BCLP. Client Intelligent

Insights

PART 2 OF 5: PIPL REQUIREMENTS AS SUPPLEMENTED BY OTHER RELEVANT LAWS, REGULATIONS AND INSTRUMENTS

Feb 17, 2022

INTRODUCTION

In Part 1 of this series, we identified ten key legal instruments forming part of China's current data protection law. These laws, regulations and legal instruments were identified in an Information Booklet[1] published by the Hong Kong Privacy Commissioner for Personal Data ("PCPD").

In the Information Booklet, the PCPD highlighted a number of key provisions under China's Personal Information Protection Law ("PIPL") and analysed them alongside similar provisions in other relevant legal instruments.

This present article (part 2 of the current series of 5 articles) briefly discusses how some of the key PIPL provisions compare against the parallel provisions in relevant legal instruments (other than the Personal Information Security Specifications ("PISS") which will be discussed separately in Part 3 of this series). Some useful examples from recent decided cases also are set out in brief to demonstrate how some PIPL provisions have been applied.

By way of five examples below, we will consider how the PIPL intersects with other laws and how some of the PIPL requirements were interpreted by the PRC courts.

(a) Definition of "personal information" ("PI") and examples

Under the PIPL, PI is information which "relate to" identified or identifiable individuals[2]. On the other hand, the Cybersecurity Law ("CSL") and the Civil Code define PI slightly differently. Under the CSL and the Civil Code, PI refers to pieces of information which individually or when combined with other information, makes a natural person identifiable.

Examples of PI as seen in the CSL and the Civil Code include the name, date of birth, ID number, biometric data, address, telephone number, email address, health data, and location data of an individual[3].

There is a relevant Decision of the Supreme People's Court regarding the applicable laws to civil cases involving the handling of personal information using face detection technology[4] (the "SPC's Decision" which further adds account password(s) and financial data to the above list.

The PCPD, in the Information Booklet, noted that China's definition of PI is wide, meaning that in practice China's data protection regime potentially has a wide reach and catchment.

(b) Basic principles of PI processing

A number of PIPL requirements or principles underpinning the processing of PI overlap with the CSL and the Civil Code in the following ways:

	PIPL	CSL (§§41-42)	Civil Code (§1035)
Data activity which needs to be kept to a minimum	Collection of PI (§6)	Handling or processing of PI	Handling or processing of PI
Requirement for direct relevance	The handling of PI must be directly related to clear and reasonable purposes (§6)	The Collection of PI must not extend to PI unrelated to the provision of service	Not mentioned
Requirement that the purpose, method and scope of PI handling must be clearly stated	Yes (§7)	Yes	Yes
Consent for PI handling	Consent is one of the seven legal bases upon which PI may be handled (§13)	Consent needs to be obtained for: - the collection of PI; - the use of PI; and - the provision of PI to third parties.	Consent needs to be obtained for the handling of PI, unless otherwise provided by laws or administrative regulations.

(c) The requirement for "separate" consent

The PIPL requires that "separate" consent be obtained from data subjects when:

- Providing PI to other data handlers (§23);
- Making PI available to the public (§25);
- Using PI collected in public places for purposes other than public security (§26);
- Handling sensitive PI (§29); or

- Transferring PI out of the PRC (§39).

The PIPL does not further specify what constitutes "separate" consent and how consents should be obtained in order to be considered "separate". The Supreme People's Court has provided written and oral indications which shed some light on what "separate consent" means. According to the SPC's Decision[5], if the handling of facial information is based upon the data subjects' consent, the data handler needs to obtain either (i) the separate consent of the data subjects, or (ii) the written consent of the data subjects in accordance with laws and regulations[6]. The Chairman of the Research Office (Civil Division) of the Supreme People's Court indicated to the press that "separate consents" from individuals for the handling of facial information cannot be obtained by means such as "wholesale" provision of information and requests for consents[7].

(d) Openness and transparency

The PIPL provides that certain specified information needs to be made known to individuals in a clear, accurate and prominent way, using language that is easy to understand[8]. However, the PIPL does not tell us what in practice would constitute clear, accurate and prominent language for the purpose of communicating such information.

The Intermediate People's Court of Zhongshan, Guangdong considered a similar issue in the context of a civil claim under China's Contract Law[9]. In the context of the user agreement of an online shopping platform, the Court ruled that the emboldening and underlining of specific terms was insufficient to alert consumers "by reasonable means". This was because consumers' attention easily could be distracted by the multitude of information displayed on the website. Data handlers should use measures suitable for each of their specific situations. For instance, consumers may be alerted by way of pop-up windows.

(e) Protection of minors

The protection of minors is a key element in China's data protection regime. Different pieces of legislation have different age thresholds in their definitions of "minors":

- The PIPL[10]: persons below the age of 14
- The Law on the Protection of Minors[11]: persons below the age of 18
- The Provisions on the Cyber Protection of Children's Personal Information[12]: persons below the age of 14

The PIPL regards PI belonging to minors as Sensitive PI which is subject to more stringent regulations[13]. A specific data policy needs to be devised for such Sensitive PI, and consent needs to be obtained from the parents or guardians of the minors for the handling of such PI[14].

The Law on the Protection of Minors provides specifically that minors and their parents or their guardians have the right to request that their PI be corrected or deleted upon request[15] and that this be

done in a timely manner.

The Provisions on the Cyber Protection of Children's Personal Information adds to the above by prescribing more stringent requirements for network operators, as follows:

- Specific rules and user agreements must be set up for the protection of children's PI. An officer needs to be appointed for the protection of children's PI[16].
- Children's guardians are to be informed in clear and prominent ways about the collection, use, transfer and/or disclosure of children's PI[17].
- Staff members and officers must be given the minimum possible level of authorisation and access in relation to children's PI. Approval must be obtained from the designated department or pre-authorised staff responsible for children's PI before other members of staff can be given access to children's PI. Technical safeguards also have to be put in place to prevent unlawful copying and downloading of children's PI[18].
- Before transferring children's PI to any third party, security assessments have to be carried out either internally or by an external organisation[19].

A company which operates a video-sharing mobile application was prosecuted by the Procuratorate of Yuhang District of Hangzhou in the Zhejiang Province for the following breaches of the Provisions on the Cyber Protection of Children's Personal Information:

i. That it failed to inform the parental guardians in clear and prominent ways when children create accounts;

ii. That it failed to obtain valid and express consents for the collection and storage of children's PI; and

iii. That it failed to carry out the specific protection measures required in relation to children's PI.

The case eventually was concluded by way of settlement. The defendant company agreed to implement remedial and compliance measures such as devising rules and user agreements for the protection of children's PI, as well as developing real-name verification procedures for children[20].

CONCLUDING REMARK

The above examples show that the PIPL must not be read in a vacuum. The PIPL may be used as an entry point, but due regard also must be given to other laws, regulations and legal instruments which touch upon this area. Data governance policies of data handlers should reflect the requirements set out in the array of relevant laws, regulations and instruments set out above, and be reviewed periodically to take on board new additions to and revisions of the law.

[1] Available on the website of the PCPD at: https://www.pcpd.org.hk/tc_chi/resources_centre/publications/books/files/pcpd_china_pipl_book2021.pdf

[2] §4 of PIPL.

[3] §76 of the CSL; §1034 of the Civil Code.

[4] Available (only in the Chinese language) on the website of the Supreme People's Court of the PRC.

[5] Available (only in the Chinese language) on the website of the Supreme People's Court of the PRC.

[6] §2(3) of the SPC's Decision.

[7] Available (only in the Chinese language) on the website of the Supreme People's Court of the PRC.

[8] §17 of PIPL.

[9] Case No: （2018）粤20民辖终680号

[10] §31 of PIPL.

[11] §2 of the Law on the Protection of Minors.

[12] §2 of the Provisions on the Cyber Protection of Children's Personal Information.

[13] §28 of PIPL.

[14] §31 of PIPL.

[15] §72 of the Law on the Protection of Minors.

[16] §8 of the Provisions on the Cyber Protection of Children's Personal Information.

[17] §9 of the Provisions on the Cyber Protection of Children's Personal Information.

[18] §15 of the Provisions on the Cyber Protection of Children's Personal Information.

[19] §17 of the Provisions on the Cyber Protection of Children's Personal Information.

[20] The official report of the case (in Chinese language only) is available at the website of the Supreme People's Procuratorate of the PRC at https://www.spp.gov.cn/spp/zdgz/202103/t20210317_512919.shtml.

RELATED CAPABILITIES

- Corporate
- Data Privacy & Security

MEET THE TEAM

Glenn Haley

Hong Kong SAR

glenn.haley@bclplaw.com
+852 3143 8450
