Data. Protection. Adding Value.

Data Protection Laws - China

Legislation

Various laws and regulations govern data privacy in China and the key law is the Personal Information Protection Law ("PIPL") which came into effect on November 1, 2021. Meanwhile, the Provisions on Facilitating and Regulating Cross-border Data Flow effective on March 22, 2024 is a refinement and supplement to the PIPL in connection with cross-border data transfer. The legal requirements which were in effect before then are largely still effective and enforceable.
Scope: PIPL applies to the processing of personal information of natural persons in China, as well as the processing outside of China of personal information of natural persons in China in the following circumstances: (1) Having the purpose of providing products or services to the natural persons, (2) analyzing or evaluating the behaviour of the natural persons, or (3) Other circumstances which the law may prescribe.
Exemptions: PIPL does not apply to the processing of personal information conducted by a natural person for personal or family affairs. Where other law prescribes in respect of personal information processing during statistical or archival management activities organized by the government, such law is instead applicable.

Risk Level: High

Supervisory Authority

Supervisory Authority: The key regulator is the Cyberspace Administration of China with its local branches and there are various other regulators (with their local branches) such as the Ministry of Industry and Information Technology, Ministry of Public Security, State Administration for Market Regulation, which have jurisdiction over data privacy.
Registration/Approval Requirements: Yes, in respect of breach reporting and certain cross-border transfers.

General Data Privacy Principles

When processing the personal data of Data Subjects under PIPL the following principles must be adhered to guarantee its legality:

- Accountability
- Collection/Use Limitation
- Data Minimisation
- Data Quality/Accuracy
- Purpose Specification
- Storage Limitation
- Integrity and confidentiality/Security Safeguards
- Openness Principle
- Privacy by Default
- Privacy by Design

Enforcement

Enforcement (Fines, Criminal Penalties): Penalties for non-compliance are hefty, including remediation orders, confiscating of income, a fine of up to CNY 50 million or 5% of the income in the previous year, suspension of business operations, and revocation of business licenses.

Remedies for Individuals: The directly responsible person may be fined up to CNY 1 million and may be prohibited from holding important positions for a certain time period.

Criminal penalties are also possible. Where the processing of personal information infringes upon personal rights and interests and causes damage and the data controller cannot prove that it is not at fault, it shall assume liability, among other things.

Data Processing

Legal Basis for Processing: Consent should be obtained for personal information processing excepting for contract performance to which the individual is a party, implementation of human resource management in accordance with labour rules and regulations as well as collective contract signed according to China law, performance of statutory duties, response to public health emergencies or protection of the life, health, or property of natural persons during emergencies, news reporting, processing of publicly disclosed personal information, or other circumstances which the law may prescribe.
Sensitive Personal Data: Proper, unbundled informed consent ("Separate Consent") should be obtained for sensitive personal data processing.
Other Restrictions on Processing: To process the personal information of minors under the age of 14, the data controller must obtain the consent of the minor's parents or other guardians. In processing the personal information of minors under the age of 14, the data controller must formulate special processing rules.

Transparency Requirements

Before collecting or otherwise handling personal information, data controllers must truthfully, accurately, and fully inform individuals of the following matters in a conspicuous and lucid manner:
(1) The name and contact information of the data controller.
(2) Processing purposes and methods, as well as types of personal information processed and retention period.
(3) Methods and procedures for individuals to exercise their rights.
(4) Other matters as required by law (e.g. there is additional information which must be informed to the individual if sensitive personal data are to be collected from the individual).
Individuals have the right to request the data controller to explain the rules on processing their personal information.
Where there is any change, the individual shall be informed.
Where a data controller informs the above matters by formulating personal information processing rules (privacy policies), the rules shall be made public, and convenient for access and storage.

pwc

Individual Rights

The following Data Subject rights are provided under the PIPL:

- **Right to access:** Yes
- **Right to correction:** Yes
- **Right to restriction:** Yes
- **Right to deletion/be forgotten:** Yes
- **Right to portability:** Yes

Right to opt out of all or specific processing: Yes

Where a natural person dies, his or her next of kin may, for his/her own legal and legitimate interests, exercise the rights to access, copy, correct, and delete the relevant personal information of the deceased, unless otherwise instructed beforehand by the deceased.

Security & Data Breaches

Security Requirements: Yes

Data Breaches: In situations where the breach has occurred or may occur, data controllers must notify the regulator. In situations where the measures taken by the data controller can effectively prevent the harm, it may choose to not notify the individuals unless the regulator orders otherwise.

Notification to Supervisory Authorities: Yes.

Notification to Individuals: In situations where the measures taken by the data controller can effectively prevent the harm, it may choose to not notify the individuals unless the regulator orders otherwise.

Other Business Obligations

Data Protection Officer: Data controllers that handle personal information reaching the prescribed threshold amount must designate DPOs. Data controllers must report the names and contact information of the DPOs to the regulator.

Risk Assessments: Risk assessments must be conducted prior to:
(1) Processing sensitive personal data.
(2) Using personal information for automated decision-making.
(3) Entrusting personal information processing to others, providing personal information to other data controllers, or disclosing such information to the public.
(4) Transferring information overseas.
(5) Other information processing activities with significant impact on personal rights or interests.
The impact assessment report and processing record must be kept for at least three years.

Audits: Yes
Record Keeping: Yes
Trainings: Yes

Cross-Border Transfers

Cross-Border Data Transfers: Chinese government approval (security assessment) is required prior to the outbound transfer of Important Data, the outbound transfer of personal information by critical information infrastructure operators, the outbound transfer of sensitive personal data of > 10,000 individuals each year, or the outbound transfer of non-sensitive personal information of > 1 million individuals each year.

Chinese government recordal of Chinese SCCs or certification is required prior to the outbound transfer of < 10,000 individuals' sensitive personal information each year, or the outbound transfer of non-sensitive personal information of between > 100,000 individuals and < 1 million individuals each year.

Any outbound transfer of personal information or sensitive personal information must meet the following legal requirements:

- Separate consents having been obtained from the individual
- Data transfer impact assessments having been conducted
- Data transfer agreement having been signed between the data controller and the overseas recipient

Prior Chinese government approval is needed for a transfer of personal or other data by a Chinese organization or individual to a foreign law enforcement or judicial body.

Exemption rules on cross-border data transfer: Compliance obligations for cross-border data transfer mentioned above can be waived when:

- Cross-border data transfer is necessary for performance of a contract to which the individual is a party
- Cross-border data transfer is necessary for implementation of human resource management in accordance with labour rules and regulations as well as collective contract signed according to PRC law
- Responding to public health emergencies or protection of the life, health, or property of natural persons during emergencies
- Except for critical information infrastructure operators, the outbound transfer transfers non-sensitive personal information of less than 100,000 individuals

Localization Requirements: Critical information infrastructure operators and data controllers handling a volume of personal information that reaches the prescribed threshold amount must store in China the personal information collected or generated in China. Other sectoral laws and regulations have other data localization requirements.

Other/To Watch

China has various free trade zones ("FTZs"). The Shanghai, Tianjin and Beijing FTZs have issued new data rules for outbound transfer of data from these FTZs. In essence, under the FTZ data rules, the regulators would prepare lists of data that companies operating in the FTZs can transfer outside of China.

Let's connect to discuss how we can help:

Martyn Huckerby
Partner, Tiang & Partners (an independent Hong Kong law firm and a member of the PwC network)

+852 2833 4918
martyn.p.huckerby@TiangandPartners.com

This publication has been prepared for general guidance on matters of interest only and does not constitute professional advice. You should not act upon the information contained in this publication without obtaining specific professional advice. No representation or warranty (express or implied) is given as to the accuracy or completeness of the information contained in this publication, and, to the extent permitted by law, PwC, its members, employees and agents do not accept or assume any liability, responsibility or duty of care for any consequences of you or anyone else acting, or refraining to act, in reliance on the information contained in this publication or for any decision based on it.

© 2025 PwC. All rights reserved. Not for further distribution without the permission of PwC. PwC refers to the PwC network and/or one or more of its member firms, each of which is a separate legal entity. Please see www.pwc.com/structure for further details