RESPONSE TO CONSULTATION PAPER

Consultation Topic:	Public Consultation For Approaches To Managing Personal Data In The Digital Economy (issued 27 July 2017)
Organisation:	Tokio Marine Life Insurance Singapore Ltd.
Contact number for any clarifications:	6592 5707
Email address for any clarifications:	Henry.Koh@tokiomarine-life.sg

S/N	Questions:	Feedback:
1	Should the PDPA provide for Notification of Purpose as a basis for collecting, using and disclosing personal data without consent?	Although this is a practical approach, PDPC should provide more specific guidelines or principles to help companies implement it within the spirit and intent of the PDPA, and avoid possible misinterpretation or abuse. While we understand PDPC's rationale and intention not to take a prescriptive approach on this, we are of the view that leaving it solely to organizations may have the unintended consequence of differing standards being developed amongst companies and creating some confusion for customers. A sample DPIA or guidance on how to conduct a Risk and Impact Assessment on data protection will also help smaller companies carry this out.
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)?	We agree that some conditions should be applied, and what has been proposed suffice from a high level perspective. However, more detailed examples and clarification how what constitutes "adverse" will help companies adhere to certain norms and expectations.
3	Should the PDPA provide for Legal or Business Purpose as a basis for collecting, using and disclosing personal data without consent and notification?	We agree with the approach. As suggested in #1 above, more examples and perhaps elaboration of what should not qualify under "business purpose" will help mitigate potential abuse of the provision.
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	We agree that some conditions should be applied, and what has been proposed suffice from a high level perspective. As with #2 above, useful tips on what constitutes "clearly outweigh" will help companies put in place the proper processes and assessment criteria to comply with the requirements.

	to obtain consent and benefits to the public clearly outweigh any adverse impact or risks to the individual)?	
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?	The proposed approach is sensible and provides customers with some safeguards. However, instead of specifying an absolute amount (e.g. 500 or more), PDPC may wish to consider allowing companies to take a risk-based approach. This is because for small companies, 500 may be more than 50% of their customer base, while for large companies, it may be <1%. In addition, there are other factors, e.g. confidentiality and sensitivity of the information, that should be considered, and companies can then assess the impact better and report to PDPC accordingly.
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?	We agree with the approach. We propose that PDPC's approach in para 6.3 a) of the consultation paper be similarly reflected in the final revised regulations or guidance, to explicitly clarify that by copying PDPC concurrently with a reporting to the sectoral regulator (per the sectoral regulator's reporting requirements) would satisfy PDPC's breach notification requirements.
7	What are your views on the proposed exceptions and exemptions from the data breach notification requirements?	We agree with the approach. However, the general criteria for exceptions and exemptions should be made known, and cases should be published for better awareness, unless there are extenuating reasons not to do so (e.g. national security purposes). Reference to Para 6.6 where it states that "PDPC proposes that the DI be required to ***immediately*** inform the organisation…", we propose to change the requirement to "DI be required to inform the organization **without undue delay upon discovery**." To be more pragmatic on the reporting requirement, while still emphasizing the need and urgency for the DI to inform the organization.
8	What are your views on the proposed time frames for data breach notifications to affected individuals and to PDPC?	We agree with the proposed time frames.

Conclusion	We would appreciate if PDPC is able to provide more specific guidelines or principles to help companies implement the act so that standards can be aligned to prevent possible misinterpretation or abuse.

	In addition, we would like to suggest that a sunrise period of 6-12 months be provided (i.e. before the revised Act come into effect). This will definitely aid companies in preparing themselves to meet the new requirements, such as making necessary changes to their existing third-party contracts or agreements.