BCLP. Client Intelligent

Insights

CHINA'S DRAFT PERSONAL INFORMATION PROTECTION LAW: WHAT BUSINESSES SHOULD KNOW

Dec 02, 2020

SUMMARY

In October 2020, China unveiled its draft law on personal data protection. Once promulgated, this law is going to be the first comprehensive set of PRC laws on personal data protection. The draft law comes with provisions for extraterritorial application, clarifications as to definitions and hefty fines. This article will set out the key highlights of this set of draft laws.

The much-anticipated and long-awaited draft of the Personal Information Protection Law of the People's Republic of China[1] (the "draft PIPL") was released for public consultation on 21 October 2020. The consultation window closed on 19 November 2020.

The PIPL, once promulgated, will be China's first comprehensive set of laws targeted at addressing the problems with personal data leaks and hacks prevalent in the country. With the rapid growth in big data industries and the vast number of netizens in China, the PIPL is expected to play an important role in regulating the processing of personal data and combatting misuses of data collected.

At present, China's Cybersecurity Law ("CSL"), which came into force in 2017, governs the protection of personal information. The CSL has a focus on the protection of information in the cyberspace, the protection of "critical information infrastructure" and the regulation of "network operators". The PIPL is going to be a more comprehensive piece of law which governs more aspects of personal information protection.

Key Highlights of the draft PIPL

The draft PIPL comprises a total of eight Chapters with 70 Articles. Various aspects of the draft PIPL resemble the GDPR of the EU. Among other things, the draft PIPL sets out data protection principles, specific rules for the processing of both "personal information" and "sensitive personal information", the rights of individual data subjects and also penalties for breaches.

Below is a summary of what we consider to be key highlights of the draft PIPL:

(i) Extraterritorial application of the PIPL
(ii) More bases on which the handling of personal information is allowed
(iii) More rights and protections given to individuals
(iv) Regulation of the role of "personal information handlers"
(v) Data localisation and cross-border transfer of personal information
(vi) Fines up to RMB 50 million (US$7.5 million) or 5% of annual turnover. Unfortunately, there is no indication in the draft PIPL as to which of these sets a lower or upper limit. This clearly is an important matter that needs early clarification.

Extraterritorial application of the PIPL

PRC laws generally do not have extraterritorial effect. However, the draft PIPL will apply to the processing of personal information outside the borders of China if:

(i) The information in question relates to natural person(s) within the borders of China; and
(ii) The processing of such information falls within one of the circumstances below:

> (a) Where the purpose of the processing of personal information is to provide products or services to natural persons within the borders of China; or
> (b) Where the purpose is to analyse or assess the activities of natural persons within the borders of China; or
> (c) As required or provided for in laws or administrative regulations.

The assertion of extraterritorial application of the draft PIPL closely follows the GDPR of the EU. The effectiveness of any extraterritorial jurisdiction of the draft PIPL likely will have to be seen in the light of relevant enforcement rules and procedures. As a matter of prudent practice for the purpose of compliance with the PIPL, a non-PRC-based business establishment or organisation which has a presence in China or touches upon personal data of persons within the Chinese borders should appoint a data protection officer or representative in the PRC to oversee the handling of personal data.

More bases on which the handling of personal information is allowed

Under the CSL, consent of the individual is the only basis upon which personal information can be collected and processed. Personal information only can be collected when the relevant individual is informed and agrees to the aims and scope of the collection.

The CSL therefore is rather narrow.

The draft PIPL is expected to be welcomed because it provides alternative legal bases on which personal information can be collected and processed. Other than obtaining consent, personal information can be collected and handled in any one of the following circumstances:

(i) Where necessary for the entering into or performance of a contract to which the individual is a party;
(ii) Where necessary for compliance with duties or obligations prescribed by law;
(iii) Where necessary for responding to sudden public health incidents, or protecting the lives, health and property security of natural persons in cases of emergency;
(iv) The handling, within the parameters of reasonableness, of personal information in news reporting and scrutiny of public opinion for public interest; or
(v) Other circumstances prescribed by law or administrative regulations.

Although more legal bases now are being proposed, most of these legal bases do not appear to be of great assistance to businesses or organisations in the private sector. Most notably, unlike the GDPR, the draft PIPL does not allow collection or handling of personal information based on "legitimate interest", which is the most flexible basis available under the GDPR.

If a business establishment or organisation, or a "data information handler" (as will be discussed further below), tends to rely on the "legitimate interest" ground for its collection and processing of personal data under GDPR, it will need to be careful because it will have to consider if any of the alternative bases stated in the draft PIPL may be relied on. Otherwise, informed consent of the individual still has to be obtained.

More rights and protections given to individuals

The rules in the draft PIPL governing consent afford more protection to individuals. Generally, consent under the draft PIPL has to be well-informed, voluntary, and clear. It is revocable by the individual at will, and should be obtained from the individual in the event of any change in the purpose of handling, method of handling and the kind of information being handled. It expressly is provided that the refusal or revocation of consent cannot be a reason why the provision of products or services should be withheld from the individual.

The need to obtain consent from individuals also extends to the use of publicly available personal information, depending on how such information had been used at the time when it first became publicly available. If the intended use of publicly available information is not reasonably relevant to its original purposes, consent will have to be obtained.

Stand-alone consent will need to be obtained in relation to "sensitive personal information". "Sensitive personal information" under the draft PIPL is described as information which may cause discrimination to the individual or damage to the physical or property safety of the individual in the case of leakage or illegal use. Unlike the GDPR which sets out an exhaustive list of special categories of personal data, the list of "sensitive personal information" given under the draft PIPL is shorter than the corresponding list under the GDPR and is not exhaustive. It can cover a broader scope of personal information when compared to the GDPR, depending on how strictly or loosely this definition of "sensitive personal information" is going to be interpreted. When formulating data

policies, personal information handlers should be prepared to scrutinise the kinds of personal information being handled via the lens of the potential consequences if data security is compromised.

In addition, individuals also have rights to be informed. Matters which have to be communicated to the individuals include (but are not limited to) the following:

(i) The identity and contact information of the personal information handler;
(ii) Where data needs to be transferred by the personal information handler to a third party due to merger or demerger, the identity and contact information of such receiving third party;
(iii) The purpose and method of handling, the kinds of personal information being handled and the how long such personal information is kept;
(iv) The rights of the individual under the draft PIPL and the procedures involved in the exercise of such rights; and
(v) The necessity of the handling of sensitive personal information and the impact of such handling to the individual.

Notably, unlike the GDPR, the draft PIPL is silent on the timing of compliance with the requirements to inform individuals and obtain consent. However, it is implicit from the draft PIPL that the informing of individuals needs to be done in a timely manner.

Regulation of the role of "personal information handlers"

A "personal information handler" under the draft PIPL is defined to mean an organisation or individual which autonomously decides the purpose and manner of the handling of personal information.

Unlike the GDPR, the draft PIPL does not differentiate between a "data controller" and a "data processor". It would appear that the role of a "personal information handler" under the draft PIPL is more akin to a "data controller" under the GDPR. A "personal information handler" has the primary obligation under the draft PIPL to obtain consent from individuals and inform individual of the matters discussed above.

The draft PIPL refers also to "third parties" which receive personal information from "personal information handlers". Such receiving third parties are akin to "data processors" under the GDPR. In the event that a third party receives personal information from a "personal information handler", the individuals concerned should be informed of the identity and contact information of that receiving third party, in addition to the purpose, method of handling and the kinds of personal information being handled. Further and notably, where a third party receives anonymised information from a "personal information handler", the receiving third party expressly is prohibited from reconstituting or reconstructing such information using any technological means with a view to recovering the identities of the individuals.

Data localisation and cross-border transfer of personal information

The existing CSL provides localisation requirements for "critical information infrastructure operators" (also known as "CIIOs"). CIIOs are required to store personal information and important data gathered during their operations within the territory of the Chinese borders. Where overseas transmission of personal data is necessary, security assessments have to be conducted by China's cyberspace administration bodies and relevant departments of the State Council.

Under the draft PIPL, personal information prima facie still should be stored domestically within the territory of the Chinese borders. However, in necessary cases, data can be transmitted overseas if the personal information handler does one or more of the things below:

(i) Passes the security assessment conducted by the Cyberspace Administration of China ("CAC");
(ii) Obtains certification of data security by a professional body recognised by the CAC;
(iii) Enters into an agreement with the overseas receiving party which governs the rights and liabilities of the parties in ways consistent with the requirements under the draft PIPL; or
(iv) Satisfies other conditions required by law, administrative regulations or the CAC.

For business establishments which have existing policies in place to deal with the requirements under the GDPR, data controllers most likely have entered into data processing agreements with all their data processors. It appears that similar data processing agreements adapted to suit the requirements of the draft PIPL should enough to satisfy condition (iii) above.

If the amount of personal information processed by the "personal information handler" exceeds a certain amount to be designated by the CAC, the CAC security assessment will have to be passed before personal information can be transmitted overseas. Although the threshold for the triggering of the security assessment is yet to be determined by the CAC, the threshold amounts proposed in the draft Measures on Security Assessment of Cross-Border Transfer of Personal Information and Important Data[2] released in 2017 could be of reference value. Under those draft Measures, security assessments were to be conducted by the CAC where the outbound transfer of data involved personal information of over 500,000 individuals or where the data volume exceeds 1,000GB. The applicable thresholds for the PIPL (once implemented) may be along similar lines, but we will need to wait and see.

Fines up to RMB 50 million (US$7.5 million) or 5% of annual turnover

One of the reasons – although there are many - why the draft PIPL warrants the attention of and consideration by business establishments (even before the law formally is promulgated) is that it comes with hefty maximum penalties for infringements.

Both the draft PIPL and the GDPR come with two tiers of fines. However, they differ in some significant ways. Unlike the GDPR which sets out which obligations trigger which level of fines

when breached, the applicable level of fines under the draft PIPL very much is dependent on "seriousness" or "gravity" of the breach alone.

Under the draft PIPL, the penalty provision is triggered if a person or an organisation:
(i) handles personal information in breach of the rules set out in the draft PIPL; or
(ii) fails to take necessary protection measures required by law when handling personal information.

In normal circumstances, a person or organisation would face a maximum penalty of RMB 1M (approx. USD 152,000) if it refuses to rectify the breach after having been warned by the regulatory body.

If the breach is "serious", the person or organisation, amongst other sanctions such as suspension of business and/or cessation of operation permits and without first having to be warned by the regulatory body, would be subject to a fine up to RMB 50M (approx. USD 7.6M) or up to 5% of the total revenue of the preceding financial year[3].

The current edition of the draft PIPL does not elaborate on the meaning of a "serious" infringement of the law for this higher tier of fines to operate. Further and remarkably, it is not clear from the draft law whether the higher or lower of RMB 50M or 5% of the total revenue applies in the event of a "serious" infringement. It remains to be seen whether the PIPL would give us more clarity on its penalties when it officially is promulgated.

Managers and data protection officers also need to exercise and maintain heightened caution, because the draft PIPL expressly and separately penalises individuals who directly are involved in the relevant infringement.

Takeaway points for businesses

The draft PIPL has the obvious potential to be of great impact to business establishments because of its extraterritorial application and hefty fines. While businesses already may have policies in place to comply with the GDPR requirements of the EU, it is possible that those existing policies may not fully be able to address the compliance requirements required under and in respect of the draft PIPL.

In particular, consent will have to be obtained under the draft PIPL in situations where "legitimate interest" could have been relied upon under the GDPR. Cross-border transfer of personal data may be subject to the scrutiny of Chinese regulatory bodies. The operation of the penalty provision still is clouded with uncertainty.

Prudent businesses or "personal information handlers" should begin reviewing their policies and practices in preparation for this significant new law.

1 Name translated. See the official draft law in the original Chinese language at https://www.dataguidance.com/sites/default/files/china_draft_personal_data_law.pdf. The English translations of the provisions in the draft PIPL are provided only for the purpose of discussion in this article and are not official or formal translations. In case of conflict or discrepancy between the meanings of the English and Chinese terms, the Chinese official meaning prevails.

2 Name translated. See the official draft law in the original Chinese language at www.cac.gov.cn/2017-04/11/c_1120785691.htm.

3 See above: there is no indication in the draft PIPL as to which of these two sets a lower or upper limit.

RELATED CAPABILITIES

- Data Privacy & Security
- Corporate

MEET THE TEAM

Glenn Haley

Co-Author, Hong Kong SAR

glenn.haley@bclplaw.com
+852 3143 8450