RESPONSE OF

Tokio Marine Life Insurance Singapore Ltd.
20 McCallum Street #07-01 Tokio Marine Centre Singapore 069046

Contact Details of Data Protection Officer	
Name	Henry Koh
Designation	Head of Compliance
Contact	6592 5707
Email	Henry.Koh@tokiomarine-life.sg
Date	28 May 2020

Summary of Major Points

The comments herein are pertaining to "Part VIA – Notification of Data Breaches" and "Part VIB – Data Portability" of the PDP Amendment Bill.

Firstly, we would like to clarify on the interplay between Sections 26D(2) and (6) – Duty to notify occurrence of notifiable data breach.

Secondly, we would like to clarify if there would be an elaboration of requirements in the event of the occurrence of a notifiable data breach.

Lastly, with regards to porting of applicable data, we would like to clarify if the definition of "*excluded class of applicable data prescribed*" will be included.

Statement of Interest

Based on the 3 questions below, our interest is on clarification of scope and definition of certain terminology.

Comments

1. Notification of data breach to affected individual and PDPC – Section 26D(2) and (6):

   Under paragraph 20 of the consultation paper, it is explained that organizations are permitted to notify PDPC of a data breach which meets the criteria for notification **at the same time** as affected individuals are notified. However, paragraph 23 goes on to add that organizations must not notify any affected individual if so instructed by a law enforcement agency or the PDPC.

   If an organization notifies the PDPC at the same time as the affected individuals, and the organization is subsequently instructed by the PDPC that such affected individuals are subjects of investigations and should not be notified, would organizations be held liable for failing to comply with section 26D(6) of the revised PDPA? It would be helpful for the PDPC to clarify the interplay between sections 26D(2) and 26D(6) of revised PDPA.

2. Duty to notify occurrence of notifiable data breach - 26(D)(2):

   With regards to notifying "***each affected individual to whom significant harm results or is likely to result from a notifiable data breach in any manner that is reasonable in the circumstances***", we would like to clarify if there will be elaboration on the requirements of notifying each affected individual. Specifically, does notification require acknowledgement from the affected individuals? In a practicable example, if 500 customers' credit card details were to be compromised, we would want all customers to acknowledge notification and undertake appropriate measures (i.e. cancel credit card). Therefore, the utopian method is probably to call each affected individual for confirmed

acknowledgement. However, this would be relatively time consuming (as opposed to SMS notification). Additionally, the success rate of notification is also subject to customers' response (i.e. whether customers pick-up the call). For such scenarios, would SMS notification, with no need for customer to respond as acknowledgement, be deemed reasonable?

3. Porting of applicable data - 26(G)(5):

   Will a definition of "***excluded class of applicable data prescribed***" be included? Understand there was a consultation issued earlier in that PDPC will reach out to the industry and relevant sector regulators to discuss on relevant parameters. Upon confirming the relevant parameters, we should have a clearer picture of "excluded class". Having said, would like to know if there is intention to include associations like Life Insurance Association (LIA) in the discussion process. As LIA is currently the body that consolidates input from various members in the industry on relevant topics, their involvement will definitely assist to provide clarity on the definition of "excluded class".

Conclusion

We seek clarity on the scope and terminology used with regards to the abovementioned questions.