The new Personal Information Protection Law (PIPL) of the People’s Republic of China (the PRC), which came into effect on 1 November 2021, is the country’s first comprehensive law in the area of personal information protection. The PIPL strengthens the existing data security and cybersecurity regulatory framework in the PRC by providing individuals in the PRC with a comprehensive set of rights in relation to their personal information.

In the context of cross-border investigations, while there appears to be a noticeable trend towards greater international sharing of information, it is still important for organisations to observe the restrictions on cross-border transfer of personal information, which local data privacy laws might have on such investigations, especially those with broad extraterritorial effect (e.g. the GDPR and the PIPL, as explained below). The reality of global investigations is that data is scattered across jurisdictions; each jurisdiction has its own laws on data protection or privacy which might potentially apply to the data per se and to the overseas transfer of such data. Such local data protection/privacy laws may, directly or indirectly, have an impact on international investigations.

This article seeks to provide an overview of the restrictions which the PIPL may have on cross-border data transfer and international investigations.

**Applicability of the PIPL**

As a starting point, it would be relevant to consider the applicability of the PIPL.

The PIPL applies to personal information processing by organisations operating within the PRC. Regardless of whether the processing of personal information is by a Chinese company or a local affiliate/branch of a multinational corporation (an MNC), it will be subject to the PIPL as long as it is based in the PRC.

For an organisation carrying out personal information processing activities outside of the PRC, the PIPL will apply to it where such activities are for: (a) the purpose of providing products or services to individuals in the PRC; (b) analysing or assessing the behaviour of individuals in the PRC; or (c) other circumstances as prescribed by law and regulations. In other words, the PIPL may potentially apply to an organisation processing personal information outside the PRC and based outside of the PRC. In this regard, it can be gleaned that the criteria for the extraterritorial reach of the PIPL is similar to the threshold tests of the GDPR.

For organisations based outside of the PRC, in the first instance, they should consider whether they are carrying out activities that might be caught within the scope of the PIPL (e.g. offering products/services to individuals in
The PIPL in Respect of International Investigations

**Legal bases for personal information processing**

When considering the potential impact of the PIPL on cross-border investigations, a key aspect would be to determine the legal ground for the processing of personal information as part of an investigation.

Apart from obtaining the individual’s consent, Article 13 of the PIPL adopts a similar approach to the GDPR by providing for other non-consent bases for the processing of personal information. One of the non-consent bases is where the processing would be necessary to fulfil "legal duties or obligations". It must be noted that there is presently no guidance on whether "legal duties or obligations" would include foreign legal duties or obligations, which an organisation may potentially need to comply with, in the situation of an international investigation. In light of this uncertainty, and out of an abundance of caution, an organisation might wish to consider relying on the consent basis in the context of a cross-border investigation. However, it needs to be aware that the individual may withdraw his or her consent to the organisation’s processing of his or her personal information, which could potentially affect ongoing investigations.

**Cross-border transfer**

In the course of an international investigation, it is arguably inevitable that there would be times where it would be necessary to transfer personal information outside the borders of the jurisdiction in question for the purpose of the investigation.

Under the PIPL, an organisation needs to fulfil certain conditions to transfer personal information outside the PRC. These conditions are: consent, performance of a personal information impact assessment, and meeting one of four criteria (one of which is the new PRC standard contractual clauses (SCCs) which is similar in principle to the GDPR’s SCCs).

In addition, the PIPL specifically allows the transfer of personal information outside the PRC in accordance with applicable international treaties and agreements, which the PRC has concluded or participated in.

On 29 October 2021 (3 days before the effective date of the PIPL), the Cyberspace Administration of China released draft guidelines for public consultation to assist organisations in their compliance with the PIPL’s cross-border transfer requirements (including the need for certain organisations to perform a security assessment prior to any cross-border data transfer).

While the draft guidelines do provide some practical operational detail on certain aspects of cross-border data transfer, there are parts which are not entirely clear. For instance, do the requirements cover remote access from overseas (which has become more mainstream amid the COVID-19 pandemic due to extensive remote working arrangements)? Is the security assessment to be performed on a per-transfer basis or a per-data controller basis? As this is simply a draft for consultation at this point, it is hoped that more clarity would be shed on these aspects.

**Data transfer to domestic regulators or enforcement agencies**

For transfers of personal information to domestic regulators or enforcement agencies within the PRC pursuant to specific laws or regulations, this is generally allowed under Article 13 of the PIPL, specifically, where the processing would be necessary to fulfil "legal duties or obligations", without the need to obtain the individual’s consent.

**Data transfer to foreign regulators or enforcement agencies**
Finally, and crucially, a notable cross-border data transfer restriction in the PIPL concerns overseas transfer to "foreign judicial or law enforcement agencies". Under Article 41 of the PIPL, an organisation may not provide personal information stored within the PRC to foreign judicial or law enforcement agencies without the approval of the relevant Chinese authorities. This provision is substantively similar to Article 36 of the PRC’s Data Security Law and Article 177 of the PRC’s revised Securities Law which prohibit an organisation or individual within the PRC to provide certain information to non-Chinese regulators and enforcement agencies.

Uncertainties remain in respect of Article 41 of the PIPL. First, the phrase “foreign judicial or law enforcement agencies” is not defined in the PIPL and could potentially be broadly interpreted to include not only foreign judicial organs but sectoral regulators (e.g. the United States Securities and Exchange Commission (SEC) and the UK Financial Conduct Authority (FCA)). Second, there is presently no guidance as to how the Chinese authorities’ approval under Article 41 of the PIPL may, in practice, be applied for by applicable organisations.

Overall, it can be seen from the above that the PIPL potentially has a significant impact on cross-border data transfer and global investigations. Organisations and their external counsels should be mindful of the potential implications the PIPL has on investigations and they should carry out careful advance planning to ensure compliance with the new law.

Should you have any query on compliance with the PIPL or require support on regulatory/investigations matters in the PRC, our team would be happy to assist. Please do not hesitate to contact Nicholas Lum or Zhen Guang Lam.

Authors:

Nicholas Lum
Partner

Zhen Guang Lam
Senior Associate

Themes:

Insurance & Reinsurance
Regulatory & Investigations