Cover Page

Public Consultation for the PDP (Amendment) Bill
Ministry of Communications and Information (MCI)
Personal Data Protection Commission (PDPC)
DataRegulation@mci.gov.sg

28-May-2020

Dear sir/madam,

Re: Asia Cloud Computing Association's (ACCA) Response to the Draft Personal Data Protection (Amendment) Bill), including Related Amendments to the Spam Control Act, issued by the Singapore Ministry of Communications and Information

: The Asia Cloud Computing Association (ACCA) is pleased to submit our comments and suggestions on the Draft PDP (Amendment) Bill. We are pleased to note that Singapore has been consistently updating its personal data protection measures to keep pace with the technology, and also use cases which have continued to present themselves as Singapore moves further into digital transformation of its economy.

Summary of Major Points: Following discussions with our member companies, we are submitting the comments on the abovementioned consultation. Our comments centre around the following clauses:

- Clause 2 / Amendment of Section 2(1)
- Clause 3 / Amendment of Section 4
- Clause 10 / Amendment of section 21
- Clause 12 / New Part VIA
- Clause 13 / New Part VIB
- Clause 17 / Amendment of Section 29
- Clause 18 / New Section 31A
- Clause 20 / Amendment to Section 35B: Unauthorized disclosure of personal data

Statement of Interest: We thank you for allowing the industry to submit feedback on this document. As the apex industry association for Asia Pacific stakeholders in the cloud computing ecosystem, the ACCA represents a vendor-neutral voice of the private sector to government and other stakeholders. The ACCA's mission to accelerate the adoption of cloud computing throughout Asia Pacific by helping to create a trusted and compelling market environment, and a safe and consistent regulatory environment for cloud computing products and services. We are committed to strengthening digital resilience, and to the development of a safe and secure ecosystem where data is protected by the best technology and regulatory frameworks, in support of Singapore's vibrant digital economy.

Comments: We have included detailed comments in the Annex which follow this cover letter.

Conclusion: Should you have any questions on our comments, I would be pleased to arrange for a videoconference discussion with our members. Thank you, and I look forward to hearing from you on the issues raised.

Yours sincerely,

Lim May-Ann
Executive Director
Asia Cloud Computing Association
mayann@asiacloudcomputing.org

ANNEX: Asia Cloud Computing Association's (ACCA) Response to the Draft Personal Data Protection (Amendment) Bill), including Related Amendments to the Spam Control Act, issued by the Singapore Ministry of Communications and Information

Topic / Locations refer to text within the Personal Data Protection (Amendment) Bill 2020	Summary of Concerns and Recommendations
1) Clause 2 / Amendment of Section 2(1) "**derived personal data**" (a) means personal data about an individual that is **derived** by an organisation in the course of business from other personal data about the individual or another individual in the possession or under the control of the organisation; but (b) does not include personal data **derived** by the organisation using any prescribed means or method; "**user activity data**", in relation to an organisation, means personal data about an individual that is **created** in the course or as a result of the individual's use of any product or service provided by the organisation;	The ACCA suggests that the word "**created**" covers too broadly under the definition of "user activity data", which could potentially overlap with the definition of "**derived** personal data" and cause confusion. ACCA suggests narrowing and simplifying both definitions to ensure clear exclusivity between "derived personal data" and "user activity data".
2) Clause 3 / Amendment of Section 4 / Paragraph 28 of Consultation Paper: Removal of exclusion for organizations acting on behalf of public agencies. PDPA now applies to Data Intermediaries (DI)'s acting on behalf of the government. DI's acting in such capacity were previously excluded.	The ACCA recommends that Sections 24 and 25 of the PDPA be reviewed and amended to clarify that where the relevant processing activity relates to a DI acting on behalf and for the purposes of a public agency, that such reasonable protection or retention should be in accordance with their contractual arrangements, and/or any other applicable law or regulation. The removal of the exclusion for organizations acting on behalf of public agencies, is confusing as it is unclear whether a DI would be reasonably able to take on its relevant obligations (i.e. retention and protection), given that the organization it is acting on behalf for (i.e. public agencies), is not subject to the PDPA.

Topic / Locations refer to text within the Personal Data Protection (Amendment) Bill 2020	Summary of Concerns and Recommendations
	We therefore recommend that sections 24 and 25 of the PDPA, be further amended to make clear that **where the relevant processing activity relates to a DI acting on behalf and for the purposes of a public agency, that such reasonable protection or retention should be in accordance with their contractual arrangements.**
3) Clause 10 / Amendment of section 21 (3A) Subsection (3)I and (d) does not apply to any user activity data about, or any user-provided data from, the individual who made the request despite such data containing personal data about another individual.	ACCA suggests that Article 3(A) be repealed, as it is unclear if the intention of the proposed amendment is meant to achieve – does it mean to exclude user-provided data and user activity data from the exception, even if it contains information about a third-party individual? If so, it would be a concern because organizations often do not know whether an individual has the right to provide third-party information. In case the organization has to "return" this data to the individual that had provided the data, the potential breach of the third-party individual's privacy would only be perpetuated. Furthermore, the information that was provided to the organization by the individual is likely to be complemented with other information regarding this third person. It is also not feasible to 'split' a data set and only provide the information that was initially received.
4) Clause 12: New part VIA/ Amendment to Section 26A: Interpretation of this Part Current definition of "data breach" is not clearly linked to the definition of a security incident/ when the data breach notification should be triggered.	We recommend **revising the definition of "data breach".** The proposed definition of "data breach" is not clearly linked to the occurrence of a security incident, or when a data breach notification should be triggered. This is problematic as the definition could be extended to non-security incident linked events. For example, limb (b) of the definition of "data breach" could also be interpreted to cover a network service outage that does not lead to harm to the individual. MCI/PDPC can consider revising the definition of "data breach" to be more consistent with international practices. For example, the EU General Data Protection Regulations states that " 'personal data breach' means a breach of security leading to the accidental

Topic / Locations refer to text within the Personal Data Protection (Amendment) Bill 2020	Summary of Concerns and Recommendations
	or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed." MCI/PDPC can consider revising the definition of "data breach" to specifically address security incidents. Again, such an approach would also be consistent with international practices (for example the EU General Data Protection Regulations).
5) Clause 12: New Part VIA / Amendment to Section 26B/ Paragraph 21 of the draft PDP (Amendment) Bill): Mandatory Data Breach Notification (DBN) 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 organization, the DI is required to notify the organization without undue delay from the time it has credible grounds to believe that a data breach has occurred.	The ACCA recommends to clarify the meaning of the "significant harm" threshold, proposed Section 26B-1(a)). We note that the threshold for notification to be based on the likelihood of "significant harm" is unclear, and could possibly result in the PDPC and individuals being inundated with numerous immaterial notices, resulting in "notification fatigue" and a very real possibility that data subjects and regulators will fail to take appropriate action in response to notifications that indicate a real risk of harm. The ACCA also recommends to clarify relevant factors that constitutes a Data Intermediary ("DI"), having "reason to believe that a data breach has occurred in relation to personal data" (proposed Section 26B-2(b)). Specifically**, we recommend that MCI/PDPC revise the PDP Amendment Bill to make clear that the DI should not be responsible more monitoring the security of the responsible organisation (for which it is acting on behalf on), or verifying whether instructions on processing the data given by the responsible organisation to the data intermediary are duly authorised.**
6) Clause 12: New Part VIA / Amendment to Section 26D: Duty to notify occurrence of notifiable data breach (1) Where an organisation assesses, in accordance with section 26C, that a data breach is a notifiable data breach, the organisation must	Rather than risk opening a vulnerability window of 3 days (in case an incident becomes public), the ACCA suggests including a provision to mandate notification be kept confidential to protect the data from further breaches. We also recommend that **section 26(D) be revised to make it clear that DIs are not required to notify the Commission and Individuals of a "notifiable data breach", as**

Topic / Locations refer to text within the Personal Data Protection (Amendment) Bill 2020	Summary of Concerns and Recommendations
notify the Commission as soon as is practicable, but in any case, no later than 3 days after the day the organisation makes that assessment.	**MCI/PDPC intends as** the current drafting of section 26(D) is ambiguous is to whether such notification obligations would apply to DIs.
7) Clause 12: New Part VIA / Amendment to Section 26D: Duty to notify occurrence of notifiable data breach (3) The notification under subsection (1) or (2) must — (a) contain all the information that is prescribed for this purpose; and (b) be made in the form and submitted in the manner required by the Commission.	The ACCA suggests that the phrase "to the extent the organisation has reasonable access to the information" be added following the word "purpose" in Section 25D(3)(a). We note that a number of other international data privacy rules, such as the EU's GDPR, allow for phased notifications, where follow-up notifications may be submitted following further investigation, providing additional detail once they are available and can be shared without causing any additional security risks.
8) Clause 13 / New Part VIB: Data Portability	The ACCA recommends that broad data portability requirements should not be mandated. **Whitelist Scoping.** If MCI/PDPC nonetheless proceeds with mandating data portability, we strongly recommend that the "whitelist" of data categories be narrowly scoped to meet the purpose of allowing individuals to switch to new service providers more easily. For example, it may be helpful for online retail users to port transaction details of their shopping history. However, data generated from using specific features provided by a company, such as browse and discovery tools, or dedicated loyalty or gift card programmes, is unlikely to be readily usable by other companies. Further, most types of user-generated content are sensitive in nature and their sharing across companies could gravely undermine the privacy of both the requesting individual and third parties. We also recommend excluding unstructured or pre-processed data as this would cause an undue compliance burden on the organization to structure and process the data. By unstructured data, we mean data may reside in data streams or lakes and may not be in a processed or structured form.

Topic / Locations refer to text within the Personal Data Protection (Amendment) Bill 2020	Summary of Concerns and Recommendations
	To summarise, we recommend that the "whitelist" of data categories exclude types of data that provide no clear value to individuals' ability to switch providers, and/or take time for organisations to process, including (i) user activity data generated from the use of proprietary tools or features, (ii) user-generated content (such as voice recordings, videos, images, customer reviews and feedback), and (iii) unstructured data. **Exceptions.** In addition, paragraph 48 of the Public Consultation document states that exceptions to the Data Portability Obligations will mirror those to the Access Obligation under the Fifth Schedule to the PDPA; however, we note that these exceptions are not included in the PDP Amendment Bill. **We strongly recommend that these exceptions (and the further exclusions we propose above) be codified in legislation, similar to how the exceptions to the Access Obligation are included in the Fifth Schedule to the PDPA.** This will provide certainty and consistency in the implementation of the new provisions. We also request that MCI/PDPC commits to consulting with industry prior to the development of prescribed requirements in the Regulations, and the new Data Portability Obligation comes into effect.
9) Clause 13: New Part VIB / Amendment to Section 26G: Porting of applicable data (2) Subject to subsections (3), (5) and (6), the porting organisation must, upon receiving the data porting request, transmit the applicable data specified in the data porting request to the receiving organisation in accordance with any requirements prescribed.	The ACCA strongly recommends that if data portability is mandated, that the time and scope of this provision should be limited. In the EU, several abuses under such EU GDPR's provision occurred in the past when individuals submitted multiple onerous requests within a short timeframe that created operations burden that negatively impacted businesses. It is very costly to respond to such a request, especially given the broad scope of this right, and this right should thus be limited "with reasonable intervals."
10) Clause 13: New Part VIB / Amendment to Section 26G: Porting of applicable data	The ACCA suggest that the GDPR's portability provision could be followed in this instance, as a broad data portability right proposed in this amendment could pose to be problematic.

Topic / Locations refer to text within the Personal Data Protection (Amendment) Bill 2020	Summary of Concerns and Recommendations
(3) Subsection (2) applies only if the following are satisfied: (a) the data porting request satisfies any requirements prescribed; (b) the porting organisation, at the time it receives the data porting request, has an ongoing relationship with the individual.	GPPR and some other laws restrict the right to data portability to data provided by the individual to the organization and such right does thus not cover generated / user activity data, or data provided by third parties.
11) Clause 13: New Part VIB / Amendment to Section 26G: Porting of applicable data (6) A porting organisation must not transmit any applicable data about an individual under subsection (2) if — (a) the transmission of the applicable data can reasonably be expected to — (i) threaten the safety, or physical or mental health, of an individual other than the individual to whom the applicable data relates; (ii) cause immediate or grave harm to the safety, or physical or mental health, of the individual to whom the applicable data relates; or (iii) be contrary to the national interest;	The ACCA suggests adding the following clause after 6(a)(iii): "(iv) cause a breach of the organisation's or a third-party's intellectual property rights or confidential information."
12) Clause 13: New Part VIB / Amendment to Section 26H: Transmission of personal data under data porting request (2) A porting organisation may disclose personal data about T to a receiving organisation	Similar to above, this amendment could possibly cause a serious breach of the third-person's privacy. For example, this would mean that a spouse of an individual may obtain the "web surfing behaviour" of the spouse of another individual. The ACCA suggests adding an additional clause along the lines of "I cause a breach of the organisation's or a third-party's intellectual property rights or confidential information."

Topic / Locations refer to text within the Personal Data Protection (Amendment) Bill 2020	Summary of Concerns and Recommendations
without T's consent only if the data porting request — (a) is made in P's personal or domestic capacity; and (b) relates to P's user activity data or user-provided data.	
13) Clause 17 / Amendment of Section 29 Increase in financial penalty cap: the maximum financial penalty to (i) up to 10% of an organization's annual gross turnover in Singapore; or (ii) S$1 million, whichever is higher.	The ACCA recommends deleting "10% annual gross turnover". Civil penalties should not be tied to a regulated entity's turnover, and should be proportionate to the harm caused to the data subjects and whether there are any aggravating or mitigating factors. Civil penalties frameworks should also not impose undue hardship on an otherwise responsible entity. If PDPC nonetheless imposes the revenue-based maximum financial penalty, then the PDP (Amendment) Bill should clarify that the cap is based on turnover "in Singapore", which would reflect PDPC's intention as stated in paragraph 58 of the Public Consultation document. To avoid penalising organisations that act in good faith, PDPC should also consider introducing a provision that it may impose a financial penalty only if the infringement has been committed knowingly or recklessly.
14) Clause 18 / New Section 31A / Further clarification to "voluntary undertakings" scheme including on due process and appeals mechanisms.	The ACCA recommends that the PDPC clarify that voluntary undertakings are undertakings that are proposed by an organization or person, and such undertakings (including any variations) will not be imposed by the PDPC, without prior agreement from the relevant organization. In addition, given the requirements that failure to "comply with an undertaking" could result in the voluntary undertaking being publicized and cost recovery (proposed Section 31A-5) – we also recommend that PDPC avoid mandating that organizations or persons to be subject to the voluntary undertaking mechanism – and provide organizations or persons the ability to reject such a proposed undertaking, without prejudice.

Topic / Locations refer to text within the Personal Data Protection (Amendment) Bill 2020	Summary of Concerns and Recommendations
15) Clause 20 / Amendment to Section 35B: Unauthorized disclosure of personal data (1) If I the individual does so — (i) knowing that the disclosure is not authorised by the organisation or public agency, as the case may be; or (ii) reckless as to whether the disclosure is or is not authorised by the organisation or public agency, as the case may be, the individual shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $5,000 or to imprisonment for a term not exceeding 2 years or to both.	The ACCA notes that there may be cases where an employee of an organization may not be in a position to assess if disclosure is authorized. If their employer orders/the job processes requires them to share data, the individual should not be held liable for simply doing their job as instructed by their employer which is expected to only give instructions that are in line with applicable law, unless it should be obvious to the employee that the latter is not the case. This applies to all similar sections related to offence throughout the PDPA. The ACCA suggests that these penalty clauses be clearly and narrowly defined based on the respective obligations under the PDPA. An employee should only be penalised if, and only if, the disclosure is done intentionally by the employee without authorisation from the organisation or public agency.