# China's Personal Information Protection Law (PIPL) vs. Brazil's General Data Protection Law (LGPD)

On August 20, China's Personal Information Protection Law (PIPL) was approved and will come into effect in November 2021.

The PIPL explicitly defines personal information (PI) and regulates personal data processing, transfers and storage, with impacts for companies that process PI for business activities in China. Foreign companies operating in China will need to review their privacy framework to comply with the new law's requirements and transfer data to other jurisdictions.

The table below compares significant similarities and differences between the PIPL and Brazil's equivalent law, the LGPD.

## Applicability

The PIPL applies to activities that involve handling the personal information of natural persons within the People's Republic of China's (China) borders.

For activities concerning the personal information of natural persons within the borders of the People's Republic of China that occur outside China's borders, the PIPL also applies in any of the following circumstances:

1. When the purpose is to provide products or services to natural persons inside the borders;
2. When analyzing or assessing the activities of natural persons inside China's borders;
3. Other circumstances provided for in other laws or administrative regulations.

The LGPD applies to any processing operation carried out by a natural person or legal entity governed by public or private law, irrespective of the way the data is processed, the country the processor is based in or of the country where the data is located, provided:

1. the processing operation is carried out in Brazil;
2. the processing activity offers goods or services to individuals located in Brazil;
3. the processing activity involves the data of individuals located in Brazil; or
4. the processed personal data has been collected inside Brazil.

## Definitions

**Personal information**
any information related to identified or identifiable natural persons (except for already anonymized information) recorded electronically or otherwise. Personal information handling regards its collection, storage, use, processing, transmission, provision, disclosure or deletion.

**Personal data**
information related to an identifiable natural person. Processing (Personal information handling) includes any operation carried out involving personal data, such as data collection, production, receipt, classification, use, access, reproduction, transmission, distribution, processing, filing, storage, elimination, information evaluation or control, modification, communication, transfer, diffusion or extraction.

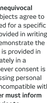
**Personal information handler**
refers to organizations and individuals that autonomously decide the purposes and methods of information processing in respect to personal information processing activities.

**Controller** (Personal information handler): a natural person or legal entity, governed by public or private law, responsible for making decisions about processing personal data.

## Legal Principles

Personal information handlers must observe the principles of **legality, propriety, necessity**, and **sincerity** when handling personal information. It is prohibited to handle personal information in misleading, fraudulent, coercive or other such ways.

Personal data processing must be carried out in good faith and observe other principles as **valid purpose, adequacy, necessity, free access, transparency, security**. If the information provided to data subjects is misleading, contains abusive content, or has not been previously presented in a transparent, clear and unequivocal manner, any prior consent shall be deemed null and void.



## Legal Basis

The PIPL sets out **seven legal bases** to justify data processing:

I. Consent;

II. Concluding or fulfilling a contract in which the individual is an interested party, or where necessary to conduct human resource management in line with legally adopted labor regulations and systems, and legally concluded collective contracts;

III. Fulfilling statutory duties, responsibilities or obligations;

IV. Responding, when necessary, to sudden public health incidents, or protecting natural persons' health and the security of their property under emergency conditions;

V. Within reason, handling personal information for news reporting, supervision of public opinion, and other such activities in the public interest;

VI. Handling personal information disclosed by the persons themselves or that has otherwise been already lawfully disclosed, within reason and in accordance with the provisions of the Law; and

VII. Other circumstances provided in laws and administrative regulations.

The LGPD sets out **ten legal bases** to justify data processing:

I. Consent;

II. The controller's need to comply with statutory or regulatory obligations;

III. The public administration's processing and shared use of data that is required for carrying out public policies set forth in laws or regulations or supported by contracts, agreements or similar instruments;

IV. For studies by research bodies, which must guarantee that data is anonymized whenever possible;

V. Performing agreements or preliminary procedures related to agreements that involve the data subjects, at their request;

VI. Exercising rights in lawsuits, administrative or arbitration proceedings;

VII. Protecting the data subject or third parties' lives or physical safety;

VIII. Protecting data subjects' health during procedures carried out by health professionals or sanitary entities;

IX. For the legitimate interests of the controller or of third parties, except where data subjects' fundamental personal data protection rights and liberties prevail;

X. Protecting credit.

## Consent

When personal information is handled based on individual consent, individuals must give this consent **in an explicitly free and informed manner**. If laws or administrative regulations provide that separate or written consent is required for handling personal information, these provisions must be followed. If the purpose or method of personal information handling changes or the categories of handled personal information are modified, **the individual must consent once again**.

Consent is a **free, informed and unequivocal** pronouncement by which data subjects agree to have their personal data processed for a specific purpose. The consent must be provided in writing or other means that manifestly demonstrate the data subject's will. When consent is provided in writing, it must be included separately in a specific contractual clause. Whenever consent is required, if the purpose for processing personal data is modified in a way that is incompatible with the original consent, **the controller must inform data subjects of these changes prior to processing. Data subjects may revoke their consent if they disagree with the changes**.

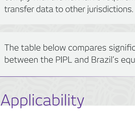
## Transparency

Prior to handling personal information, personal information handlers must explicitly notify individuals, truthfully and accurately, of the following items in clear and easy-to-understand language:

1. the personal information handler's name/personal name and contact details;
2. the purpose and method of personal information handling, as well as the categories and the retention period of the handled personal information;
3. methods and procedures for individuals to exercise their rights, as provided for in the PIPL;
4. relevant items provided for by other laws or administrative regulations.

Data subjects are entitled to have easy access to information about how their data is processed. Together with other characteristics set forth in the regulations that regard the principle of free access, data processing information must be clearly, adequately and visibly provided, covering the following items:

1. specific purpose for processing;
2. the duration and form of processing, with due regard for trade and industrial secrets;
3. the controller's identity and contact information;
4. information concerning the controller's shared use of data and its purpose;
5. the responsibilities of agents who will carry out the data processing;
6. the data subject's rights, explicitly mentioning the rights contained in Article 18 of the LGPD.



## Retention Periods

Except where laws or administrative regulations provide otherwise, handlers must apply the shortest possible personal information retention periods necessary for meeting the purpose of personal information handling.

Personal data processing must be terminated when its purpose has been achieved, or the data is no longer necessary or pertinent for achieving the specific purpose.



## Sensitive Personal Information

**Sensitive personal information** regards information that may easily cause harm to the dignity of natural persons, their personal security or the security of their property if leaked or illegally used. This includes information on biometric characteristics, religious beliefs, specially designated status, medical health, financial accounts and individual location tracking, as well as the personal information of minors under the age of 14. The individual's separate consent must be obtained in order to handle sensitive personal information. If laws or administrative regulations provide that written consent is required for handling personal information, these provisions must be followed.

**Sensitive personal data**: natural persons' personal data regarding racial or ethnic origins, religious beliefs, public opinions, affiliations with labor unions or religious, philosophical or political organizations, health or sex life data, genetic or biometric data;

Sensitive personal data can only be processed in the following situations:

1. Whenever data subjects or their legal representatives specifically and explicitly consent to the processing for specific purpos
2. Whenever data is essential for exercising rights, including for agreements and lawsuits, administrative or arbitration proceedings, the controller's compliance with statutory or regulatory obligations. In such cases, the data subject's consent is not required.

# DPOs (Data Protection Officers)

### Personal information

Handlers of quantities of personal information exceeding thresholds determined by China's Central Cybersecurity Affairs Commission must appoint personal information protection officers, who are responsible for supervising personal information handling activities and adopted protection measures.

Personal information handlers must publicly disclose the contact details of their personal information protection officers. They must also report this information to government departments in charge of personal information protection duties and responsibilities.

Personal information handlers outside the borders of the People's Republic of China must establish a dedicated entity or appoint a representative within the borders of the People's Republic of China to be responsible for the personal information they handle. The name of the relevant entity (or personal name of the representative) must be reported together with other contact details to government departments in charge of personal information protection duties and responsibilities.

### Personal data

Data protection officer: a natural person appointed by the controller who acts as a point of contact between the controller, data subjects and the supervisory authority. Data controllers must appoint a data protection officer.

The data protection officer's identity and contact details must be clearly and objectively disclosed to the public, preferably on the controllers' website.

Data protection officers are responsible for the following activities:

1. Accepting complaints and communications from data subjects, providing clarification and taking necessary measures;
2. Receiving communications from the supervisory authority and taking necessary measures;
3. Instructing the controller's employees and third-party contractors on adopted personal data protection practices;
4. Carrying out any other duties established by the controller or in line with supplementary regulations.

# Children's Personal Data

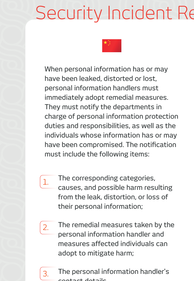
When handling the personal information of minors **under the age of 14**, personal information handlers must obtain consent from a parent or guardian.

Personal data processing concerning minors **under the age of 12** must be carried out with the express and separate consent of at least one parent or legal guardian.

# International Data Transfers

Where personal information handlers truly need to move personal information outside China's borders for business or due to other requirements, they must meet at least one of the following conditions:

1. Pass a security assessment organized by the Central Cybersecurity Affairs Commission, as per Article 40 of the PIPL;
2. Attain personal information protection certification from a specialized body according to provisions set by the Central Cybersecurity Affairs Commission;
3. Enter into a contract with the foreign entity receiving the personal information in line with a standard contract formulated by the Central Cybersecurity Affairs Commission, which defines the rights and responsibilities of both parties;
4. Other conditions provided for in other laws or administrative regulations or by the Central Cybersecurity Affairs Commission



Transferring personal data across international jurisdictions is permitted solely in the following cases:

1. Data is transferred to countries or international organizations that provide an adequate level of personal data protection as provided for by the LGPD;
2. The controller provides and demonstrates guarantees to comply with the principles, data subject rights and data protection framework established in the LGPD, in the form of:
   a. specific contractual sections for a given data transfer;
   b. standard contractual sections;
   c. global corporate rules;
   d. regularly issued seals, certificates and codes of conduct;
3. The data transfer is required for international legal cooperation between government intelligence, investigation and police bodies, in accordance with international law;
4. The data transfer is required for protecting the life or physical integrity of the data subject or any third party;
5. The supervisory authority authorizes such a data transfer;
6. The data transfer results in a commitment undertaken under an international cooperation agreement;
7. The data transfer is required for enforcing a public policy or attributing legal responsibility for a public utility, upon disclosing the provisions established in Article 23, item I of the LGPD;
8. The data subject has provided specific consent for such a transfer after having been informed of the international nature of the operation, clearly distinguishing it from any other purposes; or
9. When required to meet the hypotheses established in Article 7, items II, V and VI of the LGPD.

# Data Subject Rights

Individuals have the right to consult, copy, correct and delete their personal information. They also have the right to limit or reject others' handling of their personal information and to refuse requests for personal information handlers to make decisions solely through automated decision-making methods.

Personal information handlers must establish convenient mechanisms to accept and process applications from individuals exercising these rights.

At any time and upon request, data subjects are entitled to oblige the controller to:

1. confirm that their data has been processed;
2. provide access to their data;
3. correct incomplete, inaccurate or outdated data;
4. anonymize their data or block or eliminate unnecessary or excessive data processing;
5. pass on their data to other service providers or product suppliers;
6. eliminate the personal data processed with the data subject's consent;
7. inform which public and private entities the controller shared data with;
8. inform the data subject about the possible consequences of not providing, denying or revoking consent;
9. have a natural person review decisions made via automatized personal data processing that affects their interests.

Data subjects or their legally appointed representatives may exercise these rights by submitting an express request to the relevant processing agent.

# Security Incident Reporting

When personal information has or may have been leaked, distorted or lost, personal information handlers must immediately adopt remedial measures. They must notify the departments in charge of personal information protection duties and responsibilities, as well as the individuals whose information has or may have been compromised. The notification must include the following items:

1. The corresponding categories, causes, and possible harm resulting from the leak, distortion, or loss of their personal information;
2. The remedial measures taken by the personal information handler and measures affected individuals can adopt to mitigate harm;
3. The personal information handler's contact details.

Controllers must notify the supervisory authority and data subjects of any security incident that may result in relevant risks or harm to the data subjects. This notice must be delivered within a reasonable timeframe – as defined by the supervisory authority – and contain, at the very least:

1. A description of the nature of the affected personal data;
2. Information on the data subjects involved;
3. An indication of the technical and security measures used for data protection, with due regard for trade and industrial secrets;
4. The risks related to the incident;
5. If notice is not given immediately, the reasons for the delay;
6. The measures that have been or will be adopted to reverse or mitigate the negative effects of the security incident.

To determine the severity of an incident, an assessment will be carried out regarding the technical measures adopted for making the affected personal data unintelligible to unauthorized third parties. The assessment will take the scope and the technical limitations of the controller's services into account.

# Liability

Where personal information is illegally mishandled, the departments in charge of personal information protection duties and responsibilities have the power to **order information processes to be corrected, confiscate illegal income, and provisionally suspend or terminate related services**. Personal information handlers who refuse to comply face a fine of up to RMB 1 million, while individuals who are determined to be directly responsible face a fine of between RMB 10,000 and RMB 100,000.



Data processing agents responsible for infractions in regard to the LGPD are subject to the following administrative penalties from the supervisory authority:

1. A warning with an indication of a deadline to adopt corrective measures;
2. For private law legal entities, groups or conglomerates, a one-time fine of up to two percent (2%) of before-tax sales revenue in the previous fiscal year. The fine is limited to BRL 50 million per infraction;
3. A daily fine, with due regard for the total limit referred to in item 2;
4. Disclosure of the infraction, upon being duly investigated and confirmed;
5. The personal data corresponding to the infraction is blocked until confirmation that it has been regularized;
6. Elimination of the personal data corresponding to the infraction;
7. Partial or total suspension of the operation of the database corresponding to the infraction;
8. Suspension of the personal data processing activity corresponding to the infraction;
9. Partial or total prohibition of any data processing-related activities.