Comments for the Public Consultation on the Draft Personal Data Protection (Amendment) Bill from the Cloud Security Alliance, Singapore Chapter

Submitted by:
Suresh Agarwal
Secretory, Cloud Security Alliance, Singapore Chapter
Mobile: +65 96661106
Email: suresh@agarwal.sg

Below are the ExCo Members for the CSA Singapore Chapter:

1.	Professor SIOW Yuen Khong, Alex	President
2.	Mr. Suresh AGARWAL	Secretary
3.	Mr. LIM Shien Min, Jim	Vice President
4.	Mr. Richard LIM	Treasurer
5.	Mr. NG Yeng Yong, Steve	Marketing Director
6.	Mr. LIM Zhi Meng, Nigel	Membership Director
7.	Mr. William HO	Education Director
8.	Mr. Ian LOE	Research Director
9.	Ms. Annie CHONG	Events Director
10.	Mr. Sarbojit Madhab BOSE	Training Director

28 May 2020

To: DataRegulation@mci.gov.sg

Subject: Public Consultation for the PDP (Amendment) Bill

Summary of Major points:

Generally, the amendments are quite good and acceptable and appreciated to us.

Statement of Interest:

We have no conflict of interest.

Comments:

1. Refer the point 17 below, **100 individuals** should be good threshold.

   "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."*

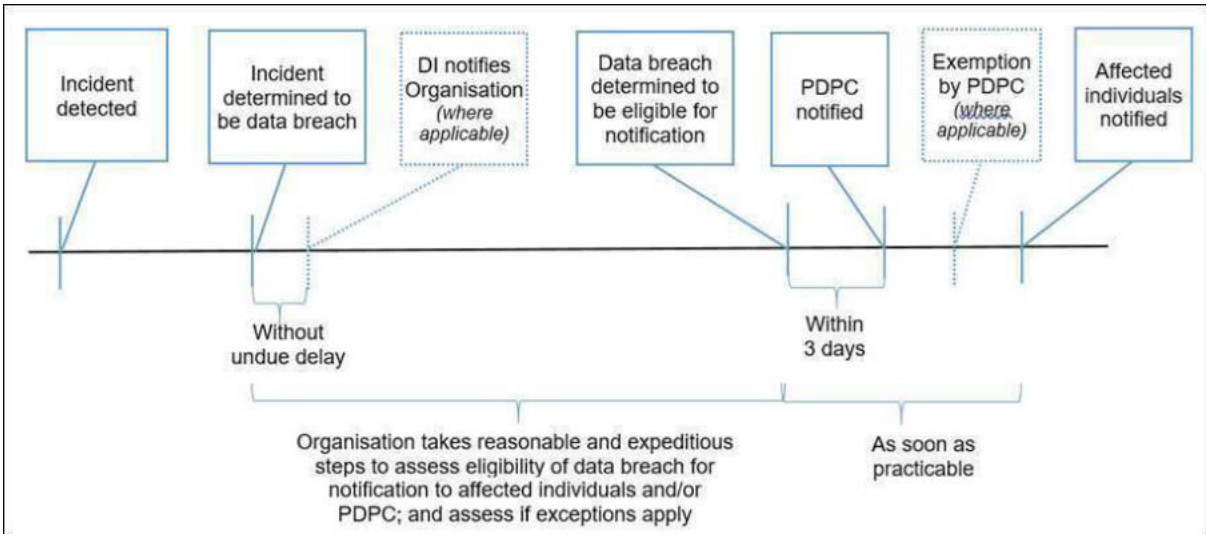
2. Refer to point 19, 20 and 21 the time taken for the Affected Individuals should be much shorter and preferably a fixed period from the actual incidence of breach, **preferably within 2 weeks**:

   *"19. Once an organisation has credible grounds to believe that a data breach has occurred, the organisation will be required to take reasonable and expeditious steps to assess whether the data breach meets the criteria for notification to the affected individuals and/or PDPC. The organisation shall document the steps taken to demonstrate that it has acted reasonably and expeditiously, and carried out the assessment in good faith. **Unreasonable** (consider : within 24 hours) **delay in assessing or notification** (consider: within 2 weeks) of data breaches will be a breach of the data breach notification requirement. PDPC will have the powers to assess these matters and to take enforcement action against the organisation for any failure to do so.*

   *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** (consider : within 2 weeks). Where a data breach meets the criteria for notifying PDPC, the organisation must notify PDPC as soon as practicable, no later than **three** (consider 2 work days) 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** (consider 2 work days) 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.*

   21. 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.

   Diagram 1: Timeline for data breach notification



Exceptions to requirement to notify affected individuals

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."

3. Refer to point 40 b**, business improvement to be closely** defined.

b) Business improvement exception: This new exception is intended to make clear that organisations may use personal data (that was collected in accordance with the DP Provisions) without consent for the following business improvement purposes: (i) operational efficiency and service improvements; (ii) developing or enhancing products/services; and (iii) knowing the organisation's customers. This will provide clarity for organisations to confidently harness personal data for business improvement purposes. The use of personal data for business improvement must be what a reasonable person would consider appropriate in the circumstances14, and it must not be used to make a decision that is likely to have an adverse effect on an individual. The intent is also for this exception to apply

Conclusion:

We are supportive of the changes suggested.

Warm Regards

Suresh Agarwal
suresh@agarwal.sg

3 Shenton Way, 24-05 Shenton House, Singapore 068805
T: +65 6276 2301 **F:** +65 6276 2302 **M:** +65 9666 1106