PUBLIC CONSULTATION FOR THE PDP (AMENDMENT) BILL

SUBMISSION OF COMMENTS

Aviva Ltd
Contact Person: Jeremaine Yeo/Jasline Pang
Contact Email: jeremaine_yeo@aviva-asia.com / jasline_pang@aviva-asia.com

28/5/2020

Instruction on Submission of Comments:

Submission to: **DataRegulation@mci.gov.sg**
Format: Word Document
Subject header: **Public Consultation for the PDP (Amendment) Bill**

Comments	
Deemed Consent by notification:	
Section 15A(2)	Please clarify the intent for subsection 2 and what does the "prescribed purpose" referred to.
Section 15A(3)(a)	Suggest including a definition or examples of adverse effect as it is rather subjective.
Amendment of section 21:	
Section 10(d)(7)	Request for clarification. If the organization were to notify the individual of the exclusion of personal data or other information requested, it may result in the individual pursuing the disclosure of the personal data which may have the consequences mentioned in subsection (3). What is the intent for this clause and how does the notification of the exclusion of any personal data or other information requested going to be for the benefit of the individual if it has negative consequences. e.g. 'expected to threaten the safety or physical or mental health of an individual other than the individual who made the request' or 'cause immediate or grave harm to the safety or to the physical or mental health of the individual who made the request' Extract for reference *(2) An organisation is not required to provide an individual with the individual's personal data or other information under subsection (1) in respect of the matters specified in the Fifth Schedule.* *(3) An organisation shall not provide an individual with the individual's personal data or other information under subsection (1) if the provision of that personal data or other information, as the case may be, could reasonably be expected to —* *(a) threaten the safety or physical or mental health of an individual other than the individual who made the request;* *(b) cause immediate or grave harm to the safety or to the physical or mental health of the individual who made the request;* *(c) reveal personal data about another individual;* *(d) reveal the identity of an individual who has provided personal data about another individual and the individual providing the personal data does not consent to the disclosure of his identity; or* *(e) be contrary to the national interest*
Notifiable data breaches:	
Section 26B(1)(a)	We need more guidance on what "significant harm" refers to? Is a mere unauthorised disclosure considered to cause significant harm and the burden is on whom to show that "significant harm" is likely to be caused?
Section 26B(2)	The prescribed class of personal data needs to be provided and the varying treatment for each class. - Noted that in other jurisdictions, the prescribed categories of personal data likely to cause significant harm to individuals include medical history and health insurance information. We require guidance on how this would apply to the insurance industry.

Exceptions to the requirement to notify affected individuals:	
Section 26D(4)	We need more details to understand to what extent the remedial actions an organisation must take to fall under this exception.
Timeline to notify PDPC & affected individuals	
Section 26D(1)	Timeline to notify PDPC - Would also suggest that PDPC provides organisations with a form or template that such notification should take.
Section 26D(6)	What scenario does this falls in? When will the organization receive the instruction from the law enforcement agency or the commission? As the organization have as part of its normal process, prepare notification to PDPC and/or the affected individual. If there is an data incident, does it mean that an organization not required to notify the affected individual unless a prescribed law enforcement agency/the Commission directs the organization to do so? Suggest that some guidance/examples of when the Commission might waive our requirement to notify individuals.
Section 26D(7)	Suggest that some guidance/examples be given on the type of conditions to be imposed by the Commission?
Data portability (Part VIB)	
-	Data portability in the insurance context: - In the insurance context, the distinction between "user activity data" and "derived personal data" may not be as clear. For instance, which category would claims history fall under? If it falls under "user activity data", then it will be subject to a data portability request whereas it would be excluded from such a request if it is seen as "derived personal data". - Guidance would be needed when prescribing the 'whitelist' of data categories that data portability will apply to.
Legitimate interest exception to requirement for consent	
-	We commend the new exceptions added, but would like to have more clarity on how 'legitimate interests' can be ascertained.

Conclusion

We agree with PDPC and MCI that the PDPA needs to be reviewed to ensure it keeps pace with the evolving technology and business landscape, while providing for effective protection of personal data in the digital economy. However, we would like to seek clarification on the above mentioned items. Thank you.