PUBLIC CONSULTATION FOR APPROACHES TO MANAGING PERSONAL DATA IN THE DIGITAL ECONOMY (Issued 27 July 2017)

SUBMISSION OF COMMENTS

Aviva Ltd - Information Governance Working Committee
Contact Persons: Jasline Pang / Kartini Ashari
Title: Manager / Senior Executive
Contact Emails: Jasline_pang@aviva-asia.com / Kartini_ashari@aviva-asia.com

9/15/2017

Instruction on Submission of Comments:

Submission to: **corporate@pdpc.gov.sg**
Format: Word Document
Subject header: "**PDPC's Public Consultation on Approaches to Managing Personal Data in the Digital Economy**".

Reference Document:

public-consult-manag
ing-pd-digital-econom

Clarifications Required on the CP

Paragraphs from the CP Requiring Clarification	Questions / Proposals
PART II: ENHANCED FRAMEWORK FOR COLLECTION, USE AND DISCLOSURE OF PERSONAL DATA	
3.8 PDPC considers that notifying individuals of the purpose ("**Notification of Purpose**") can be an appropriate basis for an organisation to collect, use and disclose personal data where it is impractical to obtain consent. Notification provides a way of ensuring individuals retain some measure of control over their personal data in such circumstances. PDPC is thus considering providing for Notification of Purpose as a basis (that is not tied to the consent requirement) for collecting, using and disclosing personal data under the PDPA, subject to the following conditions: a) it is **impractical for the organisation to obtain consent** (and deemed consent does not apply); and	**(1) Business would like to seek clarification what or when is it deemed "impractical"?**
b) the collection, use or disclosure of personal data is **not expected to have any adverse impact on the individuals**. This includes ensuring the personal data will not be used to make a decision about the individual that may have an adverse impact on the individual, or to circumvent a prior withdrawal of consent (e.g. target the individual for direct marketing after he had opted out of receiving marketing communications).	**(2) Business would like to seek clarification on what is "adverse impact".**
3.9 PDPC proposes for organisations that wish to rely on this approach to provide **appropriate notification**11 of the purpose of the collection, use or disclosure of the personal data, and where it is feasible for the organisation to allow individuals to opt out of the collection, use or disclosure, information about how individuals may opt out. PDPC does not intend to prescribe how organisations are to notify individuals, but will leave it to organisations to assess and determine the most appropriate form of notification to ensure the individuals are made aware of the purpose of the collection, use and disclosure of their personal data.	**(3) As individuals may "opt out", is there a duration for this appropriate notification, (eg on the website or other modes of notifications).** **(4) If yes, what is the recommended duration?**
3.10 PDPC also proposes that organisations must assess if there are any risks or impact to the individuals from the collection, use or disclosure of personal data. Organisations will therefore be required to conduct a **risk and impact assessment**, such as a data protection impact assessment ("DPIA"), and put in place measures to mitigate the risks when relying on Notification of Purpose to collect, use or disclose personal data.	**(5) What is the definition/criteria/method of the Risk and Impact Assessment?** **(6) Is the "risk" only of the individual's or if there are others? Can we seek clarification please?**
3.15 To cater to such circumstances, PDPC proposes to provide for the collection, use or disclosure of personal data without consent where it is necessary for a legal or business purpose ("**Legal or Business Purpose**"). In addition, PDPC considers that it may not be meaningful to notify individuals of the collection, use or disclosure for a Legal or Business Purpose since the individual may not withdraw consent. PDPC is therefore proposing not to subject organisations to the requirement to notify individuals of the purposes when collecting, using or disclosing personal data in these circumstances. The proposed Legal or Business Purpose would be subject to the following conditions: a) it is **not desirable or appropriate to obtain consent** from the individual for the purpose; and b) the **benefits to the public (or a section thereof) clearly outweigh any**	**(7) Can we seek clarification on what is considered** **"not desirable or appropriate to obtain consent"? and** **"benefits to the public (or a section thereof) clearly outweigh any adverse impact or risks to the individual"?**

adverse impact or risks to the individual.	
PART III: MANDATORY DATA BREACH NOTIFICATION	
Criteria for Breach Notification 6.2 The PDPC proposes to adopt the following criteria for notification to affected individuals and/or PDPC of a data breach: a) **Risk of impact or harm to affected individuals** – Organisations must notify affected individuals and PDPC of a data breach that poses any risk of impact or harm to the affected individuals34. For instance, a data breach that involves personal data such as NRIC number, health information, *financial information* or passwords would be considered to pose a risk of impact or harm to the affected individuals. Notifying affected individuals will enable them to take the necessary steps to protect themselves from the risks or impact from the data breach.	**(8) What if the customer is fine with a data breach or loss and it has no impact from on him or from his point of view?** **(9) Does "Financial Information" here also include insurance coverage or premiums or only other financial information such as source of wealth, bank/salary information, payment details, etc?**
6.13 Where a data breach meets the criteria for notifying PDPC under the PDPA, PDPC proposes to require that the organisation **notifies the PDPC as soon as practicable, no later than 72 hours from the time it is aware of the data breach**. For breach notifications to PDPC, prescribing a cap of 72 hours43 provides clarity for organisations as to the definitive time by which they would have to notify PDPC, and they may provide the PDPC with relevant information that is available to the organisation at the time of notification. In addition, if that data breach also meets the criteria for notifying affected individuals under the PDPA, the organisation must ensure it notifies the affected individuals as soon as practicable. *Question 8: What are your views on the proposed time frames for data breach notifications to affected individuals and to PDPC?*	**(10) Is the 72 hours from when a breach is *established by the Business,* or as long as there is an incident?** **(11) Business would like to propose it to be 5 business days instead of 72 hours.**
Obligations of Data Intermediary 6.6 Where the organisation's data intermediary ("DI")37 experiences a data breach, PDPC proposes that **the DI be required to <u>immediately</u> inform the organisation** that it processes the personal data on behalf and for the purposes of, regardless of the risk of harm or scale of impact of the data breach. The organisation will be responsible38 for complying with the breach notification requirements under the PDPA.	**(12) What is "immediate"? Business would like to propose it to be 3 working days**