5 October 2017

To: Personal Data Protection Commission

Re: Submission of feedback for Public Consultation on Approaches to Managing Personal Data in the Digital Economy

With reference to the public consultation on Approaches to Managing Personal Data in the Digital Economy issued on 27 July 2017, comments from Manulife (Singapore) Pte Ltd are as follows:

Question / paragraph from Public Consultation	Our comments
Question 1: Should the PDPA provide for Notification of Purpose as a basis for collecting, using and disclosing personal data without consent?	1. In order to rely on this approach, a risk and impact assessment must be conducted. Will PDPC be issuing a guideline on the risk and impact assessment? 2. Also, is the risk and impact assessment required for each new activity? For example, conducting analytics for age group 20 to 25 in Sep 2017 and another new analysis for age group 20 to 30 in Nov 2017. As some of the personal data are used in both analyses, do we need to conduct a new risk and impact assessment and notification to them? 3. We do agree that a notification of purpose can be appropriate. However, on the appropriate notification, PDPC's view is to allow individuals to opt out if feasible. Will PDPC be providing guidelines on the type of situations, an opt-out must be given to individuals? 4. Will PDPC be providing further guidelines/definition of "impractical" and "adverse impact"? 5. Are we allowed to use these individuals' personal data before sending out the notification? If not, will there be a specific number of advance notification required? (i.e.: 30 days before we start using their personal data)
Question 2: Should the proposed Notification of Purpose approach be subject to conditions? If so, what are your views on the proposed conditions (i.e., impractical to obtain consent and not expected to have any adverse impact on the individual)?	1. Yes. It should be subject to conditions to avoid abusive of notification. 2. The conditions are reasonable. But we would propose to have more guidance and examples on these conditions.
Question 3: Should the PDPA provide for Legal or Business Purpose as a basis for collecting, using and disclosing personal data without consent and notification?	1. Will PDPC be issuing a guideline on the risk and impact assessment? 2. Will PDPC be providing guidelines in determining if an activity is considered as legal or business purpose? 3. Yes. We are agreeable that for legal or business purpose, the consent and notification are not required.

Question / paragraph from Public Consultation	Our comments
Question 4: Should the proposed Legal or Business Purpose approach be subject to conditions? If so, what are your views on the proposed conditions (i.e., not desirable or appropriate to obtain consent and benefits to the public clearly outweigh any adverse impact or risks to the individual)?	1. Yes. To avoid abusive of the system. 2. The conditions are reasonable. However, the conditions on "not desirable or appropriate" and "clearly outweigh" are debatable. Will PDPC providing any guidance/examples/definitions? 3. For the proposed Legal or Business Purpose, are both conditions have to be fulfilled?
Question 5: What are your views on the proposed criteria for data breach notification to affected individuals and to PDPC? Specifically, what are your views on the proposed number of affected individuals (i.e., 500 or more) for a data breach to be considered of a significant scale to be notified to PDPC?	1. We agreed to the proposed number of 500 or more affected individuals. We are more inclined to have a specific number of affected individuals rather than leaving for FI to decide. 2. For clarity, in 1 privacy incident, there could be more than 1 name been compromised. Example: In the application form, there are 2 individuals stated (1 policyowner and 1 life insured), will PDPC count this as 2 affected individuals? If there is assignee form with another new name, will this be counted as a 3rd affected individual? 3. We would like to clarify the definition of "affected individual". Does it refer to only individual whose personal data has been compromised?
Question 6: What are your views on the proposed concurrent application of PDPA's data breach notification requirements with that of other laws and sectoral regulations?	1. We are agreeable. No further comments.
Question 7: What are your views on the proposed exceptions and exemptions from the data breach notification requirements?	1. In paragraph 6.6, PDPC proposes that the Data Intermediary be required to immediately inform the organisation if DI experiences a data breach. The organisation is responsible for complying with the breach notification requirements. 2. As the requirement on "immediately" is debatable and the penalty for late /not notify to PDPC is on the organisation and not DI, Will PDPC mandate a specific turnaround days/time? 3. On part 1 of the exception, do Company have to wait for the law enforcement agency's written direction whether to notify affected individuals? Or Company can make their own assessment? 4. On part 2 of exception, what does "breached personal data is encrypted to a reasonable standard" refers? Will PDPC be providing further guidelines on reasonable standard?

Question / paragraph from Public Consultation	Our comments
Question 8: What are your views on the proposed time frames for data breach notifications to affected individuals and to PDPC?	1. Organisation has to notify PDPC as soon as practicable, not later than 72 hours from the time it is aware of the data breach. For clarity, the 72 hours are business hours or calendar hours? Reason being Incident could happen in Friday and may be impossible to notify PDPC on Sunday if the 72 hours refer to calendar days. 2. For clarity, does the 72 hours start from the time Organisation (1) suspects a potential data breach or (2) established that a data breach has indeed occurred?
Paragraph 6.6 Where the organisation's data intermediary ("DI") experiences a data breach, PDPC proposes that the DI be required to immediately 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 responsible for complying with the breach notification requirements under the PDPA.	1. On the last sentence "The organisation will be responsible for complying with the breach notification requirements under the PDPA", if it is the intermediary that breached the requirements, our views are that they should be responsible to report to the PDPC directly rather than the engaged organisation.

Particulars of Insurer and contact person:

- Company Name: Manulife (Singapore) Pte. Ltd.
- Address of Company: 51 Bras Basah, Manulife Centre #09-00 Singapore 189554
- Contact Person: Teo AiLing (Ai_Ling_Teo@manulife.com)

In general, we are supportive of the proposed enhancements to the framework. However, it would be beneficial to the organisations if PDPC could provide additional advisory guidelines before the implementation of the above points.

Please feel free to contact us if you need clarification on our comments.

Thank you.