FANGDA PARTNERS
方達津師事務所

China's Personal Information Protection Law and the Roadmap to Compliance

Authors:

Kate Yin
Partner, Fangda Partners
kate.yin@fangdalaw.com

Gil Zhang
Partner, Fangda Partners
gil.zhang@fangdalaw.com

China passed its first comprehensive law on personal information protection, the Personal Information Protection Law (the "**PIPL**") on August 20, 2021. The PIPL will come into force on November 1, 2021. There is no grace period for compliance, which leaves little time for companies to prepare themselves to ensure they comply with the new law.

Many companies have already gone to great lengths to make sure they are GDPR-compliant and the hope is that these efforts will make it easier for them to become PIPL-compliant. There are, however, key differences, notably that the PIPL has a strong focus on consent by individuals on how their information is processed. The concept of "legitimate interest" for processing personal data, which is widely used in the EU, is not recognized in the PIPL. The PIPL applies both to the private and public sectors.

This article discusses the material differences between the GDPR and the PIPL and highlights some areas that leave some room for clarification.

Scope of Application of the PIPL

The PIPL applies to any processing of individuals' personal information that takes place in China regardless of data subject's nationality or the physical location. Similar to the GDPR, the PIPL also applies extra-territorially to the processing of the personal information of data subjects in China that takes places outside China if such processing is (1) for the purpose of provision of goods and/or services to data subjects in China; (2) for analyzing or assessing the behavior of data subjects in China; or (3) in other circumstances as provided by Chinese laws and regulations.

Similar to Article 27 of the GDPR, companies outside China that have no business presence in China but are subject to the PIPL are required to set up an organization or appoint a representative in China dedicated to data protection. Such companies shall file the name and contact information of any appointed organization or representative with Chinese regulators.

Different Roles in Processing of Personal Information

The "personal information processor" under the PIPL refers to organization(s) or individual(s) that determine the purpose and means of personal information processing (which is somewhat counter-intuitive). This is similar to the role of "controller" as defined in the GDPR. Joint controllers shall be liable jointly for any damages caused as a result of the infringement of data subjects' rights.

"Entrusted party" is the term that is used in the PIPL (rather than data processor) as the party entrusted by the personal information processor to process personal information. There are two primary obligations on the entrusted party: (1) to take necessary measures to safeguard personal information; and (2) to assist personal information processors in discharging their obligations under the PIPL. It is mandatory to enter into a data protection agreement between the personal information processor and the entrusted party.

The Lawful Basis for Processing of Personal information

The PIPL places a strong focus on data subjects' consent, not only at the time of collection, but also at various critical stage or type of processing of the personal information, such as disclosure, sharing with third parties, cross-border data transfer or parental consent.

Where consent is relied on as the lawful basis for processing personal information, a separate consent from the data subjects is required in certain specific circumstances, such as provision of personal information to third parties, the processing of sensitive personal information, and cross-border transfer of personal information. However, the PIPL remains silent on how exactly a separate consent should be obtained.

Other than consent, the PIPL provides other lawful bases for the processing of personal information, including where such processing:

- is necessary for the conclusion or performance of a contract to which the data subject is a party, or necessary for human resources management according to lawfully formulated employment-related company policies and collective agreements;
- is necessary for discharging legal responsibilities or obligations;
- is required for public health purposes or the protection of the life, health and property safety of people in emergency cases;
- is reasonably in the public interest, for the purposes, for example, of news, journalism and public supervision;
- has been made public either by the data subjects themselves or by other lawful means within the reasonable and permissible bounds; or
- other circumstances provided by laws and regulations.

Where any of the lawful bases other than consent are relied on to process personal information, the separate consent requirements that are scattered in various provisions of PIPL (e.g. separate consent for cross-border data transfer, processing of sensitive personal data) would not apply to such processing.

The non-consent lawful bases in the PIPL are either context-specific or subject to narrow interpretation. This is particularly the case where companies seek to argue that the processing of personal information is for contractual necessity, which might give rise to the authorities challenging that necessity. For example, if the employer of employees in China is a Chinese company, it might be difficult to argue that the cross-border transfer of employee data (such as COVID vaccination-related data for return to office management) to company headquarters actually constitutes necessity for the purpose of performance of employment contract.

More Data Subjects' Rights

Individuals – or data subjects – are given greater rights than as set out in the current China Cyber Security Law ("CSL"), including the right to information, the right to be informed of decisions, rights of access, right to ask for correction or deletion, and the right to withdraw consent, as well as the right to data portability, all of which are subject to other conditions to be clarified by the Cybersecurity Administration of China ("**CAC**").

The PIPL also protects the rights of data subjects after they have died, allowing their next of kin to exercise the rights to access, copy, rectification and deletions for legitimate purposes.

The personal information processor is required to establish a mechanism that facilitates the handling of data subjects' requests without there being unnecessary constraints. Refusal to meet requests by data subjects when exercising their rights without justifiable grounds may result in privacy litigation under Article 50 of the PIPL. There are some grounds for refusal to accede to data subjects' requests as set out in the Recommended National Standard - Personal Data Security Specification ("**PDSS**"), such as when the request is related to national security or the data subject is acting with ill intent or abusing his/her right. As the PIPL does not specifically recognize these grounds for refusal, it is worth watching this space to see how the courts in China will adjudicate on these PDSS grounds for refusal.

Obligations of Personal Information Processor

The PIPL lays down various security and organizational requirements that must be followed, such as the requirement to have regular compliance audits, data classification, keeping records of processing activities, data protection impact assessments, data breach reporting requirements and remedial measures that must be taken in the case of data breaches, and appointment of data protection responsible person, among other requirements.

The security measures under the PIPL are not exhaustively defined. The personal information processors may need to adopt such measures to provide a level of security appropriate to the risk of processing personal information.

The operators of what are regarded as mega platforms (although these are not clearly defined) containing massive amounts of personal information are subject to additional obligations. These include putting in place personal information compliance programs, establishing an independent supervisor, and regularly issuing social responsibility reports explaining how they are protecting people's data.

Data Localization Requirements

The PIPL also requires personal information processors that process personal information over a certain volume to comply with data localization requirements. As yet, it is not clear what the threshold is for the volume of data.

Cross-border Data Transfer

According to the PIPL, companies are allowed to transfer personal information outside China in any of the following circumstances where the cross-border data transfer is for business purposes as follows:

- where the CAC has given approval after its security review;
- where the information has been certified by a licensed agency, acting in accordance with the provisions of CAC in respect of the protection of personal information;
- where the information is necessary to conclude a contract in the form of a CAC-prescribed template; or
- satisfying other conditions as prescribed by laws, regulations or CAC's measures.

Regardless of how the cross-border data transfer is effected, the personal information processors must ensure that the data recipient(s) safeguard the personal information that has been received to at least the same level that is required by the PIPL. For many multinational companies, this means that the systems that are used to store personal information coming out from China and centrally managed outside China need to match the technical requirements that are laid down under the PIPL.

Consistent with China's Data Security Law and the Securities Law, the PIPL provides that the personal information processor shall not provide personal information stored in China to foreign authorities and judicial bodies unless this has been approved in advance by the Chinese authorities.

Multiple Supervisory Authorities to regulate personal information protection

The PIPL does not provide for an omnibus enforcement agency but authorizes the CAC as the coordinating and leading ministry to coordinate with other ministries on rule-making and law enforcement actions. When it comes to personal information protection, the regulators are those that might be expected, such as the CAC, the Ministry of Public Security, the Ministry of Industry and Information Technology and various sectoral regulators.

Increased Legal Ramification

Those found to be in violation of the PIPL are subject to criminal, administrative and civil penalties. Those found to be in serious breach of the PIPL are liable to be fined up to RMB50 million (US$7.4 million) or up to 5 percent of the preceding year's revenues. Regulators also have the power to suspend or terminate any App or online service that illegally process personal information. Those who are responsible for causing the violation may be disqualified from being directors, supervisors, general managers or personal information protection officers.

When it comes to litigation, the presumption is that the personal information processor is at fault when the claimant sues on tort for infringement of the right to personal information protection. In order to discharge that presumption, the personal information processor will have to demonstrate that they have complied with the provisions of the PIPL. If the personal information processor fails to prove that they are not at fault, the personal information processor shall be liable to the data subjects. The PIPL also authorizes the People's Procuratorate, consumer protection organizations and other organizations designated by the CAC to claim against the company in breach of the PIPL.

Roadmap to compliance with PIPL

With just two months before the PIPL becomes law, companies should take the necessary actions to localize the data protection processes and product designs to bring them in line with the PIPL. Companies can refer to the appendix to this article for a quick check on the requirements under PIPL in comparison with GDPR.

- Conduct data mapping for China related processing of personal information and document these activities and prepare RoPA (record of processing activities). On the lawful basis, companies should consider the substitute of legitimate interest under the PIPL for these processing activities.
- Compliance gap analysis is inevitable. Companies in China do not find the readiness check very helpful as this does not reveal the granularity of compliance gaps and what to address.
- Sort out the relationship with third parties and put in place data protection agreement as well as cross-border data transfer agreement if the third parties are outside China. This may not be straightforward as Chinese regulators have not yet provided clarity on how they determine joint controllership and relationship of controller (i.e. personal information processor in PIPL) and processor (i.e. entrusted party).
- Prepare China PIPL centric policies and processes, for example breach response protocol as Chinese laws require network incident and data breach incident may need to be reported to various regulators depending on different regulator-specific breach reporting threshold.
- Appoint local resource to be responsible for the personal information protection and be local DPO. One notable difference between the PIPL and the GDPR is that the PIPL requires companies to appoint a person or team to be directly responsible for PIPL compliance and implementation, and not just advisors. Hiring of local resources in a short time could prove difficult since there is a shortage of experienced personal information protection professionals in China.

More generally, those businesses in China that operate Apps and other online services can expect a sweeping law enforcement campaign specifically to do with the PIPL when it comes into force.

Appendix: Comparison of PIPL with GDPR and CCPA/CPRA

This chart provides a bullet-point summary of major compliance requirements of the PIPL in comparison to the GDPR and the CCPA/CPRA, from which it can be seen that the PIPL is as strict as GDPR in general and even more strict in certain sectors.

Compliance Requirements	**PIPL**	**GDPR**
Accountability	√	√
Transparency	√	√
Lawful basis	√ (Consent, contractual necessity, compliance with laws etc.)	√
Sensitive personal information	√	√
Purpose limitation	√	√
Data minimization	√	√
Limited Retention	√	√
Manage processing	√	√
Joint processing	√	√
Data localization	√ (CIIO and some personal information processors with certain large amount of personal data)	× (Restrictions under Member States' industrial rules)
Cross-border data transfer	√ (Security assessment, personal information protection certification, or **SCC**)	√ (Different data cross-border transfer mechanisms like SCC, BCRs)
Data subject rights	√ (Rights to access, copy, correction, deletion, restriction of processing, withdraw of consent, portability; data subject rights for the deceased)	√
Safeguards	√	√
DPO	√	√
Documentation	√	√
DPIA	√	√ (High-risk data processing activities)
Privacy by design/default	√	√
Privacy Audit	√	√

Beijing

27/F, North Tower
Beijing Kerry Centre
1 Guanghua Road
Chaoyang District
Beijing 100020, China

Tel: +86 10 5769 5600
Fax:+86 10 5769 5788

Guangzhou

17/F, International Finance
Place, 8 Huaxia Road,
Zhujiang New Town
Guangzhou 510623, China

Tel: +86 20 3225 3888
Fax:+86 20 3225 3899

Hong Kong

26/F, One Exchange Square
8 Connaught Place, Central
Hong Kong

Tel: +852 3976 8888
Fax:+852 2110 4285

Shanghai

24/F, HKRI Centre Two,
HKRI Taikoo Hui
288 Shi Men Yi Road
Shanghai 200041, China

Tel: +86 21 2208 1166
Fax:+86 21 5298 5599

Shenzhen

17/F, Tower One, Kerry Plaza
1 Zhong Xin Si Road
Futian District
Shenzhen 518048, China

Tel: +86 755 8159 3999
Fax:+86 755 8159 3900