CHINA'S PERSONAL INFORMATION PROTECTION LAW (PIPL)

Category: Privacy Law and POPIA,Privacy Law, Infosec, and POPIA
written by Sadia Rizvi | August 25, 2022

INTRODUCTION

On 1 November 2021, the Personal Information Protection Law ("PIPL") took effect in China. China's PIPL is the first comprehensive piece of legislation that is aimed at protecting the personal information of Chinese citizens. Therefore, Chinese organisations and foreign organisations that process Chinese citizens personal information are now required to comply with the provisions of the PIPL.

SUMMARY OF CHINA'S PIPL

Similar to South Africa's Protection of Personal Information Act ("POPIA")[1], China's PIPL protects individuals' personal information. Therefore, organisations who collect and use data subjects must obtain informed consent to use it. Collection, processing, storage, and sharing is referred to as "handling" and organisations who handle personal information are referred to as "personal information handlers". A personal information handler is the equivalent of a data controller in terms of the European Union's General Data Protection Regulation ("GDPR")[2] or a responsible party under POPIA.

There are 6 lawful bases for collecting personal information:

1. consent;
2. where it is necessary to conclude or fulfill a contract in which the individual is an interested party, or where necessary to conduct human resources management according to lawfully formulated labour rules and structures and lawfully concluded collective contracts;
3. where it is necessary to fulfill statutory duties and responsibilities or statutory obligations;
4. where necessary to respond to sudden public health incidents or protect natural persons' lives and health, or the security of their property, under emergency conditions;
5. handling personal information within a reasonable scope to implement news reporting, public

opinion supervision, and other such activities for the public interest;
6. when handling personal information disclosed by persons themselves or otherwise already lawfully disclosed, within a reasonable scope in accordance with the provisions of the PIPL; and
7. other circumstances provided in laws and administrative regulations.

It is important to note that the other bases for collecting personal information does not require consent from the data subject. Unlike the GDPR and POPIA, there is no "legitimate interest" basis to collect and process personal information. Legitimate interest means that the information can be collected without the data subject's consent, provided that it is in the interests of the responsible party or the data controller and that there is a justifiable reason for its use. Article 14 further states that consent must be given by an individual under full knowledge, and in a voluntary and explicit statement, and consent can be revoked at any time.[3] Where the purpose for handling changes, consent must be obtained afresh.

Articles 44 to 50 provides for data subjects' rights. In this respect, the PIPL aligns closely with the GDPR in that it provides for similar rights including the right to access, correction, deletion, erasure, and objection to the processing of personal information. Data subjects have the right to bring civil action against infringers and are liable under tort law (the equivalent of the law of delict in South Africa). Regulators are allowed to take action against infringers which include ordering corrective actions, issuing warnings, issuing a fine, and even revoking operating licenses for the entity. Violations of the PIPL may also be recorded into the "credit files" of the processing entity under China's national social credit system. The law creates personal and criminal liability for officers in violation of their duties under the PIPL. The director or head of an organisation can be held personally responsible and issued with a fine, or even be suspended from holding positions of director, supervisor, high-level manager or Personal Information Protection Officer for a stipulated period of time.

China's PIPL also offers protections to sensitive personal information. Article 28 states that sensitive personal information means personal information that, once leaked or illegally used, may easily cause harm to the dignity of natural persons grave harm to personal or property security. This includes biometric information, religious beliefs, specific identities, medical health, financial accounts, individual location tracking, as well as the personal information of minors under the age of 14.

Separate and specific consent must be obtained from the data subject before handling sensitive personal information. In addition, personal information handlers must have a specific purpose and must demonstrate sufficient necessity when processing sensitive personal information. They must take "strict protection measures" and furthermore, notify individuals.

China's PIPL further includes provisions similar to the GDPR and POPIA such as:

1. notification to data subjects;
2. data retention periods;
3. the implementation of security measures to protect personal information;
4. conducting of data protection impact assessments for certain processing activities;
5. the appointment of a data protection officer;
6. notification to the authorities regarding a data breach.

Importantly, if an organisation is located outside of China, a representative in China must be appointed to conduct regular audits relating to practices of data handling. There are additional rules that applies to personal information handlers that provide important internet platform services". However, platforms such as Facebook and WhatsApp are blocked in China.

China's PIPL also covers important provisions relating to cross border transfers of data, and these provisions are similar to the GDPR. Measures include providing individuals with specific information relating to transfers and obtaining the specific consent of the data subject. Organisations must adopt measures to ensure that foreign recipients provide the same level of protection as under the PIPL. An organisation must perform a personal information protection impact assessment and keeps a record of the processing for at least 3 years. There are certain other additional requirements. For example, Article 40 states that where an organisation processes large amounts of personal information, they need to store that information locally. If it is necessary to transfer the information, it must pass security assessment that is administered by the Cyberspace Administration of China ("CAC") and other enforcement authorities. Other entities can choose to obtain a personal information protection certification from a professional body that is recognised by the CAC.

CONCLUSION

In summary, the PIPL affords greater protection to Chinese citizens' personal information and harmonises international business practices when conducting business with China. If a company is already compliant with the provisions of the GDPR, then they are already largely compliant with the provisions of the PIPL. However, in many instances the PIPL is stricter than the GDPR and the penalties for non-compliance are quite severe. Therefore, domestic and foreign organisations conducting business in China must ensure compliance with the provisions of the PIPL.

Contact us for more good, clear, precise advice.

[1] Act 4 of 2013.

[2] Regulation (EU) 2016/679 of the European Parliament.

[3] Article 14 and Article 15 of the PIPL.