26 MAY 2020

PUBLIC CONSULTATION ON THE DRAFT PERSONAL DATA PROTECTION (AMENDMENT) BILL, INCLUDING RELATED AMENDMENTS TO THE SPAM CONTROL ACT

Submitted by Tan Tee Jim, SC

CONTACT DETAILS:

[Redacted]

Summary

1. In general, I welcome and support the proposed amendments in the draft Personal Data Protection (Amendment) Bill (the "**Draft Bill**").

2. My suggestions below relate to:

   (a) Specifying a time period in the proposed Section 26C for data intermediaries to notify the organisations (on whose behalf they process personal data) of a data breach;

   (b) Introducing further safeguards for the transmission of third party data under the new Data Portability Obligation in the proposed Section 26H; and

   (c) Amending the proposed new Sections 15(3) and 15(4) to clarify their scope.

3. I sincerely believe the suggestion will increase clarity, efficacy and the protection of third party rights.

Statement of Interest

4. The suggestions are submitted in my capacity as a member of the PDPA Appeal Board.

Comments & Suggestions

Mandatory data breach obligation

5. The proposed move towards a mandatory data breach notification regime is a positive step in enhancing organisational accountability. I have one suggestion in this regard.

6. Clause 12 of the Draft Bill proposes to introduce a new Section 26C (reproduced below for easy reference):

> "***Duty to conduct assessment of data breach***
>
> ***26C.****—(1) Subject to subsection (2),where an organisation has reason to believe that a data breach has occurred affecting personal data in its possession or under its control, the organisation must conduct, in a reasonable and expeditious manner, an assessment of whether the data breach is a notifiable data breach.*
>
> *(2) Where a data intermediary has reason to believe that a data breach has occurred in relation to personal data that the data intermediary is processing on behalf of and for the purposes of another organisation —*
>
> *(a)* ***the data intermediary must, without undue delay, notify the other organisation*** *of the occurrence of the data breach; and*
>
> *(b) the other organisation must, upon notification by the data intermediary, conduct an assessment of whether the data breach is a notifiable data breach in accordance with subsection (1).*
>
> *(3) The organisation must carry out the assessment mentioned in subsection (1) in accordance with any prescribed requirements*." (emphasis added)

7. It is trite that the damage caused to affected organisations by a serious data breach is often irreversible, serious and costly. Data intermediaries (such as cloud hosting service providers) are often the front line detectors of data breaches. Delays by them in notifying organisations of data breaches could seriously impede efforts to mitigate the damage caused by the data breaches.

8. Hence, I take the view that there should be a specified time within which a data intermediary must notify the affected organisation of the occurrence of a data breach. The term "undue delay" in the proposed Section 26C(2)(a) is inherently

vague. It can also be subjective, which is not desirable. My suggested amendments to the proposed provision appear in red below:

> "*(a) the data intermediary must, without undue delay but in any case no later than 3 days after the data intermediary has reason to believe that a data breach has occurred, notify the other organisation of the occurrence of the data breach*".

New Data Porting Obligation

9. Clause 13 of the Draft Bill provides for a proposed Section 26H, reproduced as follows:

> "***Transmission of personal data under data porting request***
> ***26H.****—(1) This section applies where giving effect to a data porting request in respect of applicable data about an individual (P) under section 26G(2) would transmit personal data about another individual (T) to a receiving organisation.*
>
> *(2) A porting organisation may disclose personal data about T to a receiving organisation without T's consent only if the data porting request —*
>
> *(a) is made in P's personal or domestic capacity; and*
> *(b) relates to P's user activity data or user-provided data.*
>
> *(3) A receiving organisation which receives from a porting organisation any personal data about T under subsection (1) must use that personal data only for the purpose of providing any goods or service to P.*"

10. As noted in [46] of the Public Consultation Paper issued by the MCI and PDPC on 14 May 2020, this essentially removes the transmitting organisation's obligation to obtain valid consent from a third party ("**T**") for the disclosure of his personal data insofar as the data porting request made by the requestor ("**P**"):

(a) was made in P's personal or domestic capacity; and

(b) relates to P's user activity data or user-provided data.

11. I acknowledge the need for a practical approach which does not impose on the disclosing organisation the duty to redact **all** personal data belonging to third parties.

12. However, to better protect the interests of third parties who might not have the opportunity to object to the disclosure of their personal data, the disclosure of third party data should only be allowed if the organisation determines that the third party does not have a right to privacy in a public place or that disclosure is unlikely to have an adverse impact on the third party. Thus, Section 26H should be amended to incorporate such conditions.

13. Alternatively, safeguards may be incorporated by

(a) stipulating a narrow scope of third party data categories allowed to be disclosed without the third party's consent when prescribing the 'whitelist' of data categories in the coming regulations; and/or

(b) introducing a blacklist to specify that certain data categories of third party data should not be disclosed without the third party's valid consent.

14. In my view, these safeguards are particularly necessary in situations where it is difficult to determine whether T has consented to P's disclosure of his/her personal data to the transmitting organisation in the first place.

Deemed consent

15. Clause 6 of the Draft Bill introduces two new situations in which an individual's consent may be deemed under the proposed Sections 15(3) and 15(4).

16. The sections provide for deemed consent in relation to the collection and use of personal data by B after the data was disclosed to it by A, but not in relation to the collection and use of personal data by C ("another organisation") after the data was disclosed to it by B. There seems to be a lack of symmetry. I would suggest amending the proposed Sections 15(3) and 15(4) by adding the amendments in red below:

> *"(3) Without limiting subsection (2) and subject to subsection (5), an individual (P) who provides personal data to an organisation (A) with a view to P entering into a contract with A is deemed to consent to the following:*
>
> *(a) the disclosure of that personal data by A to another organisation (B), where the disclosure is reasonably necessary for the conclusion of the contract between P and A;*
> *(b) the collection and use of that personal data by B, where the collection and use is reasonably necessary for the conclusion of the contract between P and A;*
> *(c) the disclosure of that personal data by B to another organisation (C) where the disclosure is reasonably necessary for the conclusion of the contract between P and A;*
> *(d) the collection and use of that personal data by the organisation (C), where the collection and use is reasonably necessary for the conclusion of the contract between P and A.*
>
> *(4) Without limiting subsection (2) and subject to subsection (5), an individual (P) who enters into a contract with an organisation (A) and provides personal data to A is deemed to consent to the following:*

(a) the disclosure of that personal data by A to another organisation (B), where the disclosure is reasonably necessary —

(i) for the performance of the contract between P and A; or

(ii) for the conclusion or performance of a contract between A and B which is entered into at P's request, or if a reasonable person would consider the contract to be in P's interest;

(b) the collection and use of that personal data by B, where the collection and use are reasonably necessary for any purpose mentioned in paragraph (a);

(c) the disclosure of that personal data by B to another organisation (C) where the disclosure is reasonably necessary for any purpose mentioned in paragraph (a);

(d) the collection and use of that personal data by the organisation (C), where the collection and use is reasonably necessary for any purpose mentioned in paragraph (a)."

Conclusion

17. I thank MCI and the PDPC for the opportunity to make the above suggestions. I hope they are useful.

Tan Tee Jim, SC
Lee & Lee
26 May 2020