AIA Singapore Private Limited

Public Consultation for the PDP (Amendment) Bill

Contact person:

Tan, Leann

Manager, Data Privacy & Awareness, Compliance

Leann.Tan@aia.com

Statement of interest

AIA Singapore Private Limited ("AIAS") would like to seek clarifications on the following items so that we can be better prepared for the implementation of Personal Data Protection (Amendment) Bill.

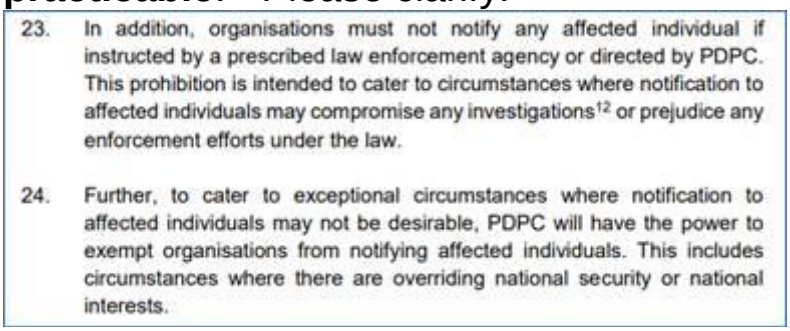
Summary of major points

1. Mandatory data breach notification
2. Changes to the Consent Framework
3. Data portability
4. Offences relating to egregious mishandling of personal data
5. PDPC's expanded enforcement powers

Comments

1) Mandatory data breach notification regime

i) the following 2 paragraphs (para 23 and 24) seem to imply that organisations should inform PDPC prior to informing the affected individuals. However, this seems to contradict with paragraph 20 which states that "Upon determining that a data breach meets the criteria for notifying affected individuals, the organisation must notify all affected individuals **as soon as practicable**." Please clarify.



23. In addition, organisations must not notify any affected individual if instructed by a prescribed law enforcement agency or directed by PDPC. This prohibition is intended to cater to circumstances where notification to affected individuals may compromise any investigations[12] or prejudice any enforcement efforts under the law.

24. Further, to cater to exceptional circumstances where notification to affected individuals may not be desirable, PDPC will have the power to exempt organisations from notifying affected individuals. This includes circumstances where there are overriding national security or national interests.

ii) The PDPC eService portal to report data breaches to PDPC, https://eservice.pdpc.gov.sg/case/db, states that the sectoral regulator may contact the Company to seek further information. Does this mean that once the data breach is reported to PDPC, the sectoral regulator (i.e. the Monetary Authority of Singapore, "MAS") will be informed as well? Do we need to separately notify MAS?

2) Changes to the Consent Framework

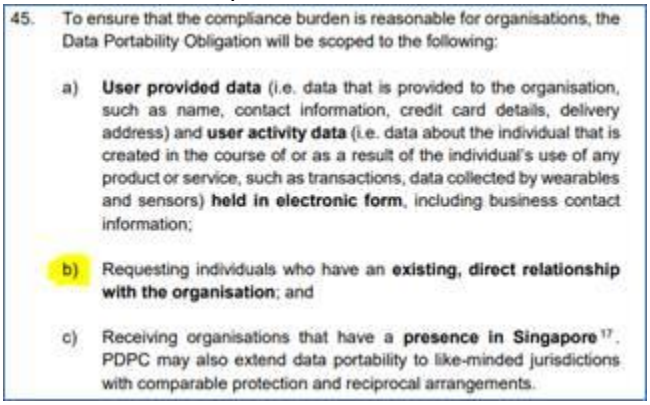
i) AIAS notes the expanded deemed consent by notification. There might be a scenario where the organisation has notified the individual via SMS or email and the individual is no longer using that mobile number or email address in the organisation's record and the individual did not update his contact details with the organisation. Should there be a complaint by the individual on the deemed consent by notification, can the organisation effectively argue that it had notified the individual and the individual should have ensured that his contact details are updated in the organisation's record?

ii) On meaningful consent, what is considered to be a "reasonable" period to opt out? Some guidance would be useful. Would the PDPC consider extending the scope of deemed consent or an opt out mechanism to the DNC regime?

iii) On business improvement exception, please confirm that this exception is limited to the use of the personal data only, and does not apply to disclosure to 3rd parties. If so, we would like to understand why this exception does not apply to disclosures.

3) Data Portability Obligation

i) section 45(b), in the context of an insurance company, does the 'requesting individuals who have an existing, direct relationship with the organisation' refer to Policyowners only, or does it include life assureds, beneficiaries, and etc



45. To ensure that the compliance burden is reasonable for organisations, the Data Portability Obligation will be scoped to the following:

a) **User provided data** (i.e. data that is provided to the organisation, such as name, contact information, credit card details, delivery address) and **user activity data** (i.e. data about the individual that is created in the course of or as a result of the individual's use of any product or service, such as transactions, data collected by wearables and sensors) **held in electronic form**, including business contact information;

b) Requesting individuals who have an **existing, direct relationship with the organisation**; and

c) Receiving organisations that have a **presence in Singapore**[17]. PDPC may also extend data portability to like-minded jurisdictions with comparable protection and reciprocal arrangements.

ii) Also on Data Portability, we understand that data obtained from 3rd party sources (for eg medical information) - not being "user provided data" - need not be transferred to a receiving organisation. Please let us know if this is not the case. Please clarify the amount of fees that may be charged – it would be helpful if a quantum or a ceiling may be prescribed or alternatively, the factors that may be taken into account in determining the quantum of fees chargeable.

4) On offences relating to egregious mishandling of personal data, it would be useful if the criteria/thresholds/definitions on what constitutes "knowing", "reckless", "legitimate interests" could be prescribed and clarified; and the degree of proof that is needed establish these. For example, does knowledge have to be actual, as opposed to constructive or imputed knowledge.

5) On PDPC's expanded enforcement powers, please consider if an express carve-out may be made for legally privileged communications, information and documents as well as the disclosure of the same by legal counsel (whether internal within an organisation or external).

Conclusion

The above comments for your consideration. Looking forward to your response.