China’s new privacy law imposes heightened safeguards for the protection of personal information of its residents and may have extra-territorial application to organizations outside the country. The Personal Information Protection Law (PIPL), which went into effect on November 1, 2021, will work together with China’s existing Cybersecurity Law (CSL) and Data Security Law (DSL) to establish a broader framework governing cybersecurity and data privacy protection in China. The new privacy law impacts both domestic and multinational companies to the extent they process or use the personal information of individuals located within China.

PIPL specifies the scope of personal information; clarifies the legal bases for processing personal information; lays down the obligations and responsibilities imposed on processors; and imposes stringent requirements on data localization, safeguarding China’s interests in the case of cross-border transfer of personal information. While PIPL is similar to the European Union’s General Data Protection Regulation (GDPR), there are some key differences and additional requirements companies must keep in mind to stay compliant.
Scope

Similar to GDPR, PIPL extends its territorial scope to encompass “personal information processing entities” outside of China, provided that the purpose of the processing is:

- To provide products or services to individuals in China
- To “analyze” or “assess” the behavior of individuals in China, or
- For any other circumstances as provided by law or regulations.

PIPL also requires offshore entities to establish a “dedicated office/entity” or appoint a “designated representative” in China for purposes of personal information protection. The name and contact details of such local agent or representative will need to be provided to the relevant domestic authority.

Key Definitions

PIPL’s key definitions regarding protected data and entities subject to the law are summarized below; these are similar in many respects to definitions set forth in GDPR.

**Personal Information** is broadly defined to include “any information (such as video, voice, or image data) relating to any identified or identifiable natural person, notwithstanding whether it is in an electronic form or any other form, exclusive of any anonymized information.”

**Sensitive Personal Information** includes “personal information that, once leaked, or illegally used, may easily infringe the dignity of a natural person or cause harm to personal safety and property security, such as biometric identification information, religious beliefs, specially designated status, medical health information, financial accounts, information on individuals’ whereabouts, as well as personal information of minors under the age of 14.”

However, anonymized (or de-identified) information is not deemed to constitute protected “personal information” under PIPL. For purposes of the application of PIPL, **Anonymization** refers to the processing of personal information in a way that makes it impossible to identify natural persons, and the personal information cannot be restored after processing.

PIPL applies to a **Personal Information Processing Entity** and/or an **Entrusted Party**. The former includes an “organization or individual that independently determines the purposes and means for processing of personal information.” This is equivalent to the concept of a “data controller” under GDPR. The latter applies to a “data processor” as defined under GDPR.

The **processing** of personal information includes, but is not limited to, the collection, storage, use, processing, transmission, provision, disclosure and deletion of personal information.
Legal Basis for Processing Personal Information

PIPL broadens GDPR’s “legitimate interests” requirement to process personal information. A data subject’s personal information may be processed with the express “consent” of the individual, or in certain other limited circumstances. Such consent “must be informed, freely given, demonstrated by a clear action of the individual, and may later be withdrawn.”

In particular, an individual’s consent to process their personal information is required when:

- Sensitive personal information is processed
- The personal information is provided by the processor to another processor
- The personal information is transferred outside of China.

In addition, Article 13 of PIPL affords the following exceptions whereby personal information may be processed without the individual’s consent, when it is:

- Necessary to enter into or perform a contract to which the individual is a party, or where necessary to conduct human resources management according to lawfully formulated internal labor policies and lawfully concluded collective labor contracts.
- Necessary to perform legal responsibilities or obligations.
- Necessary to respond to a public health emergency, or in an emergency to protect the safety of individuals’ health and property.
- To a reasonable extent, for purposes of carrying out news reporting and media monitoring for public interests.
- Personal information that is already disclosed by individuals or otherwise lawfully disclosed, within a reasonable scope in accordance with PIPL.
- In other circumstances as required by laws.

Individuals’ Rights

PIPL closely aligns with GDPR with respect to an individual’s rights over their personal information, including (1) the right to access, correct, erase, object to and restrict the processing of the individual’s data; (2) the right to data portability; (3) the right not to be subject to automated decision making; (4) the right to withdraw consent; and (5) the right to lodge a complaint with the regulator.

PIPL requires processing entities to “timely” respond to an individual’s requests concerning their data rather than providing a specific timeline for responding. Under PIPL, individuals also will have the right to bring lawsuits against processing entities if they reject the individuals’ requests to exercise their rights.
Processors' Obligations to Safeguard Personal Information

Similar to GDPR, PIPL sets forth a regulatory framework that imposes stringent security safeguards and controls on all entities that process personal information, including:

- Formulating internal management systems and operation procedures
- Implementing classified management of personal information
- Adopting corresponding technical security measures, such as encryption and de-identification
- Reasonably determining the operational authorizations for personal information and providing regular security education and training for operational staff
- Formulating and implementing response plans for security incidents relating to personal information
- Conducting regular compliance audits
- Adopting other security measures as stipulated by laws and regulations.

A processor that provides an important internet platform service, has a large user base and/or operates complex types of businesses is further required to build a robust data compliance program (including preparing a personal information protection compliance policy) and establish/appoint an independent body to supervise its implementation. They also must actively monitor the behaviors of the service or product providers on their platform that have the potential to violate any laws or administrative regulations in conducting processing activities.

Cross-Border Transfer of Personal Information

In general, a processing entity that plans to transfer personal information to entities outside of China is required to:

- Provide individuals with certain specific information about the transfers and obtain separate consent
- Adopt necessary measures to ensure that the overseas recipients can provide the same level of protection as required under PIPL
- Carry out a personal information protection impact assessment.

PIPL has some additional requirements compared with GDPR regarding the cross-border transfer of personal information. For example, operators or entities processing a large amount of personal information need to store personal information locally. If it is indeed necessary to transfer such personal information overseas, it shall pass a security assessment administered by the Cyberspace Administration of China (CAC) and other enforcement authorities.

Other processing entities can choose to obtain a personal information protection
certification from a professional body recognized by the CAC, execute an agreement with the overseas recipient based on a standard contract to be released by the CAC for their transfers, pass the security assessment by the CAC, or meet other requirements as provided by relevant laws and regulations.

**Personal Information Protection Impact Assessments**

Article 55 of PIPL requires personal information processing entities to carry out Personal Information Protection Impact Assessments (PIPIAs) and retain the processing records for at least three years for the following processing activities:

- Processing of sensitive personal information
- Processing of personal information for automated decision-making
- Entrusting vendors to process personal information, sharing personal information with other processing entities or publicly disclosing personal information
- Transferring personal information overseas
- Performing other personal information processing activities that may have significant impacts on the rights and interests of individuals.

Although the obligations to conduct a prior PIPIA are similar to the “data protection impact assessments” under GDPR, the processing activities that will trigger such an assessment are different. For instance, under PIPL, there is no obligation to consult a regulator in the event that an organization concludes – after completing such an assessment – that it cannot remediate certain residual risks identified.

**Joint Processing and Entrusted Processing**

PIPL provides that where two or more processors jointly determine the purpose and method with respect to processing personal information, their respective rights and obligations shall be agreed on. The law imposes joint and several liability on joint processors if the joint processing activities infringe on personal information rights and interests and result in damages.

Where a processor entrusts a third party to process personal information, under PIPL the processor must supervise the processing activities of such third party. Such entrusted third party is required to undertake necessary measures to protect personal information in accordance with PIPL and to assist the processor in complying with the law. Without the consent of the processor, the entrusted party is prohibited from permitting other parties to process personal information.

**Regulatory Fines and Penalties**

If a processing entity violates the requirements under PIPL, regulators may order it to take corrective actions, issue warnings, confiscate illegal income, suspend services, revoke operating permits or business licenses, or issue a fine. The fine can be up to 50 million RMB or 5 percent of an organization’s annual revenue/turnover.
for the prior financial year. Besides monetary fines, violations also may be recorded into the “credit files” of the processing entity under China’s national social credit system.

The person in charge or other directly liable individuals also may be held liable and subject to a fine up to 1 million RMB. Such individuals may further be restricted from serving as director, supervisor, senior management or personal information protection officer for a stipulated period of time.

Moreover, the processing entities will be liable for tort damages if they infringe the rights and interests of personal information. PIPL imposes the burden of proof on the defendant personal information processor in a civil action to facilitate damage claims, which may lead to a higher number of cases being brought forward. If the processing entities infringe the rights and interests of a large number of individuals, the Supreme People's Procuratorate (Prosecutor General's Office) and other entities authorized by the CAC may file public interest lawsuits.

Conclusion

In summary, China’s new Personal Information Protection Law affords greater protection and rights to the country’s residents over their personal data. Domestic or foreign organizations that process personal information of China’s residents are now subject to heightened requirements, including but not limited to:

- Obtaining individuals’ consent to process personal information
- Addressing individuals’ requests to exercise their rights over personal information
- Implementing adequate safeguards and security measures to protect personal information
- Adhering to limitations on cross-border transfers of personal information outside of China
- Conducting Personal Information Protection Impact Assessments
- Supervising third-party processors to ensure compliance with PIPL.

Failure to comply with PIPL’s expanded privacy law may subject both domestic and foreign organizations to substantial regulatory fines and penalties, revocation of business licenses, legal action and even personal liability.

© 2022 Wilson Elser

National Law Review, Volume XI, Number 336

Source URL: https://www.natlawreview.com/article/china-s-new-personal-information-protection-law