Public Consultation on Personal Data Protection (Amendment) Bill

Company	**Great Eastern Singapore**
Staff contact in case of enquiry	**Maryaki**
Email address	**maryaki@greateasternlife.com**
Phone number	**6248 2987**

Summary of Major Points	**Statement of interests** (from Public consultation/PDP Amendment Bill)	**Comments**
Mandatory data breach notification requirement	Para 15 For the purposes of the mandatory data breach notification requirement, "data breach" refers to any unauthorised access, collection, use, disclosure, copying, modification, disposal of personal data, or loss of any storage medium or device on which personal data is stored.	Under section 24 of the PDPA, organisations to have in place reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks. However, the mandatory breach notification requirement requires organisations to report all data breaches that (i) results in, or is likely to result, in significant harm to the individuals to whom any personal data affected by a data breach relates (the "affected individuals"); or (ii) is of a significant scale. Noted that this is regardless of whether the organisation has put in place the reasonable security measures, and that it does not matter whether an organisation has breached the PDPA provisions.
Mandatory data breach notification requirement	Para 16 – 17 MCI/PDPC intends to prescribe in Regulations a numerical threshold on what constitutes "a significant scale" in terms of the number of individuals affected in a data breach. Based on its past enforcement cases, PDPC notes that data breaches affecting ***500 or more individuals would be an appropriate threshold***.	MCI/ PDPC may consider using the amount/ quantum of personal data leaked as using only the no. of individuals affected as a threshold may not be comprehensive. For example, "500 individuals with their names leaked" Versus "10 individuals with their names, IC and address leaked". The amount of personal data leaked in the latter makes it easier to identify the unique person. Hence, the impact may be significant although the no. of affect individual is only 10.
Mandatory data breach notification requirement	Para 18 MCI/PDPC also intends to prescribe in Regulations categories of personal data which, if compromised in a data breach, will be considered likely to result in significant harm to the individuals	To seek clarity on the definition of significant harm. Based on data breach definition in Section 26(A) PDP Amendment Bill, it suggested that the breach would affect any prescribed class of personal data relating to the individual by nature.

	Under PDP Amendment Bill – Notifiable Data Breaches **Section 26B** (1) A data breach is a notifiable data breach if the data 25 breach — (*a*) results in, or is likely to result in, ***significant harm*** to the affected individual; or (*b*) affects not fewer than the minimum number of affected individuals prescribed. (2) Without limiting subsection (1)(*a*), a data breach is deemed to be likely to result in significant harm to an individual if the***data breach affects any prescribed class of personal data relating to the individual***.	As such, the current definition of "significant harm" may be further enhanced to help reader to distinguish between "insignificant harm" and "significant harm". This may be critical, as it will form the basis to determine if the breach is notifiable. MCI/PDPC may want to consider to be clear: • if 'significant harm' applies when the data loss is a combination of the categories of data types or any one of the categories of data types • if certain loss of data types for different categories of people may affect what constitutes as 'significant harm', e.g. public figure, PEP, member of public.
Mandatory data breach notification requirement	Para 20 Where a data breach is discovered by a data intermediary ("DI") that is processing personal data on behalf of and for the purposes of an organisation, the DI is required to notify the organisation without undue delay from the time it has credible grounds to believe that a data breach has occurred. Please see timeline for data breach notification in Diagram 1 below.	It will be helpful if MCI/PDPC can further clarify if an intermediary that is storing data on behalf is in scope for this requirement and consider a data intermediary as well.
Mandatory data breach notification requirement	Para 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.	As part of data breach management and investigation, it is inevitable that some affected individual(s) will be contacted and notified of the incident as the organisation performs fact-find. Is this allowed? Since the PDPC dictates where or not affected individual(s) are to be notified, will the PDPC be committing a timeline to the organisations on when the notification assessment will be completed? The term "as soon as practicable" is very wide and if containment efforts are not implemented timely by the organisations, it may cause more harm and/or impact to the individuals.

Data Portability Obligation	Para 47b The technical and process details to ensure the correct data is transmitted safely to the right receiving organisation, and in a usable form. The technical details could include data formats, transfer protocol, authentication protocols and cybersecurity standards to enable interoperability between organisations porting and receiving the data. The processes involved could include how customers request for data porting, verification of customers' requests and the expected service level (including timeline for porting) between organisations and consumers.	While Regulations may prescribe adequate cybersecurity standards and controls, no security measures are infallible. For operational efficiency, it is possible that porting data could be transmitted in bulk. In the event porting data in transmission is compromised through an unforeseeable issue (protocol implementation vulnerability such as Heartbleed bug, or compromised certificate authority such as DigiNotar, etc), would the porting and/or receiving organisation be held accountable and responsible for user notification?
Data Portability Obligation	Section 26E (2) This Part applies only to applicable data that — (a) is in electronic form on the date the porting organisation receives a data porting request relating to the applicable data; and (b) was collected or created by the porting organisation within the prescribed period before the date the porting organisation receives the data porting request relating to that applicable data	In the case where an individual has made request for applicable data which is not in electronic form on the date, a data-porting request was received, can an organisation explain the situation and turn down the request per any requirements?
Data Portability Obligation	Section 26H (1)This section applies where giving effect to a data porting request in respect of applicable data about an individual (P) under section 26G (2) would transmit personal data about another individual (T) to a receiving organisation.	Referring to the statement "transmit personal data about another individual (T) to a receiving organisation" Will it only be restricted to one individual (T) or there could be instances of more than one individual (T)?
Data Portability Obligation	Section 26H (2)A porting organisation may disclose personal data about T to a receiving organisation without T's consent only if the data porting request — (a) is made in P's personal or domestic capacity; and	Customer service that requires personal touch may be associated with personal data (phone, ID, phone number, etc) of insurance agents or relationship managers. It is in the interest of the porting organisation to keep such third party details confidential, and these details are not necessary for the provision

	(b) relates to P's user activity data or user-provided data	of goods and service by the receiving organisation. As porting obligation of third party personal data associated with user activities does not seem to exclude staff or agents of the porting organisation Request for the consideration to amend the Fifth Schedule to exclude from porting data any third party personal data that are irrelevant and unnecessary to the provision of goods and services by the receiving organisation
Data Portability Obligation	Preservation of copies of personal data or applicable data Section 32(A) : (1) where an organisation **refuses** to provide access to personal data requested by an individual under section 21(1)(*a*): the organisation or porting organisation (as the case may be) must ***preserve, for not less than the prescribed period,*** a copy of the personal data or applicable data concerned, as the case may be or Para 72 (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.	To clarify, the preservation clauses would have an impact on the Retention Obligation since Organizations can no longer remove the data when they deem no longer required? It will be helpful if MCI/PDPC can prescribe the longest period that personal data should be preserved under criteria (b)
Data Portability Obligation	Exceptions to the Data Portability Obligation will be provided: Section 65 (2)(iv): the ***fees*** that a porting organization may charge in respect of such requests.	To clarify if there is any guidelines over the fees charges (i.e. charged to receiving organizations/ charged to individual requestor)? Would the Organization be required to submit the fees structure to PDPC/ MCI for review prior to rolling out, to ensure reasonableness and no overcharges?
Data Portability Obligation	Others	For data exchange under data portability obligations, e.g.: with other insurers/ organisations in the near future, will there be any form of a collective agreement template or similar for businesses?