BCLP. Client Intelligent

Insights

CHINA'S PIPL EXPLAINED AND INTERPRETED BY THE LAW MAKER

Oct 08, 2021

SUMMARY

China's new legislationon personal information protection ("PIPL") will come into force on 1 November 2021. Mr Yang Heqing, an official from the responsible law making commission, has given some helpful explanatory comments and an "authoritative interpretation" of the PIPL.

Yang's comments and interpretation provide a useful starting point for the public to understand which aspects of the law are the most significant and which might be expected to attract the most attention from the perspective of the law maker.

China's new PIPL is a piece of legislation which highlights the need for data subjects' knowledge and consent, said law expert Mr Yang Heqing. One day after the PIPL was passed, Yang issued explanatory comments which, according to what was reported by Legal Daily[1] and the Cyberspace Administration of China (CAC)[2], represented an "authoritative interpretation" of the law.

The PIPL aims at (i) detailing and refining the principles governing personal information protection and the rules surrounding the handling of personal information, (ii) clarifying the rights and responsibilities in relation to data handling, and (iii) improving the personal information protection regime as a whole.

Yang, an official with the Legislative Affairs Commission of the NPC Standing Committee, commented that "the PIPL will put into practice the maintenance, protection and development of the legal rights of the many people using the cyberspace. The law will increase the 'sense of gain, sense of happiness and sense of security'[3] of people in the light of the growth of digital economy."

Below is a brief discussion of the ten points highlighted by Yang.

Highlight No 1: Establishing personal information protection principles

Personal information protection principles form the basis of the collection and use of personal data. They act as the foundation for the formulation of specific personal information protection rules.

Yang said that the PIPL has taken reference from international experience and is rooted in the realities of the country. The new law establishes the following principles governing the handling of personal data:

- The handling of personal data is to be governed by principles of legality, appropriateness, necessity and integrity.
- The handling of personal data needs to be related directly to clear and reasonable purpose(s).
- Personal data is to be handled in ways which cause the minimum impact on personal rights.
- The handling of personal data is to be limited to the smallest extent required to fulfill its purpose(s).
- Data handling rules and policies are to be made available to the public.
- The quality of personal information collected and handled is to be guaranteed.
- Measures which safeguard and protect personal information must be implemented.

According to Yang, these principles must be observed in all processes and phases of personal information handling.

Highlight No 2: Regulating data handling in order to safeguard rights

The PIPL relates closely to the handling of personal data with a view to safeguarding personal information rights.

Yang indicated that “informed consent”, as the core of the personal information protection principles, is very important in safeguarding individuals’ right to know and the right to make decisions with regard to the handling of information belonging to them.

Under the PIPL, data handlers should obtain consent from individuals after having adequately informed them in respect of data handling activities. Where there are significant changes to the handling of data, the relevant individuals again should be informed before separate consents are obtained from them.

Yang further noted that the society has reacted strongly to issues such as blanket authorisations and compulsory consents. In the light of these issues, the PIPL specifically requires that separate consent is required for (i) the handling of Sensitive Personal Data, (ii) the provision of personal data

to third parties, (iii) the publication of personal data, and (iv) cross-border transfers of personal data.

Yang also stated that over-collection of personal data is prohibited under the PIPL. Data handlers will not be entitled to refuse to provide goods or services to individuals because the individuals refuse to give consent. The law will give individuals the right to revoke their consent. Upon revocation of consent, data handlers should stop processing the relevant data or delete the relevant data in a timely manner.

Having considered the complexities of the country's socio-economic situation and the ever-changing scenarios in data handling, the PIPL offers various alternatives to consent which will allow personal data to be handled legally. These alternatives have been designed from the perspective of safeguarding public interest and maintaining a normal way of living.

In addition, specific rules have been put in place to target (i) joint handling of data and (ii) the assignment of handling duties to third parties, both of which were said to be "rather prevalent in practice".

Highlight No 3: Banning price discrimination to the disadvantage of existing customers as enabled by big-data analysis. Regulating automated decision making processes.

Legal Daily reported that more and more enterprises make use of big-data analyses in assessing the personal traits of consumers for marketing purposes. Upon understanding information such as the consumers' financial statuses, spending habits and sensitivity to prices, some companies mislead and deceive customers by implementing differentiated treatments to customers in aspects such as prices. A typical example of such malpractices found in the society is the use of price discrimination to disadvantage existing customers.

Yang commented that the use of price discrimination based on big-data analyses is inconsistent with the principles of honesty and trust. It infringes consumers' rights to fair conditions of trade as provided by China's Consumer Rights Protection Law and therefore should be banned by law.

Against the above background, the PIPL provides that data handlers are to ensure that when using personal data, decisions made by automated processes are transparent, fair and just, with no unreasonable differentiated treatment to individuals in conditions of trade such as prices.

Highlight No 4: Protecting Sensitive Personal Data

The PIPL provides that information such as biometric data, religious beliefs, specific identities, medical health, finance account information and the records of a person's whereabouts are to be regarded as Sensitive Personal Data.

Sensitive Personal Data are to be handled only in the light of specific purposes and adequate necessity, under stringent protection measures. Impact assessments should be carried out before

the handling of such data. Individuals also have the right to be informed of the relevant necessity and how their personal rights are affected.

Yang indicated that more stringent restrictions in relation to Sensitive Personal Data were included within the PIPL, after having regard to the high likelihood of damage caused to an individual's personal dignity, personal safety and property safety, in the event of such data being leaked or used illegally.

Another noteworthy point is that personal information belonging to minors below the age of 14 also falls under Sensitive Personal Data. The PIPL will have to be read in conjunction with the Protection of Minors Law. Consent will need to be obtained from the parents or the guardian of the minor for the handling of such data.

Highlight No 5: Regulating how the State handles personal data

As reported by Legal Daily, national authorities need to handle an enormous amount of personal data for purposes such as maintaining national security, penalising criminals and managing socio-economic affairs. Accordingly, national authorities should bear the duty and responsibility of protecting personal information rights and security.

Legal Daily continued to report that, in recent years, some instances of personal data leakage demonstrated that some national authorities do not in fact have a sufficiently strong personal data protection mindset. There were no standardised procedures for the handling of personal data. Safety measures for personal data simply are not good enough, according to Legal Daily.

Against this background, the PIPL sets out specific rules for national authorities to handle personal data, with specific emphasis that the law also applies to national authorities. Data handling needs to be carried out in accordance with the law, administrative rules and procedures. It should not exceed the scope and extent necessary for the carrying out of statutory duties.

Highlight No 6: Providing adequate rights to individuals

Various of individual persons' rights to (i) know of how and what data are being handled, (ii) give consent, (iii) revoke consent, (iv) inquire about their data, (v) make copies of data, (vi) correct data, and (vii) delete data, have been consolidated and "upgraded" by the PIPL to become the right to know and the right to decide. The law makes it clear that individuals will have the right to set limits as to how their personal information is to be handled.

Meanwhile, the PIPL also makes provisions regarding the portability of personal data having regard to the realities of the multitude of services offered through the internet. The new law requires data handlers to provide to its data subjects mechanisms for the transfer of personal data which are compliant with conditions imposed by the Cyberspace Administration of China (CAC). It is hoped

that such requirements will address and satisfy the increasing need for cross-platform transfers of personal data.

Highlight No 7: Strengthening the duties required of data handlers

The PIPL emphasises that data handlers, as entities primarily responsible for the protection of personal data, are to take responsibility for their own data handling activities and must take necessary measures to protect the safety of personal data they handle.

On this basis, the PIPL sets out clear compliance regulations and the duties required of data handlers. Among other duties, data handlers are required to do the following:

- Devise internal management policies and set up operation plans.
- Take appropriate technical measures with regard to safety.
- Appoint persons-in-charge to monitor data handling activities.
- From time to time perform compliance audit with regard to data handling activities.
- Perform personal information impact assessments on high-risk activities such as the handling of Sensitive Personal Data, use of automated decision making processes, provision of personal data to third parties, and the publication of personal data.
- Comply with data leak notifications and remedial requirements.

Highlight No 8: Imposing special duties on large-scale internet platforms

Internet platform services are key features of the digital economy which sets it apart from traditional economy. Internet platforms host news release as well as providing a technical support and transaction forum for the transactions of goods and services.

Yang commented that internet platforms are key to personal information protection because they provide infrastructural technical services to platform operators who set basic rules with regard to data handling. He further pointed out that data handlers which provide important internet platform services, have a large number of users or have complex business operations have strong influential power over transactions and handling activities conducted in internet platforms. Therefore, greater power has to come with greater responsibilities.

Accordingly, the PIPL contains personal information protection responsibilities which specifically are targeted at large-scale internet platforms, including requirements to:

- Establish a comprehensive compliance regime for the protection of personal information;

- Set up an independent committee comprising mainly of external members to monitor the company's protection of personal data;
- Abide by principles of openness, fairness and justice in the setting up of platform rules;
- Stop providing services to product or service providers using the platform who have breached the law in significant ways; and
- Periodically publish social responsibility reports on the protection of personal information in order to be monitored by the public.

These rules are aimed at increasing the transparency of the operations of large-scale internet platforms and strengthening external monitoring. The aim is for the whole society to participate in China's personal information protection regime.

Highlight No 9: Regulating cross-border data movements

Legal Daily reported that cross-border transfers of personal information are becoming more and more frequent due to the development of digital economy and the increasing degree of openness of China to external economies. The risks that come with cross-border transfers of personal data are becoming more and more difficult to control in light of geographical distances, differences in national laws and discrepancies in protection levels.

"The PIPL establishes a clear and systematic set of rules for cross-border transfers of personal information in order to satisfy the objective needs to protect personal information rights and safety, as well as to adapt to the realities of international trade", said Yang.

On this issue, Yang specifically indicated five key points as set out below:

1. The PIPL applies to data handlers outside China which either provide products or services to natural persons located in China, or analyse or assess behaviours of natural persons located in China. Foreign data handlers which fall within the above description have to establish a special organisation or appoint a representative to take responsibility for matters relevant to the protection of personal information.
2. The PIPL provides the permitted ways by which personal data may be transferred out of China. These include security assessment by CAC, certification by professional bodies, the use of standard contract terms provided by the CAC, and other ways in accordance with international treaties to which China is a signatory.
3. Data handlers are required to take necessary measures to ensure that receiving parties located outside China handle personal data with a standard of protection that is on par with what the PIPL requires.

4. The requirement for informed consent is more stringent in the context of cross-border transfers. This is to protect individuals' right to know and the right to make decisions.

5. There are specific rules which aim to safeguard national autonomy, safety and development interest. For example, there are rules which require security assessments for cross-border transfers of personal information, allow the provision of personal information to foreign judiciary or law enforcement agencies, restrict cross-border transfers generally, and also sanction discriminatory measures demonstrated by foreign countries.

Highlight No 10: Fleshing out practices relating to the protection of personal information

Legal Daily's report made the point that personal data protection has a wide reach. The implementation of the actual relevant measures will depend upon a well-developed supervisory and enforcement regime.

Under the PIPL and in accordance with the realities of personal information protection work, the CAC and relevant authorities of the State Council of the PRC are to carry out and supervise personal information protection measures within their respective scope of duties. The PIPL also sets out responsibilities with regard to supervision and protection which include:

- Launching public education campaigns;
- Instructing the supervisory work relevant to the protection of personal information;
- Dealing with relevant complaints;
- Organising tests and assessments for "Apps"[4]; and
- Investigating and dealing with breaches of the law.

Furthermore, in order to strengthen the synergy between the supervision and enforcement of personal information protection, the PIPL also confirms the role of and sets out specific requirements for the CAC in the planning and coordination of personal information protection work.

BCLP comments and observation

On the face of Legal Daily's report, it is unclear whether the content set out under Highlights Nos 1 to 10 was all mentioned by Yang, or whether any part of it was added by the author of the report. Our reading is that all content set out under those ten highlights was attributable to Yang and fell within the "authoritative interpretation".

Yang's reported comments helpfully expanded on the socio-economic background against which certain of the PIPL's provisions have been designed and then pointed out the key relevant

requirements which are found in the PIPL. This will assist data users understand which areas are likely to be most frequently policed by the national authorities, so that appropriate and timely business plans can be implemented in advance of 1 November 2021.

Furthermore, Yang highlighted and explained the spirit and key principles behind the PIPL. This will assist data handlers in formulating their compliance policies in areas where some commentators might prefer that the PIPL provisions were clarified, or where there might be gaps which the law has not covered expressly.

---

1. China's state-owned newspaper under the supervision of the CCP's Central Commission for Political and legal Affairs.
2. The official news reports were made in the Chinese Language. This piece of news subsequently was summarised and reported in the English language by Xinhua News.
3. The phrase was first used by China's President Xi Jinping in the 19th Report of the CCP in 2017.
4. The news report contained no further explanation as to what "Apps" mean. From the context, we believe "Apps" would cover mobile applications and computer software.

RELATED CAPABILITIES

- Data Privacy & Security
- Corporate

MEET THE TEAM

Glenn Haley

Co-Author, Hong Kong SAR

glenn.haley@bclplaw.com
+852 3143 8450