accountability and Security

DataMapper maps all the sensitive data you store. Make sure you have a purpose for keeping it. Keep only what you need, and make sure only the right people have access to it.

Local representative

PIPL: Offshore organizations that process data belonging to Chinese citizens must establish a dedicated office or appoint a representative inChina to be responsible for personal information protection in China.

GDPR: An EU representative is required

Sensitive information processing

PIPL:Only collect information necessary to achieve the specified purpose, adopt strict protective measures, and obtain a separate, specific consent when processing sensitive information. You must also inform individuals of the necessity and impact on individuals' rights and interests of processing of their sensitive personal information.

GDPR: Only process sensitive personal data with the data subject's explicit consent (some exceptions).

Key takeaway: The PIPL takes a risk-based approach, imposing heightened compliance obligations in specified high-risk scenarios, for example, internet platforms with large numbers of users, large volumes of data, and sensitive data.

Tip: Use DataMapper to categorize the data you store by risk level, see who has access to them; evalute and improve your data storage practices.

Data subject rights fulfillment

PIPL: Specifically requires that organizations establish a mechanism for receiving and processing individuals' rights requests. No specific timeline or extension period requirements. If an individual's request for the exercise of their rights is rejected, the reasons shall also be explained. Individuals may in turn file a lawsuit with a People's Court according to the law to challenge the rejection of their DSR requests.

GDPR: Data controllers should respond to data subjects' rights requests 'without undue delay' and usually within one month of the receipt of the request. The response time may be extended to two further months in case of complex requests.

Key point of difference: PIPL has not set a timeline for request response, while there is a 30-day deadline for GDPR requests.

Tip: DataMapper lets you access all of the data your team stores from one dashboard, so it's easy to find someone's data when requested to.

Right to know and decide

PIPL: Individuals have 'the right to know and the right to decide' when it comes to their personal information; and request handlers explain their handling rules.

GDPR: The right to be informed requires the controllers to provide certain information to the data subject when personal data is collected. Any relevant information in connection to the data processing must be given in a concise, transparent, intelligible, and easily accessible form, using clear and plain language to the data subject.

Point of difference: The PIPL includes an additional requirement for personal information handlers to notify individuals of the name/personal name and contact method of the receiving party when sharing their data with third-parties. The GDPR only requires the data controller to notify data subjects of the type of third-party recipient.

DataMapper keeps track of the data you have across all departments and who can access it.

Right to access

PIPL: Individuals have the right to access and copy their personal information from the data controllers. A few exceptions:

- Where state organs process personal information for the purpose of fulfilling statutory duties and responsibilities.
- Where laws or administrative regulations provide that confidentiality of personal information shall be preserved

GDPR: Under the GDPR, the right of access includes the right to obtain confirmation from the controller as to whether or not personal data is being processed and access to the personal data.

Did you know? A unique characteristic of the PIPL is that all data rights extend beyond an individual's death and can be exercised by close relatives of the decedent, unless otherwise arranged by that person during their lifetime.

With DataMapper, the sensitive data you store is already easy to find, structured, and ready to share (accessible).

Right to deletion

PIPL: Individuals can ask a data controller to delete their personal information if:

- The agreed retention period has expired
- The handling purpose has been achieved
- Data handlers cease the provision of services
- The individual rescinds consent
- The information is handled in violation of laws, regulations or agreements

GDPR: The right to deletion of personal data applies in the following instances:

- When the personal data is no longer necessary for the purposes it was collected.
- When consent is withdrawn by the data subject.
- When the data subject objects to data processing based on legitimate interest.
- When the data subject objects to data being processed for direct marketing purpose.
- When the personal data is unlawfully processed.
- When personal data has to be erased for compliance with a legal obligation.
- When a child wants to erase data in case of the provision of information society services to a child.

Tip: DataMapper makes it easy to find and delete sensitive data. Tidy up regularly, keeping only the data you need.

Right to data portability

PIPL: When individuals request that their personal information be transferred to a personal information handler they designate, if such request meets conditions set up by State cyberspace administrations, personal information handlers shall provide a channel to transfer it.

GDPR: The data controller should send data requested in a structured, commonly used, and machine-readable format and to transmit the data to another controller without any hindrance, when it is technically feasible to do so. The GDPR limits the exercise of the right to data portability where it adversely affects the rights and freedoms of others.

Key takeaway: GDPR provides more specifics regarding how companies are expected to respond to data portability requests, while the PIPL only says it is 'subject to the conditions set by the State cyberspace administrations'. It's likely those administrations will release further regulations to better implement the rule.

Tip: The data you store should already be easy to find, tidy, and ready to send (portable). You can export/download files in a machine-readable format directly from your DataMapper dashboard.

Right to refuse/limit/object

PIPL: People have the right to refuse and limit the handling of their data.

GDPR: The GDPR provides data subjects with the right to object and withdraw consent to personal data processing for a variety of reasons.

Right to withdraw consent

PIPL: Individuals have the right to withdraw consent.

GDPR: None, however, the right to object could be used in this way.

Note: The PIPL states that withdrawal of an individual's consent does not affect the effectiveness of the personal information processing activities that have been carried out based on the individual's consent before the withdrawal.

Right to object to automated decision making

PIPL: An individual can require the personal information controller to give an explanation, and to reject the decision made by the personal information controller only through automated decision making.

GDPR: Data subjects have the right not to be subject to a decision based solely on automated processing, including profiling, that produces legal effects or similarly significantly affects them.

Right to correct and amend

PIPL: Individuals have the right to request their information be corrected or complered in a timely manner.

GDPR: Data subjects have the right to request rectification of inaccurate personal data and to have incomplete personal data completed.

Tip: DataMapper makes it easy to find someone's data and check it for errors, keeping all the data you store up-to-date and accurate.

Security Measures

PIPL: The data controller must have an internal management structure and operating rules, processing limits framework, and technical security measures such as encryption & de-identification.

Data controllers should also have a mechanism for the categorized management of personal information.

Data controllers should conduct audits of their processing activities and compliance with other laws; conduct security education and training of its employees; and implement additional safeguards for sensitive personal information and processing.

GDPR: Requires organizations to adopt appropriate technical and organizational measures to ensure personal information processing security. These measures may include the following:

- Encryption and pseudonymization of personal data
- Ensuring integrity, confidentiality, and availability of processing system
- Restoring the availability and access to personal data promptly
- Assessing and evaluating the effectiveness of technical and organizational measures.

Showcase your commitment to consumer privacy by using advanced security and compliance software and mentioning it in policies and contracts.

In case of data breach

PIPL: You must take immediate action and notify the relevant agency and affected individuals. When the measures taken can effectively avoid damages to personal information, you do not have to notify individuals

GDPR: You must notify supervisory authorities of any personal data breach that is likely to result in a risk to natural persons' rights and freedoms without undue delay and not later than 72 hours after becoming aware of the breach.

Point of difference: The PIPL does not set out an exact deadline for notifying supervisory authorities of data breaches, while the GDPR allows 72 hours.

Prevent breaches

DataMapper quickly **identifies high-risk data** in your team's systems **(that you may not know existed)** and classifies it by risk level.

Data protection officer (DPO)

PIPL: You must appoint Personal Information Protection Officers in some cases, depending on the volume of personal information they process. China's state cybersecurity and informatization department will provide clarity on the volume threshold. Data controllers are also required to disclose the methods of contacting Personal Information Protection Officers and report the names of the officers and contact methods to the departments fulfilling personal information protection duties and responsibilities

GDPR: You must appoint a data protection officer when data processing activities are carried out by a public authority (except for courts in their judicial capacity), where the core activities of the organization consist of regular and systematic monitoring on a large scale, or where the core activities of the organization consist of the sensitive personal data or personal data relating to criminal convictions and offenses. Organizations must publish the contact details of the DPO and communicate them to the supervisory authority.

Help for DPOs

Since the role of DPO already requires technical, legal, and business skills, the **data management/compliance software** you choose should be **easy-to-use, with high security and the ability to coordinate and monitor data processing** across the entire company.

Cross-border data transfer

PIPL: Transferring personal information outside the territory of China should meet three necessary conditions: (1) obtaining the personal information subject's separate and informed consent; (2) conducting personal information protection impact assessment and making record; and (3) adopting one of the measures set forth in the PIPL to ensure that adequate safeguards would be provided for the transfer.

The PIPL also imposes an obligation on personal information exporters to ensure data protection standards are met after transfer. The PIPL stipulates that without the approval of the Chinese regulatory authority, personal information stored in China shall not be provided to judicial or law enforcement agencies outside China. This provision is in line with the newly enacted Data Security Law of China.

GDPR: Data controllers must inform the data subject of their intention regarding the transfer of data to a third country at the time personal data is collected from the data subject including information on the existence of an adequacy decision by the Commission, or in case of transfers based on appropriate safeguards, the means by which to obtain a copy of them.

Personal data transfers to a third country or international organization may take place only where an adequate level of protection is ensured (adequacy to be determined by the EU Commission) or there are safeguards in place to ensure the level of protection is essentially equivalent to that currently guaranteed inside the EU.

Point of difference: Unlike the GDPR, the PIPL has not adopted an adequacy decision mechanism, and the transfer of personal information must meet requirements regardless of the location of the recipient of the personal information.

Third-party processors

PIPL: If data controllers engage entrusted parties for the processing of personal information, they are required to conclude an agreement with the entrusted parties on the purpose for entrusted handling, the time limit, the handling method, categories of personal information, protection measures, as well as the rights and duties of both sides, etc., and conduct supervision of the personal information handling activities of the entrusted person.

Entrusted parties are required to handle personal information according to the agreement, and are required to take necessary measures to safeguard the security of the personal information they handle and assist data controllers in fulfilling the obligations provided in the PIPL.

GDPR: Data controllers are allowed to engage with only those processors that provide sufficient guarantees to implement appropriate technical and organizational measures and protect data subjects' rights as per the requirements of the GDPR. Data processors are required to process the personal data only on documented instructions from the controllers.

Note: The PIPL states that data controllers who 'jointly process personal information' will bear joint and several liability in case of mishandling.

Internet platform services

PIPL: Data controllers that provide internet platform services to a large number of users and have complex business models must:

- Establish and complete personal information protection compliance structures
- Establish an independent body to supervise personal information handling
- Follow the principles of openness, fairness, and justice
- Immediately cease their service offerings when in serious violation of the law
- Regularly publish reports on the social responsibility of personal information handling.

GDPR: Internet platforms are not addressed separately.

Point of difference: PIPL has stricter requirements for organizations that provide internet platform services, while the GDPR does not separately define or provide obligations for internet platform service providers.

Risk assesment (DPIA)

PIPL: Organizations should conduct risk assessments and record them before conducting specific personal information processing activities that have a significant impact on individuals, such as processing sensitive PI, automatic decision-making, entrusting processors, providing PI to third parties and so on.

GDPR: A Data Protection Impact Assessment (DPIA) is required under the GDPR any time you begin a new project that is likely to involve "a high risk" to other people's personal information.

Did you know? One of the most important ways to demonstrate to authorities that your organization complies with the PIPL and the GDPR is to prepare a DPIA for each of your high-risk data processing activities.

Even when the high-risk standard is not met, it is still prudent to conduct a DPIA to minimize liability and ensure best practices for data security and privacy are being followed in your organization.

A risk assesment (or DPIA) should:

- Describe your data processing activities (GDPR)
- Explain the purpose of data handling and why it is lawful, legitimate and necessary (PIPL and GDPR)
- Assess the necessity and proportionality of processing in relation to the purpose (GDPR)
- Explain possible impact on people's interests, rights and freedoms, along with security risks (PIPL and GDPR)
- Show the measures that will be taken are legal effective and suitable to the degree of risk (PIPL and GDPR)

Records and documentation of data processing and requests

PIPL: No explicit requirement for having a record of data processing activities. Instead, PIPL imposes obligations on data controllers to regularly engage in audits of their personal information activities and compliance with laws and administrative regulations. It also requires personal information protection impact assessment reports and handling status records be preserved for at least three years.

GDPR: Data controllers are required to maintain a record of processing activities. This obligation does not apply to organizations with fewer than 250 persons unless the processing is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes special categories of data or personal data relating to criminal convictions and offenses. For the purposes of demonstrating compliance, data controllers are also required to document personal data breaches and consent statements where data processing is based on data subjects' consent.

Documentation with our software

DataMapper helps you track (and improve) your data storage procedures

Connectid Business documents every step in the data request process

Connectid Mail logs consents before sharing personal data safely w/email

For more information visit: bysafeonline.com