BCLP. Client Intelligent

Insights

PART 3 OF 5: THE PIPL AND THE PERSONAL INFORMATION SECURITY SPECIFICATION

Feb 18, 2022

INTRODUCTION

In Part 2 of this series, we discussed how the Personal Information Protection Law ("PIPL"), the centerpiece of China's personal information ("PI") protection law, needs to be read in conjunction with other relevant laws, regulations and instruments. Excluded from our previous article was the Personal Information Security Specification ("PISS"), which is an important ancillary legal document which deserves discussion in its own separate article.

The PISS was issued jointly by the State Administration for Market Supervision and the Standardization Administration of the PRC. The PISS lays out granular guidelines for the implementation of PI protection rules. In an Information Booklet[1] published by the Hong Kong's Privacy Commissioner for Personal Data ("PCPD") in November 2021, the PCPD took the view that the PISS is not a legally binding instrument in and of itself; however, the PISS likely will operate as an important reference document for monitoring authorities and enforcement agencies[2].

The PISS came into force before the PIPL. The PISS, technically therefore was not issued as a piece of supplementary legislation specifically intended to clarify the PIPL. However, there is a substantial degree of overlap in the topics addressed in these two documents, as identified in the PCPD's Information Booklet. These aspects of overlap are set out in the 12 broad areas discussed below:

BASIC PRINCIPLES OF PI PROCESSING

The PIPL requires data handlers to abide by the principles of lawfulness, justification, necessity and honesty[3]. §4 of the PISS provides more clarity as to what these broad principles mean in practice by elaborating on the following seven aspects:

- Balancing of rights and responsibilities. Controllers of PI are to take necessary measures to safeguard the security of PI and will be held accountable for any harm done to the legitimate interest of data subjects caused by their PI processing activities or practices.
- Clear purpose. Controllers of PI need to specify unequivocal, clear and specific purpose(s) for its PI processing activities.

- Informed Consent. Data subjects have the right to be informed explicitly of the purpose, method, scope and other rules for PI processing before giving their consent.
- Minimum necessity. Only the minimum amount of PI essential to meeting the purposes to which the data subjects have consented is to be processed. PI needs to be deleted once that purpose has been fulfilled.
- Data policies setting out the scope, purpose and rules for PI processing need to be made available to the public in a clear, understandable and reasonable manner.
- Controllers of PI need to possess security capabilities that match the potential security risks posed by their PI processing activities. Adequate administrative and technical measures are required to be put in place to protect the confidentiality, integrity, and availability of PI.
- Participation by data subjects. Data subjects need to be provided with channels to access, rectify and delete their PI. Data subjects also are to be given ways to withdraw their consent, de-register or to lodge complaints.

INFORMATION SECURITY MEASURES

The PIPL requires data handlers to take necessary measures to protect the safety of personal information they handle[4].

Common ways to minimise personal information risks include anonymisation, de-identification and pseudonymisation.

The PIPL highlights encryption and de-identification as possible security measures[5]. The PISS elaborates on this point by defining and explaining the term “de-identification”. According to the PISS, “de-identification” is the “technical process that makes data subjects unidentifiable or unassociated without the help of additional information”[6]. It maintains data granularity by using pseudonyms, encryption, hash functions and other technical means to replace personal identifiers.

PI STORAGE TIME LIMIT

The PIPL requires that PI is stored only for the minimum period of time necessary for the handling purpose[7]. The expiry of the minimum storage period, among other events[8], triggers the need for PI to be erased.

In addition to erasure, the PISS provides the alternative option of anonymising PI upon expiry of the minimum storage period[9]. Anonymisation differs from de-identification in that data subjects irreversibly are made unidentifiable and unassociated by the anonymisation process.

PERSONAL INFORMATION SECURITY IMPACT ASSESSMENT (“SIA”)

SIAs form an important part of a data handler's responsibilities under China's data protection regime. The PIPL and the PISS together provide a fuller picture as to when an SIA is needed and what an SIA needs to cover.

Based on the PIPL and the PISS, an SIA needs to be undertaken in the event of any of the following:

§55 of PIPL	ü The handling of sensitive PI ü Automated decision making based on PI (also §7.7 of PISS) ü The provision of PI to third parties ü Outbound cross-border transfer of PI ü The handling of PI significantly affects the personal rights of data subjects
§7.6(b) of PISS	ü When PI collected for different business purposes is merged or "fused" together
§9.1(b) of PISS	ü When entrusting data processing activities to third party processors
§9.2(a) of PISS	ü Before any share or transfer of PI not arising from acquisition, merger, reorganization or bankruptcy
§9.4(a) of PISS	ü Before publicly disclosing any PI as authorised by the law or with reasonable causes
§11.4(c) of PISS	ü Before the release of a product or service ü When there is a major change in business functions
§11.4(d) of PISS	ü When new legislative requirements come into effect ü When there is a major change in business model, information systems or operation environments ü When a significant PI security incident occurs

The PISS explains that an SIA mainly is to assess (i) the compliance of data handling activities with the basic principles of PI security, and (ii) the impacts of PI processing activities on the lawful rights and interests of PI Subjects[10].

Considering both the PIPL and the PISS, SIAs need to cover the following aspects:

§56 of PIPL	ü Whether the purpose and method of PI handling is legal, justified and necessary ü The impact on personal rights and security risks

	ü Whether security measures taken are legal, effective and proportionate to risk levels
§11.4(b) of PISS	ü Whether the collection of PI complies with the principles of explicit purposes, independent consent and minimum necessity ü Whether the handling activity may cause adverse impacts on the lawful rights and interests of data subjects ü The effectiveness of PI security measures ü Possible risks of anonymised or de-identified data sets becoming identifiable again ü Possible adverse impacts on the lawful rights of data subjects in respect of the sharing, transfer and public disclosure of PI ü Possible adverse impacts on the lawful rights of data subjects in the event of a security incident

DATA PROTECTION OFFICER

Data handlers who handle an amount of PI significant enough to reach the threshold imposed by the Cyberspace Administration of China ("CAC") are required by the PIPL to appoint data protection officers to monitor data handling activities and any security measures taken[11].

As of December 2021, the CAC has not announced any specific threshold for the purpose of the PIPL. The PISS, on the other hand, prescribes a number of more detailed requirements in respect of the appointment of data protection officer and a department dedicated to data security.

Notably, the PISS requires that a full-time data protection officer be appointed if any of the following thresholds is met:

- Data handling forms part of the main business of the data handler and the data handler has more than 200 employees;
- The data handler handles or expects to handle PI belonging to more than 1 million individuals; or
- The data handler handles sensitive PI belonging to more than 100,000 individuals.

APPOINTMENT OF THIRD PARTY DATA PROCESSORS

If a data handler wishes to engage third party data processors, the PIPL requires that such appointment or engagement be subject to the parties' agreement on a number of prescribed matters which enable the data handler to supervise processing activities carried out by the data processor[12].

The PISS expressly states that such supervision may be done by way of contracts or audits[13]. If the third party data processor fails to comply with the terms of engagement, the PISS imposes an additional requirement for the data handler immediately to implement remedial measures to control or eliminate the security risk[14].

SENSITIVE PI

The PIPL contains detailed prescriptions about the handling of sensitive PI[15]. Sensitive PI needs to be handled in the light of specific purposes and adequate necessity, as well as under stringent protection measures. Separate consent and SIA requirements also apply to sensitive PI.

The PISS supplements the PIPL by adding that security measures such as encryption need to be taken when transmitting and storing sensitive PI[16].

DATA BREACH NOTIFICATION

The PIPL requires that actual or potential data leaks be notified and remedied immediately[17].

The PISS contains more detailed prescriptions to supplement the PIPL requirements. Data subjects are to be notified by email, correspondence, telephone call, push notification or other means as appropriate. Where it is difficult for the affected data subjects to be notified individually, a notification may be made to the public in a reasonable and effective manner. Notifications must contain the following details:

- Details about the security incident and its impact;
- The measures which have been and/or will be taken in response;
- Recommendations to the affected data subjects as to how to prevent and minimise risks on their part;
- Remedial measures which have been and/or will be provided to the affected data subjects; and
- Contact information of the person and department in charge of PI protection.

CROSS-BORDER DATA TRANSFER

The PIPL restricts outbound data transfers of PI. In the Information Booklet, the PCPD indicates that the expression “outbound data transfers” means transmission of PI outside of Mainland China. The Information Booklet took reference from existing PRC laws and regulations[18] and deduced that a transfer of PI from Mainland China to Hong Kong would fall within the ambit of “cross-border data transfer”. This means that although not expressly stated in any legal instrument of direct relevance, PI transfers from Mainland China to Hong Kong most likely count as “cross-border data transfers” for the purpose of China’s data law.

In addition to the requirements for SIAs and separate consent, the PIPL requires a further level of safeguard – through the State - in the form of any of the following[19]:-

- Passing the CAC's security assessment;
- Obtaining PI protection certification from a professional body recognised by the CAC;
- Adopting the standard form agreement to be issued by the CAC when contracting with the receiving party; or
- Fulfilling other conditions imposed by other laws, regulations or the CAC.

It is mandatory for both (i) critical information infrastructure operators ("CIIOs") and (ii) data handlers who handle an amount of PI substantial enough to exceed the thresholds to be specified by the CAC, to pass the CAC's security assessment prior to any cross-border data transfer. According to the Law on the Security and Protection of Critical Information Infrastructure which came into force on 1 September 2021, "critical information infrastructure" refers to a non-exhaustive list of important industries such as public communication, energy, transport, water, finance, public services, electronic services and national defence.[20]

In the "Assessment Mechanism for Data Export Security (Consultation Draft)"[21] released in October 2021, the CAC proposed that security assessments need to be carried out by the CAC if any of the following criteria is satisfied:

- The PI and important data have been collected and produced by CIIOs;
- The data to be exported include important data;
- The data handler who seeks to export data handles PI belonging to more than 1 million individuals;
- The data handler has exported PI belonging to more than 100,000 individuals or sensitive PI belonging to more than 10,000 individuals in total; or
- Other situations as required by the CAC.

The consultation window for the "Assessment Mechanism for Data Export Security (Consultation Draft)" closed on 28 November 2021. The information provided in the Consultation Draft may be used by businesses as reference for compliance pending the formal publication of the document.

AUTOMATED DECISION MAKING

The PIPL defines "automated decision making" as the process under which a computer programme automatically analyses and assesses the behaviours, habits, preferences, finances, health or credit data of individuals, and then on the basis thereof makes decision[22].

- 24 of the PIPL prescribes a number of safeguards for consumers which apply specifically in situations involving automated decision making. For example, consumers need to be given the option to opt out from personalised marketing notifications arising from automated decision making processes. The PISS further requires a channel of complaint against the results of automated decision making processes and a procedure for manual review be provided to data subjects[23].

In addition, the PIPL requires an SIA to be carried out prior to the use of automated decision making[24]. The PISS clarifies that SIAs are required to be carried out at least once every year while automated decision making mechanisms are in use[25]. The PISS further requires effective protection measures to be implemented in response to the assessment results[26].

RIGHT OF ACCESS TO PI

The PIPL gives data subject the right to view and copy PI in the data handler's possession[27].

The PISS specifies the categories of information which need to be made accessible to data subjects:

- The PI or types of PI belonging to the data subject in the data handler's possession;
- The source of PI mentioned above;
- The purpose for which the PI mentioned above is used; and
- The identity or type of any third party who has obtained the PI mentioned above.

RIGHT TO DELETION OF PI

- 47 of the PIPL specifies the circumstances under which data handlers proactively are to delete PI in their possession (see above section on PI storage limit).

The duty to comply with data subjects' deletion requests extends also to third party data processors. The PISS provides that in the event of the data handler sharing PI with or transmitting PI to third parties in breach of the law or agreement with the data subject, the data subject has the right to request that such data be deleted[28].

CONCLUDING REMARK

The PIPL and the PISS go hand in hand in many broad areas. Although the PISS seemingly does not enjoy the same legal status as the PIPL, it offers much-needed clarity and specificity to the requirements set out in the PIPL. The PISS undoubtedly is a document which needs to be given due regard when businesses formulate their data governance policies and handle PI belonging to Chinese citizens.

---

[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] Ibid., at page 8.

[3] §5 of PIPL.

[4] §9 of PIPL.

[5] §51 of PIPL.

[6] §3.15 of PISS.

[7] §19 of PIPL.

[8] §47 of PIPL.

[9] §6.1 of PISS.

[10] §11.4(b) of PISS.

[11] §52 of PIPL.

[12] §21 of PIPL.

[13] §9.1(d) of PISS.

[14] §9.1(f) of PISS.

[15] §§28 to 31 of PIPL.

[16] §6.3(a) of PISS.

[17] §57 of PIPL.

[18] §89 of the PRC Exit and Entry Administration Law, and the Guidelines issued by the PRC State Taxation Administration on profits tax privileges for the Greater Bay Area. See page 35 of the booklet.

[19] §§38 and 39 of PIPL.

[20] §2 of the Law on the Security and Protection of Critical Information Infrastructure.

[21] http://www.cac.gov.cn/2021-10/29/c_1637102874600858.htm

[22] §73(2) of PIPL.

[23] §7.7(c) of PISS.

[24] §55 of PIPL.

[25] §7.7(b) of PISS.

[26] §7.7(a) of PISS.

[27] §45 of PIPL.

[28] §8.3 of PISS.

RELATED PRACTICE AREAS

- Corporate
- Data Privacy & Security

MEET THE TEAM

Glenn Haley

Hong Kong SAR

glenn.haley@bclplaw.com
+852 3143 8450

This material is not comprehensive, is for informational purposes only, and is not legal advice. Your use or receipt of this material does not create an attorney-client relationship between us. If you require legal advice, you should consult an attorney regarding your particular circumstances. The choice of a lawyer is an important decision and should not be based solely upon advertisements. This material may be “Attorney Advertising” under the ethics and professional rules of certain jurisdictions. For advertising purposes, St. Louis, Missouri, is designated BCLP’s principal office and Kathrine Dixon (kathrine.dixon@bclplaw.com) as the responsible attorney.