PIPL

Who is it for?

✓ All public/private organizations/platforms

✓ Protects Chinese citizens (+their data)

Data collection/legal basis

✓ Informed, voluntary and explicit consent (more in Art. 13)

✗ Does not recognize “Legitimate interests pursued by the controller” as legal basis.

✓ Easy-to-read, detailed Privacy Policy required

✓ Excludes anonymized/pseudonymized data

✓ Open list of sensitive data

✓ Strict roles for third-party processing

Cross-border data transfer

✓ Separate and informed consent required

✓ Data protection impact assesment required

✓ Adopt adequate safeguards

✓ The exporter must ensure data protection standards are met after transfer

Consumer rights:

✓ Right to know and decide

✓ Right to access

✓ Right to data portability

✓ Right to withdraw consent

✓ Right to correct and amend

✓ Right to deletion/ blocking/ restriction

✗ Right to object (not explicitly mentioned)

✗ Right to object to automated decision making (But, you must provide the option to not target a person’s characteristics OR provide the person with a convenient method to refuse to the automated decision-making processing.)

Privacy request fulfillment

✓ Timely response (deadline unspecified)

✓ Data privacy rights may be exercised by close relatives after an individual’s death

More compliance requirements

✓ DPO required

✓ Dedicated office or representative in China

✓ Regularly engage in audits of your data processes

✓ Data protection impact assessment (DPIA)

Fines

✓ Max 50 mio CNY/5 percent annual revenue

Security and Liability

✓ Internal management structure, operating rules, processing limits framework and technical security measures such as encryption & de-identification required. Data controllers must also have a mechanism for categorized management of personal information, w/additional safeguards for sensitive personal information.

✓ Stricter obligations for certain ‘high-risk’ scenarios, including internet platforms with large numbers of users, large volumes of data and sensitive data.

✓ Take immediate action and notify the relevant agency and affected individuals.

✓ If you offer goods or services to Chinese citizens or your website is accessible to them, you must comply with the PIPL when collecting their data.

Our compliance software:

DataMapper finds and tracks your company’s sensitive data across employees, cloud storage, systems and apps. Sensitive data is sorted by risk level, and you can see where it is and who has access to it, making it easy to evaluate and monitor your data storage practices.

Connectid Business automates the data privacy request process by receiving and verifying requests, quick data collection, encryption for data you send, notifications and documentation of every step in the data request process.

Connectid Mail lets you share sensitive data with anyone in the world safely, with no certificates required, from the email you already use. It also gets and logs consent before accepting any personal data you request from others.

bysafeonline.com

GDPR

Who is it for?

✓ All public/private organizations/platforms

✓ Protects anyone in the EU (+their data)

Data collection/legal basis

✓ Freely given, specific, informed, and unambiguous consent (more in Art. 6)

✓ “Legitimate interests pursued by the controller can as legal basis for data collection.

✓ Easy-to-read, detailed Privacy Policy required

✓ Excludes anonymized/pseudonymized data

✓ Closed list of sensitive data categories

✓ Strict roles for third-party processing

Cross-border data transfer

✓ Inform the data subject

✓ Ensure adequate protection levels will be met by the third country/international organization (adequacy determined by the EU Comission) or provide safeguards equivalent to the EU’s to ensure data subject rights

Data subject rights:

✓ Right to be informed

✓ Right to access

✓ Right to data portability

✓ Right to withdraw consent

✓ Right to rectification

✓ Right to deletion/ blocking/ restriction

✓ Right to object

✓ Right to object to automated decision making

Privacy request fulfillment

✓ Respond to privacy requests within 30 days

✗ No inherited data rights mentioned

More compliance requirements

✓ DPO required

✓ EU representative required

✓ Record your data processing activities

✓ Data protection impact assessment (DPIA)

Fines

✓ Max fine €20 mio/4 percent annual revenue

Security and Liability

✓ Technical and organizational measures that may include:

- Encryption and pseudonymization of 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.

✓ Specific requirements for record-keeping

✓ Notify supervisory authorities not later than 72 hours after becoming aware of the breach.

✓ If you offer goods or services to individuals within the EU or your website is accessible to them, you must comply with the GDPR when collecting their data.

Our compliance software:

DataMapper finds and tracks your company’s sensitive data across employees, cloud storage, systems and apps. Sensitive data is sorted by risk level, and you can see where it is and who has access to it, making it easy to evaluate and monitor your data storage practices.

Connectid Business automates the data privacy request process by receiving and verifying requests, quick data collection, encryption for data you send, notifications and documentation of every step in the data request process.

Connectid Mail lets you share sensitive data with anyone in the world safely, with no certificates required, from the email you already use. It also gets and logs consent before accepting any personal data you request from others.

bysafeonline.com