



中倫
ZHONG LUN

WHAT CHANGES WITH THE NEW CHINESE PRIVACY LAW

Intro: On Nov. 1, 2021 the **China's Personal Information Protection Law (PIPL)** is into effect, aimed to "protect the rights and interests of individuals," "regulate personal information processing activities," and "facilitate reasonable use of personal information" (Article 1).

With its entry into force, the broader cyber and data security governance in China is regulated by three pieces of legislation: **the PIPL, the Cybersecurity Law, and the Data Security Law.** Implementing regulations have been adopted and some have yet to be adopted, making it complex to comply with this framework without proper legal and cybersecurity guidance.

On a comparative perspective, the PIPL aligns with the strictest international privacy benchmarks of the European Union's General Data Protection Regulation (**EU GDPR**) in large part, but it differs from the EU framework to a relevant extent. For instance, the PIPL includes certain substantive obligations that differ from the EU GDPR but there are also obligations found in the EU GDPR that are not included in the PIPL.

IMPACT OF THE PIPL ON COMPANIES AND ENTITIES:

- **Data subjects are given more rights over the use of their data:** They can request to edit, remove, restrict the use of their data, or withdraw consent given previously.
- There are More **stringent requirements on data sharing and cross-border data transfers,** demanding companies and any third party joint data controllers may to conduct data related impact assessments.
- **Penalties and fines** for data breaches and violations of the law can amount to up to 50 million RMB, revenue confiscation up to 5% annual revenue, business cessation, and individual responsibility of managers.
- **Mandatory cybersecurity controls** must be applied when storing and processing personal information, and training has to be provided to responsible personnel who handles such personal information.
- **obligatory data localization** when the amount of personal information exceeds the threshold set by the Cybersecurity Administration of China (CAC).

New Legal Framework of Data Protection in China

The "Three Pillars" of Cyberspace Administration and Data Protection

The Cybersecurity Law

effective as of June 1, 2017

- Multi-Level Protection Scheme ("MLPS")
- Network Critical Device and Dedicated Products Testing and Certification
- Critical Information Infrastructure ("CII") Security Protection
- Cybersecurity Review
- Cybersecurity Monitoring, Early Warning and Information Notification

The Personal Information Protection Law

effective as of November 1, 2021

- Determination of Personal Information ("PI")
- Basic Principles on PI processing
- Rights of PI Subjects
- Rules on Data Localization and Cross-border Transfer
- PI Processor Obligations .

The Data Security Law

effective as of Sept. 1, 2021

- Applicable scope: Data processing activities within the territory of the People's republic of China
- Data Security Standardization System
- Data Security Testing and Evaluation, Certification Administration
- Classified and Graded Data Protection Scheme
- Important Data Catalog
- Data Security Early Warning and Incident Response Scheme
- National Security Review
- Data Transaction and Online-data Processing Activities
- Cross-border Data Transfer Supervision



Main novelties of the PIPL

6 Legal Bases

- Expand the legal bases (consent, performance of contract, statutory duties, vital interest, public interest, and legal requirements)
- Introduces "Consent" but also "Separate consent"

Extra-territoriality

- For the purpose of providing products or services to natural persons within China
- Analyze and assess the conduct of natural persons within China

9 Principles

Lawfulness, legality, necessity, sincerity, purpose limitation, data minimization, transparency, accuracy, and accountability

Individuals' Rights

- Know and decide
- Restrict or refuse
- Access and copy
- Obtain and reuse
- Correct and delete

Liabilities

- CNY 50M or 5% of annual revenue
- Private right of action
- Personal liability of managers

Cross-border PI Data Transfer Regime & Localization Requirement

- Localization obligation (CIIOs, processors who exceed the threshold)
- Outbound PI Transfer restrictions and requirements including impact assessments

Contact PrivacyRules for legal and technical guidance and assistance on the PIPL:
www.privacyrules.com - info@privacyrules.com - +1 513 8132145