28 May 2020

To: Personal Data Protection Commission

Re: Public Consultation for the PDP (Amendment) Bill

With reference to the Public Consultation for the PDP (Amendment) Bill issued on 14 May 2020, comments from Manulife (Singapore) Pte Ltd are as follows:

Question / paragraph from Public Consultation	Our comments
20) Upon determining that a data breach meets the criteria for notifying affected individuals, the organisation must notify all affected individuals as soon as practicable. Where a data breach meets the criteria for notifying PDPC, the organisation must notify PDPC as soon as practicable, no later than three calendar days after the day the organisation determines that the data breach meets the notification criteria (e.g. if the organisation makes the determination on 9 March, it must notify PDPC by 12 March). Prescribing a cap of three calendar days provides clarity for organisations on when they must notify PDPC. As the considerations in determining how expeditiously PDPC can be notified are different from those in determining how expeditiously the affected individuals should be notified, the expectation is not for notifications to PDPC and affected individuals to be made simultaneously. However, PDPC must be notified before or at the same time as affected individuals are notified, to allow PDPC to assist affected individuals who contact PDPC once they are notified.	1) On the notification to PDPC no later than 3 calendar days after the day the organisation determines that the data breach meets the notification criteria, MLS would like to propose to increase the timeframe to 5 calendar days or 3 working days. 2) Reason being that if a data breach occurred on a Friday afternoon, it would be challenging to have the complete information by Monday in order to notify PDPC. 3) Should organisations continue to file data breach via https://eservice.pdpc.gov.sg/case/db? and in the event of the unavailability of website, is there a template and email address that we can file the data breach?
22) MCI/PDPC will provide the following exceptions to the requirement to notify affected individuals: **a) Remedial action exception**: where organisations have taken remedial actions to reduce the likely harm or impact to the affected individuals such that the data breach is unlikely to result in significant harm to the affected individuals. **b) Technological protection exception**: where the personal data that was compromised by the data breach is subject to technological protection (e.g. encryption) that is of a reasonable security standard, such that the data breach is unlikely to result in significant harm to the affected individuals.	1) The expectation is to notify PDPC before affected individuals for allowing PDPC to assist affected individuals who contact PDPC once they are notified. If the Company has taken remedial actions to reduce the likely harm or impact to the affected individuals after notifying PDPC, does PDPC expect a follow up email on the remedial action?
23) In addition, organisations must not notify any affected individual if instructed by a prescribed law enforcement agency or directed by PDPC. This prohibition is intended to cater to circumstances where notification to affected individuals may compromise any investigations or prejudice any enforcement efforts under the law.	1) We agree to this instruction. However, my suggestion is to state the xx calendar days for law enforcement agency and/or PDPC to provide such instruction to the company. So that the company is able to inform the affected individuals as soon as practicable otherwise, this notification to affected individuals might be delayed.

Question / paragraph from Public Consultation	Our comments
24) Further, to cater to exceptional circumstances where notification to affected individuals may not be desirable, PDPC will have the power to exempt organisations from notifying affected individuals. This includes circumstances where there are overriding national security or national interests.	1) Same comments as above point 23.
38) MCI/PDPC is enhancing the framework for the collection, use and disclosure of personal data under the PDPA to ensure meaningful consent by individuals, complemented by accountability requirements to safeguard individuals' interests. MCI/PDPC will **expand deemed consent** under section 15 of the PDPA to include: **b) Deemed consent by notification**: Consent may be deemed to be given if (i) the organisation provides appropriate notification to inform the individual of the purpose of the intended collection, use or disclosure of his/her personal data, with a reasonable period for the individual to opt-out of the collection, use or disclosure of his/her personal data for that purpose; and (ii) the individual did not opt-out within that period. In order to rely on deemed consent by notification, organisations are required to assess and ascertain that the intended collection, use or disclosure of personal data for the purpose is not likely to have any adverse effect on the individual after implementing measures to eliminate, reduce the likelihood of or mitigate the identified adverse effect to the individual. Organisations also may not rely on this approach to obtain consent to send direct marketing messages to the individuals. Individuals will also be able to withdraw their consent to the collection, use or disclosure of their personal data.	1) Would like to seek clarity on "reasonable period". Please advise the duration of a reasonable period. 2) Upon receiving the opt-out consent, does a company have the 30 days period to process? Within the 30 days period to process, can the company still use the deemed consent for that intended purpose?

Question / paragraph from Public Consultation	Our comments
40) In addition, to cater to situations where there are larger public or systemic benefits where obtaining individuals' consent may not be appropriate, **two new exceptions to the consent requirement will be introduced:** a) **Legitimate interests exception**: This new exception is intended to enable organisations to collect, use or disclose personal data in circumstances where it is in the legitimate interests of the organisation and the benefit to the public (or any section thereof) is greater than any adverse effect on the individual. This could include the purposes of detecting or preventing illegal activities (e.g. fraud and money laundering) or threats to physical safety and security, ensuring IT and network security; and preventing misuse of services. To rely on this exception to collect, use or disclose personal data, organisations must first: (i) assess any likely adverse effect to the individuals and implement measures to eliminate, reduce the likelihood of or mitigate identified adverse effect to the individual; (ii) determine that the benefit to the public (or any section thereof) outweighs any likely residual adverse effect to the individual; and (iii) disclose their reliance on legitimate interests to collect, use or disclose personal data. This exception must also not be used for sending direct marketing messages to individuals.	1) As part of a claim fraud investigation, an organisation (A) would check with another organisation (B) for information (e.g.: If a claimant submitted the same medical invoice). For checking, A would disclose some personal data for verify to B. The adverse effect on the claimant might not be reduced or mitigated if the fraud case goes into criminal suit and eventually published on any newspaper. We would like to know if we can still rely on the exception for such claim fraud investigation with B.
44) Under the Data Portability Obligation, an organisation must, at the request of an individual, transmit his/her personal data that is in the organisation's possession or under its control, to another organisation in a commonly used machine-readable format. This allows individuals to switch to new service providers more easily. Organisations can also have access to more data, thereby spurring the development of innovative data-driven applications that will benefit consumers and support the growth of the Digital Economy.	1) Please advise if PDPC would be providing the examples on acceptable data portability format and transmission technical standard. 2) Could PDPC consider allowing the transmitting organisation to impose administrative charges on individual requestor if the request is beyond reasonableness or require extensive efforts, to cover operational costs on retrieving/preparation of the personal data.
45) To ensure that the compliance burden is reasonable for organisations, the Data Portability Obligation will be scoped to the following: a) **User provided data** (i.e. data that is provided to the organisation, such as name, contact information, credit card details, delivery address) and **user activity data** (i.e. data about the individual that is created in the course of or as a result of the individual's use of any product or service, such as transactions, data collected by wearables and sensors) **held in electronic form**, including business contact information;	1) In the context of insurance industry, does the "transmit a copy of their personal data" refers to the pre-sales and post-sales documents (such as insurance application form, fact-find, identification document, change of particulars form etc) as these forms contained user provided data? 2) Would like to seek clarity on the duration of use activity data. If the existing customer is with the organisation for 10 years, and upon receiving such request, is the organisation required to transmit all the transactions in 10 years?

Question / paragraph from Public Consultation	Our comments
54) As the PDPA and SCA impose overlapping requirements on unsolicited marketing text messages, MCI/PDPC has reviewed both legislation to make it easier for organisations to comply with their requirements. The proposed amendments also take into account developments in the current landscape. Specifically, MCI/PDPC intend to make the following amendments. b) **The DNC Provisions will prohibit the sending of specified messages to telephone numbers obtained through the use of dictionary attacks and address harvesting software**: The sending of electronic messages to electronic addresses generated through the use of dictionary attacks and address harvesting software is prohibited under the SCA today. MCI/PDPC will introduce a similar prohibition under the DNC Provisions, in respect of the sending of specified messages to telephone numbers. This aims to deter spammers who use technologies that make it easier to indiscriminately send unsolicited commercial messages (including robocalls) to a large number of recipients and helps ensure Singapore does not become a haven for such spammers. Persons who send specified messages to mobile telephone numbers obtained through the use of dictionary attacks or address harvesting software will be dealt with under the amended PDPA.	1) Under the definition of "dictionary attack", does the method included randomly generated numbers?
72) MCI/PDPC will introduce a requirement for organisations to preserve personal data requested pursuant to an access request (or a copy) for a prescribed period of a) at least 30 calendar days after rejection of the request, or b) until the individual has exhausted his/her right to apply for a reconsideration request to PDPC or appeal to the Data Protection Appeal Committee, High Court or Court of Appeal, whichever is later. This will help to preserve the availability of a meaningful remedy should the individual succeed in his/her application. MCI/PDPC will similarly require preservation of personal data requested pursuant to a data porting request.	1) Would suggest stating a maximum period for point (b).

Particulars of Insurer and contact person:

- Company Name: Manulife (Singapore) Pte. Ltd.
- Address of Company: 8 Cross Street, #15-01 Manulife Tower, Singapore 048424
- Contact Person: Teo AiLing (Ai_Ling_Teo@manulife.com)

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

Thank you.