Cigna Singapore's feedback to the Consultation Paper on Personal Data Protection (Amendment) Bill

Contact Person:	Luis Tan
Company Name:	Cigna Europe Insurance Company S.A – N.V. Singapore Branch
Designation:	Compliance Specialist
Email Address:	Luis.Tan@Cigna.com
Telephone Number:	6549 3644

No.	Extract from Consultation Paper	Comments
1.	Para 17 of CP: Data breaches of a significant scale could indicate a systemic issue within the organisation, which may require PDPC's further investigation and guidance on appropriate remedial actions that the organisation should implement. To provide clarity for organisations to ascertain whether a data breach meets this notification criteria, 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.	Para 17 of CP: In determining 'significant scale', please clarify whether there is requirement to aggregate the number of impacted individuals from a few separate incidents in different timeframe if the root cause is the same/similar (e.g. evolved from the same issue). If so, there should also be a prescribed timeframe for purpose of aggregation of the numbers. Please consider to restrict determination of 'significant scale' based on per incident basis. This is because for each data incident, organisation would have done the necessary to put in place remediation actions before the data incident is closed.
2.	Para 18 of CP: 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. This makes clear the types of data breaches that organisations will be required to notify affected individuals. Several jurisdictions have adopted a similar "whitelist" approach for data breach notification to	Para 18 of CP: We would like to highlight that '*health insurance information*' is a very wide term, for e.g. premium, premium frequency, mode of payment, inception date, date of application, name, NRIC, mobile number, email address, claims incurred date, claims amount, treatment code, name of healthcare provider etc.

	affected individuals and/or the authorities. Examples of data categories prescribed by other jurisdictions include social security numbers, drivers' licence numbers, state identification numbers, credit/debit card numbers, health insurance information and medical history information.	As the purpose of prescribing categories of personal data is related to 'significant harm' to individuals, please consider to limit to '*medical information*' instead. For e.g., the disclosure of an individual's HIV treatment or transgender surgery would likely pose significant harm to the individual.
3.	Para 20 of CP: 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.	Para 20 of CP: Please consider amending 3 calendar days data breach notification to 3 business days for the following reasons: 1. Consistency with other regulatory reporting which usually use 'business days' requirements, for e.g.: • Fraud notification to MAS (MAS Notice 123 Notice on Reporting of Suspicious Activities & Incidents of Fraud) - the report shall be lodged not later than **5 working days** after the discovery of the activity or incident by the registered insurer. • Suspicious Transaction Reporting to CAD (Guidelines to MAS Notice 314 Notice on Prevention of Money Laundering and Countering the Financing of Terrorism – Life Insurers, Guidelines to Notice FAA-N06 on Prevention of Money Laundering and Countering the Financing of Terrorism and Guidelines on Prevention of Money Laundering and Countering the Financing of Terrorism – Direct General Insurance Business, Reinsurance Business, and Direct Life Insurance Business) - A Suspicious Transaction Report (STR) should be filed within **15 business days** of the case being referred by the relevant officer, employee or agent, if the insurer has assessed that the matter should be referred to the STRO, unless the circumstances are exceptional or extraordinary.

		2. Reasonableness and Practicality- sometimes data incident may involve third parties and if the data incident falls on a long weekend (including public holiday), it may be challenging for the organisation to obtain response from the relevant third party.
4.	Para 21 of CP: 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.	Para 21 of CP: The term '*undue delay*' is rather subjective. As the organisation which engaged the DI has obligation to conduct its own assessment, any delay of notification from the DI may further prolong the investigation/assessment period which leads to delay in notification to PDPC and/or the impacted individuals. Please consider imposing a maximum time period for this. For e.g., since an organisation is given 30 days to conduct its investigation/assessment, the maximum time period for DI's notification could be 'no later than 30 days from the first day the DI has reason to believe that a data breach has occurred'.
5.	Para 33 of CP: In addition, MCI/PDPC does not intend for these offences to apply in situations where the conduct is in the nature of a private dispute for which there is recourse under private law (e.g. ex-employee taking an organisation's customer list when joining a competitor). Such private disputes should continue to be settled through civil suits or other forms of dispute resolution.	Para 33 of CP: The civil suits or other forms of dispute resolution may take a long time to completion or it may be withdrawn (e.g.: settlement between parties). This will prejudice the 'victims' where their personal data had been disclosed without their consent. PDPC should consider dealing with the PDPA offences separately, regardless of the private law recourse. This will send a strong message to prevent egregious mishandling of personal data by individuals, as the current framework only imposed obligations on organisations/employers.

6.	Para 40(a) of CP: 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. Please refer to clause 31 of the draft PDP (Amendment) Bill.	Para 40(a) of CP: We are of the view that for '*legitimate interests exception*', it is not necessary to disclose this as long as the organisation has sufficient justification. This is consistent with the rest of the exceptions under PDPA.
7.	Para 54(b) of CP: 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	Para 54(b) of CP: Please consider including an exception for this or to allow this to be a defence if an organisation obtained telephone numbers from a third party where the third party affirmed that the list was not obtained with address-harvesting software or dictionary attacks, and the organisation has no reason to believe that this is false or inaccurate.

	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. Please refer to clause 27 of the draft PDP (Amendment) Bill.	
8.	Para 58 of CP: Under section 29(2)(d) of the PDPA, PDPC may impose a financial penalty of up to S$1 million for data breaches under the PDPA. The amendments will increase the maximum financial penalty to (i) up to 10% of an organisation's annual gross turnover in Singapore; or (ii) S$1 million, whichever is higher.	Para 58 of CP: We are of the view that civil penalties should not be tied to an organisation's turnover, and should be proportionate to the harm caused to the data subjects. If a stricter penalty has to be imposed on a defaulting organisation, please consider revising this to 10% of the organisation's annual net profit instead. This is because an organisation with high turnover does not necessarily mean it is profitable. If an organisation is not profitable despite the high turnover, such punitive penalty may impact sustainability of the business and in worst-case scenario, may impact solvency of the organisation. It is important to note that civil penalty framework should not impose undue hardship on an organisation, especially if the organisation is committed to implement remediation actions to prevent such incident from happening again.