Transamerica Life (Bermuda) Ltd., Singapore Branch

Response to Public Consultation on the Draft Personal Data Protection (Amendment) Bill

Contact Person: Ann Chong, Manager, Compliance

Email: ann.chong@transamerica.com

Direct Line: +65 6212 0537

b) Summary of Major Points

Our Company has explored the public consultation paper issued on 14 May 2020 on the four key areas of proposed amendments to the Personal Data Protection Act 2012 (PDPA). While we are in support of all four proposed amendments, we would like to seek the following clarifications from the PDPC/MCI.

c) Statement of Interest

NIL.

d) Comments

Mandatory Data Breach Notification

i. With reference to the proposal on mandatory breach notification (para 19 of the public consultation paper), *could the PDPC provide further clarity on the timeframe for organisations to investigate and assess if there are "credible grounds to believe a data breach has occurred"?*

Previously, based on the PDPC's Guide to Managing Data Breaches 2.0, organisations were given up to 30 days to carry out an assessment from when they first become aware of a potential data breach.

ii. With reference to the same Guide as above, we *would like to clarify our understanding of PDPC's expectations of the notification timelines* as such:

1. After assessing breach to be reportable, to send interim notification to the PDPC within three calendar days (where specific information is not yet available).
2. Organisation then has to notify affected individuals after the first notification to the PDPC.
3. Organisation makes subsequent notification to the PDPC on specific information as required in Annex B of the Guide.

iii. In the event of a data breach, if an organization is able to immediately mitigate and reduce the impact on the affected individuals such that it would not cause "significant harm", would the organization still be required to report the breach to the PDPC since it would no longer fall into the criteria for reporting?

Data Portability Obligation

i. How can an organization be seen as complying to the regulations to support an individual's request to transmit his/her personal data, if the organization does not possess the necessary technology or infrastructure to facilitate the data port? Will a rejection of an individual's request be viewed as not fulfilling the data portability obligation?

ii. Would the PDPC provide any lee way for small organisations who may not have the resources to upgrade their systems to facilitate such data ports? Such upgrades may not be economically practical given the potentially low volume of such requests.

iii. Will a rejection of an individual's request be viewed as not fulfilling the data portability obligation?

Individual Accountability

i. Could the PDPC provide some scenarios of how individual accountability will come into practice? We note that employees acting in the course of their employment, in accordance with their employer's policies and practices, or whose actions are authorised by their employers, will not run the risk of criminal sanctions.
What would be considered not to be in the course of an employment?

Improved controls for unsolicited commercial maessages (Spam Control Act and Do-Not-Call ("DNC") Provisions)

i. Does the new DNC scope cover all future and current text messaging platforms as well? Same question for the Spam Control Act.

e) <u>Conclusion</u>

Our Company is supportive of and views the proposed amendments as progressive and meaningful steps towards strengthening Singapore's data privacy laws. We look forward to PDPC/MCI's response on the queries raised.