WINSTON & STRAWN LLP

BLOG

China Passed Personal Information Protection Law – How should we view this Chinese "GDPR"?

SEPTEMBER 3, 2021

On August 20, 2021, the National People's Congress Standing Committee finally passed the Personal Information Protection Law, which aims to establish a personal information protection system with Chinese features and, meanwhile, in line with international standards. It provides a variety of rights for personal information subjects to strengthen their control of personal information, while imposing strict obligations to personal information handlers. The law shall enter into force on November 1, 2021, leaving companies less than three months to prepare for their compliance obligations. Therefore, we would introduce the law in comparison to the EU General Data Protection Regulation to help companies better understand the key points and provide companies with preliminary guidance.

The publication of the EU General Data Protection Regulation ("**GDPR**") in April 2016 (effective May 2018) may be regarded as the beginning of a wave of data privacy rules across the globe. Following the trend, China passed its first comprehensive law regulating personal information protection on August 20, 2021, namely the Personal Information Protection Law[1] ("**PIPL**"), which will come into effect on November 1, 2021.

As a law dedicated to personal information protection, the PIPL tracks the GDPR in many perspectives. For example, both laws enjoy extraterritorial reach, provide various rights for personal information subjects, impose **high administrative fines** (PIPL sets a fine up to **RMB 50 million or 5% of annual revenue**) for infringements, and **set joint liability** upon the entities who jointly conduct data processing activities. However, the PIPL retains unique Chinese features, reflecting the government's regulatory approach toward personal information, especially from the perspectives of cross-border personal information transfer and the **public interest litigation system**. In short, in addition to protecting the rights and interests of personal information subjects, the PIPL also aims to safeguard national security and public interests.

Considering the PIPL would significantly impact the Chinese data protection legal framework, companies need to heed China's "GDPR." To better understand the regulations of the PIPL, we would compare it with the GDPR in the following aspects:

Territorial Scope

According to PIPL Article 3, the law primarily regulates how personal information[2] is handled within the territory of the People's Public of China ("**PRC**"), regardless of whether the entity that conducts handling activities has an establishment within the PRC.

As cross-border data transfers are essential in a globalized world, entities outside of China routinely may come into the possession or control of personal information relating to natural persons in China. The possession or control of this data adds both the risks for personal information infringement and the difficulty of personal information protection. It is thus important to include clauses for extraterritorial reach in the data protection legislation to better protect the interests of individuals, as well as maintain social stability and national security.

Therefore, it is not surprising to see that both the GDPR and the PIPL provide provisions regarding extraterritorial effects. PIPL Art. 3 states that it shall also apply to handling activities outside the territory of the PRC regarding the personal information of natural persons inside the territory of the PRC under certain circumstances. Examples include the provision of products or services from outside of the PRC to natural persons within the PRC. Other instances include where an entity outside of the PRC analyzes or assesses activities of natural persons within the PRC.

These concepts within the PIPL are not unfamiliar. The GDPR also applies to the processing of personal data of data subjects who are in the EU by a controller or processor not established in the EU, where the processing activities are related to the offering of goods or services to such data subjects in the EU or the monitoring of their behavior takes place within the EU. To confirm whether the processing activities are related to the offering of goods or services, the GDPR further clarifies that, factors such as the use of a generally used language or currency in the States with the possibility of ordering goods and services in that other language, or the mentioning of customers or users who are in the EU may be considered, which to some extent helps us better understand the provision in the PIPL.

Rights of the Personal Information Subjects

The PIPL provides abundant rights for personal information subjects, such as the right to know, the right to decide on, and the right to limit or refuse the handling of their personal information by others. Individuals also enjoy the right to access and copy their personal information from personal information handlers,[3] the right to request correction or completion of their personal information, the right to withdraw consent, and the right to request that personal information handlers explain the handling rules. Under certain circumstances, the PIPL grants individuals the right to delete, such as when the handling purpose has been achieved, is impossible to achieve, or is no longer necessary to achieve.

Although adopting different terms, the data subjects enjoy similar rights under the GDPR, such as the right of access, the right to rectification, the right to be forgotten, the right to object, etc. It is worth noting that the PIPL imposes higher obligations on the personal information handlers regarding the individual's right to know. For example, when providing personal information to other parties, regarding the scope of notification of the recipients' information, while the PIPL requires personal information handlers to notify individuals about the name/personal name and contact method of the receiving party, the data controller only needs to notify the data subjects about the categories of recipients under the GDPR.

In addition, the GDPR provides individuals with the right to data portability, which also appears in the PIPL after its third review. PIPL Art. 45 states that where 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. The GDPR provides more clear regulations regarding this right, stating that the data shall be transferred in a structured, commonly used and machine-readable format, and the data subject shall only exercise the right under certain circumstances, i.e., when the lawful basis for processing the data is consent or for the performance of a contract, and the processing is carried out by automated means. It is recognized that the right to data portability better enables the individual's control of personal information and to some extent promotes the data flow between different platforms. However, it may generate technical difficulties for small-scale businesses as well as aggravate unfair competition between

companies for data assets. Considering PIPL Art. 45 emphasizes that the right to data portability shall be exercised subject to the conditions set by the State cyberspace administrations, we can anticipate that the administrations will release further regulations to better implement the rule.

Personal Information Export Mechanisms

The PIPL imposes clear obligations on the provision of personal information to any foreign parties. PIPL Art. 38 provides three mechanisms for exporting personal information out of the PRC, depending on the type of personal information handlers who need to provide personal information outside the PRC for business or other such purposes.

Critical information infrastructure operators[4] and personal information handlers processing personal information reaching certain volumes shall store personal information collected and produced within the PRC domestically. Where such personal information must be provided across borders, the PIPL requires that such cross-border provision pass a security assessment administered by the State cyberspace administrations. Unfortunately, there is a lack of clear guidance on assessment procedures and standards at the current stage.

As for other personal information handlers, the PIPL provides two additional mechanisms for their cross-border personal information provision needs, namely 1) obtaining personal information protection certification; or 2) concluding a standard contract formulated by the State cyberspace administrations with the foreign receiving party.

The two export mechanisms can also be found in the GDPR. GDPR Art. 46 stipulates that a controller or processor may (in the absence of an adequacy decision) transfer personal data to a third country or an international organization only if the controller or processor has provided appropriate safeguards, and on the condition that enforceable data subject rights and effective legal remedies for data subjects are available. GDPR recognizes, inter alia, both standard contractual clauses and approved certification mechanisms as “appropriate safeguards.”

However, the PIPL also provides exemptions for the above mechanisms that the provision of personal information abroad can be conducted in the ways stipulated in the treaties or international agreements concluded or acceded to by the Chinese government.

Overall, the PIPL imposes more restrictions on the cross-border provision of personal information than the GDPR does. The PIPL provides fewer legal bases for the export of personal information. Additionally, to provide personal information abroad, personal information handlers shall conduct a personal information protection impact assessment in advance, fulfill its notification obligations to the individual, and obtain the individual’s separate consent, as well as adopt necessary measures to ensure that foreign receiving parties’ personal information handling activities reach the standard of protection provided in the PIPL.

Legal Liabilities

Many companies are quite concerned about the GDPR due to its tough fines, which could be up to €20 million, or 4% of a company’s worldwide annual revenue from the preceding financial year, whichever amount is higher. The PIPL also may fine up to RMB 50 million or 5% of a company’s turnover in the previous year (it is unclear how the 5% will be calculated and whether it refers to turnover in China or worldwide). The authorities may also order the suspension of related business activities, or cessation of business for rectification, cancellation, or corresponding professional licenses or business permits.

The directly responsible person in charge and other directly responsible personnel are fined up to RMB 1 million and may also be prohibited from holding the positions of director, supervisor, high-level manager, or personal information protection officer for a certain period.

In addition to the administrative liabilities mentioned above, the PIPL provides civil and potential criminal liabilities. Civil liabilities include penalties for damages and losses to the individual. Joint personal information handlers would

bear joint liability if their personal information handling activities harm individuals' personal information rights and interests and result in damages. PIPL Art. 70 further establishes a public interest litigation system, stating that the People's Procuratorates (the Prosecutor General's Office in common parlance), statutorily designated consumer organizations, and organizations designated by the State cyberspace administrations may file a lawsuit if the rights and interests of many individuals are infringed by the personal information handlers. Criminal liability would be pursued depending on the type of violation.

China-specific Provisions

As mentioned above, the PIPL provides some provisions with strong national features, which indicates that the government has considered personal information protection to be an important issue for national security. For example, PIPL Art. 41 prohibits personal information handlers to provide any personal information stored within the PRC to any foreign judicial or law enforcement agencies without approval of the authorities. PIPL Arts. 42-43 further provide regulations for extraterritorial and reciprocal protection systems, specifying that the government may put the foreign entities on a list limiting or prohibiting personal information provision if they engage in any personal information handling activity harming the national security or public interests of the PRC, and adopt retaliatory measures against any country or region adopting discriminatory prohibitions, limitations, or other similar measures against the PRC in the area of personal information protection.

To summarize, the protection of personal information in China is not only a matter of securing the rights and interests of personal information subjects, but also an essential element of national security and public interests.

Observations and Suggestions

As analyzed above, although the PIPL draws great inspiration from the GDPR, the PIPL imposes higher compliance obligations on companies from certain perspectives. For example, when transferring personal information abroad, individual's "separate consent" of cross-border personal data transfer is required under PIPL. Therefore, companies that fall in the regulatory scope of the PIPL shall develop their compliance system accordingly, instead of relying on the GDPR system. It is worth noting that the PIPL would come into effect within less than three months, which would be a great challenge for companies due to its strict penalties and stringent obligations placed.

In this regard, we would suggest companies start considering the questions that may arise from the new law, such as:

- Does the company need to set up a local data center?
- Does the company need to update its data processing agreement with its third-party data processors?
- How shall the company update its internal policies, such as personal information policies for employees or consumers?
- What export mechanism can the company adopt in order to achieve its data transfer needs with foreign affiliates?

Considering the PIPL is overall legislation establishing the data protection framework and provides general principles for personal information handling activities and personal information handlers' obligations, it somehow lacks detailed explanations. It is anticipated that the authorities would release further regulations and rules to provide companies with more guidance and implement the supervision work step-by-step.

---

[1] Standing Committee of the National People's Congress, PRC Personal Information Protection Law (《中华人民共和国个人信息保护法》), published on August 20, 2021, English version available at https://digichina.stanford.edu/news/translation-personal-information-protection-law-peoples-republic-china-effective-nov-1-2021.

[2] According to PIPL Art. 4, "personal information" refers to all kinds of information, recorded by electronic or other means, related to an identified or identifiable natural person, not including information after anonymization handling; "personal information handling" includes personal information collection, storage, use, processing, transmission, provision, publishing, deletion, etc.

[3] PIPL Art. 73 defines “personal information handlers” as organizations and individuals that, in personal information handling activities, autonomously determine handling purposes.

[4] According to the *Critical Information Infrastructure Security Protection Regulations* (effective September 1, 2021), critical information infrastructure refers to important network infrastructure, information systems, etc., in important industries and sectors such as public telecommunications and information services, energy, transportation, water, finance, public services, e-government, national defense science, technology, industry, etc., as well as where their destruction, loss of functionality, or data leakage may gravely harm national security, the national economy and people’s livelihoods, or the public interest.. rotection work departments would be responsible for organizing the identification of critical information infrastructure within industries and sectors and promptly notifying operators about their identification results.

10 Min Read

Authors

Cari Stinebower

Peter Crowther

Related Locations

London | Shanghai

Related Topics

Privacy and Data Security | Asia Privacy | General Data Protection Regulation (GDPR)

Related Capabilities

Privacy & Data Security

Related Regions

Asia | Europe

Related Professionals

Cari Stinebower

Peter Crowther

This entry has been created for information and planning purposes. It is not intended to be, nor should it be substituted for, legal advice, which turns on specific facts.