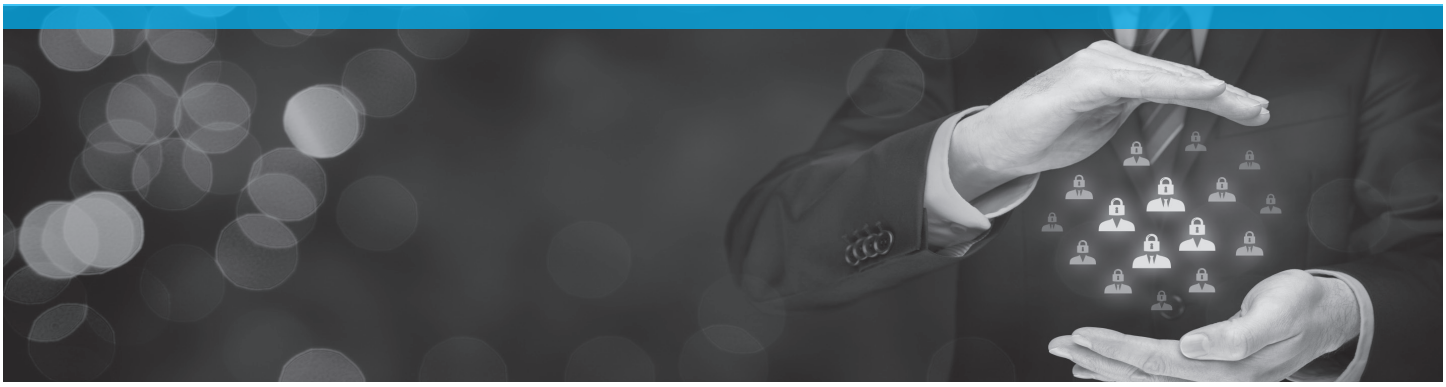
whitepaper

PERSONAL INFORMATION PROTECTION LAW OF THE PEOPLE'S REPUBLIC OF CHINA ("PIPL")

This White Paper will provide a general summary of key provisions set forth under the law.



On August 20, 2021, China joined several countries in enacting its version of a data protection law. The law is titled *Personal Information Protection Law* ("PIPL") and becomes effective November 1, 2021. PIPL implements provisions similar to other international privacy laws, such as the European Union's (EU) General Data Protection Law (GDPR); however, PIPL has some notable distinctions that employers may need to consider with when running background checks on natural persons in China.

Specifically, clients ordering background checks on individuals located in China will need to comply with international transfer requirements, which generally include: obtaining individual consent, conducting an Impact Assessment, and providing a lawful stated purpose. Further details are set forth under the **"DATA TRANSFERS OUTSIDE OF CHINA"** section below.

This White Paper will also provide a general summary of key provisions set forth under the law. Such provisions do not necessarily apply to the background check process, but cover requirements for clients to consider such as data subject rights and data security. The information below is not intended to serve as an official translation and should not be used as legal advice. Clients are encouraged to consult with counsel to determine whether they are in compliance with the law.

KEY TERMS

Below are some terms provided for under PIPL:

Personal Information: The law defines personal information as "all information related to an identified or identifiable natural person."[1] This includes any personal information that can identify a natural person directly or in combination with other information.

Personal Information Handler: A "Personal Information Handler" under PIPL is similar to a "Controller" as used under the GDPR. The law specifically defines "handlers" as organizations and individuals that independently determine the processing purpose and method in personal information processing.[2]

COVERED ENTITIES

Article 3 of PIPL provides for the territorial scope of the law, which extends its application to processing outside of China, rather than solely within China. PIPL applies under the following circumstances:

1. ***Processing personal information within China***—As long as the processing takes place in China, the requirements set forth will apply. This is the case regardless of whether the processing is carried out by Chinese-based companies or affiliates of

1 PIPL, Article 4
2 PIPL, Article 73

multinational corporations that are located in China. Additionally, PIPL requirements will still apply, regardless of whether the organization is considered a data handler or a processor.

2. ***Extraterritorial effect—*** As written, PIPL applies to all processing outside of China where:
    a. it is for the purpose of providing products and services to natural persons in China;
    b. used to analyze/assess the behavior of natural persons in China; or
    c. other circumstances as provided by laws and administrative regulations.

Currently, PIPL provides limited guidance on how to evaluate each prong. It is likely China will adopt a regulatory perspective for clarity.

PRINCIPLES FOR DATA HANDLERS

Employers who may be classified as "Handlers" are expected to comply with the data processing principles set forth under PIPL. In order to lawfully process information, organizations should consider the following principles:

1. ***Lawfulness, Necessity, and Good Faith –*** Handlers shall ensure that personal information is not processed through misleading, fraudulent, or coercive manners. Additionally, similar to the data minimization principle under the GDPR, handlers should only collect information that is necessary under all processing activities. Finally, PIPL implements a "good faith principle" to ensure fairness in all personal information processing activities.[3]
2. ***Limited Purpose –*** All processing of personal information shall provide for a specific and legitimate purpose. Additionally, processing should be in a manner that is least impactful on personal rights and interests of data subjects.[4]
3. ***Transparency –*** Handlers shall disclose all rules for processing personal information. Additionally, the scope of processing shall be clearly stated.[5]
4. ***Accuracy –*** Under Article 8 of PIPL, quality of personal information shall be guaranteed and inaccuracies shall be avoided.
5. ***Accountability and Security –*** Handlers shall be responsible for processing and take effective measures to ensure security.[6]

CONDITIONS FOR LAWFUL PROCESSING

The PIPL takes an approach similar to the GDPR and provides multiple lawful basis for processing personal information. These lawful purposes[7] include:

- Data subject has provided consent in a voluntary manner;
- Processing is necessary for the conclusion or performance of a contract with the data subject;
- Processing is necessary for the performance of statutory duties or compliance with legal obligations;
- Processing is necessary for a public health emergency;
- Personal information has already been publically disclosed by the data subject;
- Processing is necessary for carrying out public activities for the public interest; and
- Other circumstances provided for by law and administrative regulations.

3 PIPL, Article 5
4 PIPL, Article 6
5 PIPL, Article 7
6 PIPL, Article 9
7 PIPL, Article 13 & 14

Processing of sensitive personal information requires strict protection measures and must provide for a separate consent with a specific purpose.

RIGHTS OF DATA SUBJECTS

Data subjects are provided certain rights under PIPL. Organizations should keep these rights in mind when responding to individual requests. Some of these rights include: *Right of knowledge, Decision, Restriction, Objection, and Recession; Right to Access, Copy, and Portability; Right to Rectification; and Right to Deletion.*

> *Handlers should note that where a lawful purpose for processing is specifically based on consent, the Handler must provide an easy way for the individual to withdraw consent and make this option clear to the data subject.*

DATA GOVERNANCE AND SECURITY

Handlers are required to have security measures in place to protect personal information and prevent unauthorized access. The law outlines several areas within the organization that Handlers should ensure are secure.

Appointing DPO/ Representative

Handlers are expected to appoint a data protection officer (DPO) if the processing of information reaches a certain volume that is prescribed by the State Internet and Communications Department.

PIPL Article 53 also implements a measure specific to Handlers processing information outside of China as stipulated under Article 3. Such handlers must establish an office or appoint a representative in China to handle matters related to PIPL. The name of the relevant institution or representative should be sent to the Department.

Audit[8]

An audit requirement is unusual for most regulations in China. Under PIPL, Handlers are required to conduct regular compliance audits on whether their personal information processing is compliant. Chinese authorities also have the right to request handlers to engage professional institutions for a compliance audit where the authorities discover high risks in processing activities.

Personal Information Protection Impact Assessment[9]

This requirement is similar to the "Data Protection Impact Assessment" set forth under the GDPR. Handlers have an obligation to conduct these assessments in certain situations which include:

- handling sensitive personal information;
- using personal information for automated decision-making;
- entrusting the processing of personal information, providing other handlers with personal information and publically disclosing personal information;
- transferring personal information overseas (this includes sharing information with a third-party vendor); and
- conducting other personal information processing activities that have a significant impact on individuals' rights.

Impact assessment reports should be kept for at least three years and should include:

- whether the purpose of processing personal information is lawful, justified, or necessary;
- the impact on the rights and interests of individuals and security risks; and

8 PIPL, Article 54
9 PIPL, Article 55 & 56

- whether the protective measures taken are lawful, effective, and commensurate with the degree of risk.

DATA TRANSFERS OUTSIDE OF CHINA

In order to transfer information outside of China, PIPL requires three conditions to first be met. These conditions require Handlers to:

> *(1) Obtain separate and informed consent from the data subject;*
> *(2) Conduct an impact assessment and make record;*
> *(3) Satisfy one of the four stated special conditions.*

The international data transfer requirements and restrictions are set forth under Articles 38-43.

Obtain Separate and Informed Consent[10]

Under PIPL, if a Handler provides personal information outside of China, the Handler must first obtain the data subject's individual consent to do so. Additionally, the Handler must also inform the subject of the name and contact details for the overseas transfer, purpose of processing, type of personal information that will be processed, and the procedure by which the individual may exercise his or her rights.

Conduct an Impact Assessment

Before conducting an overseas transfer, Handlers must assess the impact of certain processing activities involved in the transfer. The impact assessment should include:

- the legitimacy, justifiability, and necessity of the purpose;
- the impact on individuals' rights and interests and the degree of security risks; and
- whether the security protection measures taken are legitimate, effective, and appropriate to the degree of risks.

Satisfy a Special Condition[11]

A Handler will not be permitted to transfer personal information outside the territory of China unless the Handler expressly provides for a special condition. There are four conditions set forth under Article 38 that would allow for such transfers. Specifically, Article 38(3) allows information to be transferred outside of the Republic in order to fulfill a contract with an overseas recipient in accordance with the standard contract formulated by the state cyberspace and informatization department. It is likely that the standard contract requirements will be similar to the standard contractual clauses (SCCs) under the GDPR. However, as of the date of this publication, the department has yet to provide such standard contract requirements.

CONCLUSION

As stated, the provisions discussed above are not intended to be used as an official translation of the text.[12] With PIPL becoming effective early November 2021, it is essential for entities to review current practices that may involve data subjects in China or overseas data transfers.

Most importantly, with respect to ordering background checks,

> *clients should make sure to comply with all overseas transfer requirements set forth under PIPL Article 38 through 43.*

Other provisions under PIPL that clients should generally consider include individual rights and organizational obligations for processing and data protection. While some provisions are very similar to the GDPR and may already be in place, PIPL provides for other requirements organizations are expected to comply with.

10 PIPL, Article 39
11 PIPL, Article 38
12 The guidance set forth in this white paper was primarily obtained from Dentons Law resource on PIPL which can be accessed here.