RESPONSE TO CONSULTATION PAPER

Consultation Topic	PDPC's Public Consultation on Approaches to Managing Personal Data in the Digital Economy
Name/Organisation:	Alex Luong Man-Sung / Grace Tan Peishan Great Eastern Life Assurance Co Ltd Great Eastern General Insurance Limited
Contact number for any clarifications:	6248 2796 / 6248 2529
Email address for any clarifications:	AlexLuongM@greateasternlife.com GraceTanP@greateasternlife.com

General Comments

With reference to specific sections/paragraphs	Remarks
Paragraph 5.2 To strengthen protection for individuals and build confidence in organisations' management and protection of personal data, PDPC is proposing to introduce a mandatory data breach notification regime under the PDPA. **Paragraph 5.3** With mandatory data breach notification, affected individuals who are notified of the data breach will have the opportunity to take steps to protect themselves from the risks or impact from the data breach while affected organisations will be able to receive guidance from PDPC on post-breach remedial actions when they notify PDPC. Overall, this will enable PDPC to better oversee the level of incidences and management of data breaches at the national level. ***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?***	In the event of data breach, mandatory data breach notification should exclude: 1. Corporate policies under General Insurance 2. Corporate policies under Group Insurance 3. Ex-policyholders For corporate policies under General Insurance, insurers may not have direct contact information on corporate clients' insured parties (such as individual employees). Moreover, there will be movements in the corporate accounts whereby the individual employees may no longer be with the company. For corporate policies under Group Insurance, accounts may cover dependents of employees where there will be no record of direct contacts. For ex-policyholders, there is likelihood for contact information to be outdated. Contacting the affected individuals will be on a best effort basis given the constraints as mentioned under item 1 to 3.
Paragraph 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 individuals[34]. For instance, a data breach that involves personal data such as NRIC number, health information, financial information or passwords would be considered	On mandatory data breach notification, understand that PDPC will develop and issue guidelines to provide guidance to organisations on assessing risk of impact or harm to affected individuals. The benchmark on assessment of risk impact/harm should consider being specific on what constitutes to impact or harm individuals. As such, there should be guidance to what may be the specific measurement of risk level to determine the seriousness and materiality of risk level that will impact/harm affected individuals.

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. b) **Significant scale of breach** – Organisations must notify PDPC where the scale of the data breach is significant, even if the breach does not pose any risk of impact or harm to the affected individuals. PDPC is proposing for a data breach involving 500 or more affected individuals to be considered of a significant scale that would need to be notified to the PDPC[35] . Data breaches of a significant scale could indicate a systemic issue within the organisation, which may require PDPC's further investigation and guidance to the organisation on implementing the appropriate remedial actions to address it. ***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?***	