To: The Ministry Of Communications and Information and the Personal Data Protection Commission of Singapore
Re: Public Consultation on the Personal Data Protection (Amendment) Bill, Including Related Amendments to the Spam Control Act
Date: 28 May 2020

To Whom It May Concern

Amazon is grateful for the opportunity to provide comments on the Ministry of Communications and Information (MCI) and the Personal Data Protection Commissions' (PDPC)'s public consultation on "Draft Personal Data Protection (Amendment) Bill, Including Related Amendments To The Spam Control Act".

This submission reflects the combined view of both Amazon's retail and digital businesses and Amazon Web Services, our cloud computing business. Our response is rooted in the fact that Amazon's business depends on ensuring we have our customers' trust that we will protect their personal data.

We wish to commend the Singapore Government for the proposed amendments to the PDPA that take into account Singapore's evolving digital landscape and economy, the challenges posed by changing technology trends for data protection, the potential for data collection and analysis to yield benefits for individuals and society, and the global shift in data protection laws, while nonetheless still providing for effective protection of personal data. In particular, Amazon supports the intention of the proposed amendments to strengthen the accountability of organisations to build consumer confidence, enhance the PDPA's framework to enable meaningful consent while allowing organisations to use the data for legitimate interests for wider public or systemic benefit, and to provide consumers greater autonomy over their personal data.

Nonetheless, we have some concerns over the following amendments:

- **Mandatory Data Breach Notification (DBN)**: The definition of "data breach" does not make clear when the notification should be triggered. We recommend that the definition of "data breach" be aligned with international practices. Further clarification on the meaning of "significant harm" is also essential, to limit inconvenience for data subjects and prevent "notification fatigue". There is also a lack of clarity on the split of obligations between the data intermediary (DI) and the main organisation. Each party's obligations should be clearly defined.

- **New Data Portability Obligation:** Amazon's view is that broad data portability requirements should *not* be mandated. Instead, MCI/PDPC should work with industry to develop voluntary best practices that align to regional or international standards and codes of conduct. If MCI/PDPC nonetheless proceed 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, and that key exceptions be codified in the legislation. While we commend the PDPC for aspiring to reduce the compliance burden for organisations, there remains a litany of criteria for porting organisations to qualify a data porting request, placing an undue burden on porting organisations. We propose some amendments to the PDP Amendment Bill to reduce this burden. Finally, we welcome PDPC's stated intentions to work with

the industry to develop Regulations to implement the Data Portability Obligation, and we seek PDPC's commitment that they will consult on the various aspects, including the classes of porting organisations, "whitelist" of data categories, and technical and process details for transmission.

- **Increased Financial Penalty Cap.** Amazon's view is that 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. We recommend reverting to a financial penalty cap of up to $1 million. 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". To avoid penalising organisations that act in good faith, we recommend introducing a provision that PDPC may impose a financial penalty only if the infringement has been committed knowingly or recklessly.

- **Introduction of "voluntary undertakings" mechanism including on due process and appeals mechanisms:** We support voluntary undertaking schemes as a way to improve enforcement mechanisms. However, this scheme should reflect existing obligations of organisations and powers of the Commission.

- **Removal of the exclusion for organizations acting on behalf of public agencies from PDPA obligations**: The removal of this exclusion makes it unclear whether a DI would be reasonably expected to and whether it would be able to take on its relevant obligations given that the public agency it is acting on behalf for is not subject to the PDPA. We recommend the relevant sections be further amended to make clear that where the relevant processing activity relates to a DI acting on behalf of and for the purposes of a public agency, that such reasonable protection or retention should be in accordance with their contractual arrangements.

Our detailed comments are laid out in the pages below. Once again, we thank MCI/PDPC for the opportunity to respond to the Public Consultation. We hope to have an opportunity to discuss our submission in greater detail with you.

Yours sincerely,

Genevieve Ding
Head of Public Policy, Singapore & Asean Strategic Projects
Amazon Web Services & Amazon

geneding@amazon.com

DETAILED RESPONSE TO PUBLIC CONSULTATION DOCUMENT

1. **Mandatory Data Breach Notification (DBN) (Clause 12 of the PDP (Amendment) Bill).** Amazon supports the mandatory DBN, as we recognise that this will strengthen protection for individuals and organisations' accountability for the personal data in their care. Our specific responses below:

- **Recommendation: revise the definition of "data breach" to more clearly state when the DBN should be triggered. (proposed Section 26A).** Under the current formulation, the definition of a data breach is not tied to a security incident and in part (b) the phrase "likely to occur" captures potential data breaches which have not transpired. This is inconsistent with other DBN regimes such as the EU General Data Protection Regulation (GDPR) which defines a personal data breach as "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed". Linking a data breach to a security incident means that organisations can create effective mechanisms to constantly monitor threats, detect failures in security and trigger investigations. Moreover, because of the "likely to occur" language in limb (b) of the definition, organisations, including data intermediaries will be required to notify of potential data incidents, this will distract resources from investigating and curtailing the impact of any incident and potentially lead to over-notification causing notification fatigue. This issue is addressed in the GDPR definition which captures only actual unauthorized or unlawful process and in Article 34 that recognizes that notification should not be required if organizations have taken subsequent measures to address the risk. We recommend that MCI/PDPC can consider revising the definition of "data breach" to be more consistent with international practices, and ensuring that organisations' obligations are clearer by adopting the EU GDPR definition." **Our recommended revisions to the language in the PDP Amendment Bill, are reflected in the Appendix**.

- **Recommendation: further clarification on the meaning of "significant harm" (proposed Section 26B).** While we support the introduction of the "significant harm" threshold for a data breach affecting an individual to be notifiable, neither the Public Consultation Document nor the Bill provide clarity on what are the relevant thresholds and tests for a breach to be considered as having caused "significant harm". The lack of clarity on this threshold could result in the PDPC and individuals being inundated with numerous immaterial notices, resulting in "notification fatigue". This would in turn lead to inconvenience for data subjects, increase in administrative costs and burden for PDPC, and most importantly result in 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. We therefore **recommend that MCI/PDPC define or provide further clarification on the meaning of "significant harm" in Regulations.**

- **Recommendation: revise Section 26C(2) to make clear that data intermediaries do not have the obligation to monitor security breaches that are the responsibility of the main organization (proposed Section 26C(2)).** As currently proposed in the Bill, the DI is required to notify the organisation without undue delay where it has "reason to believe that a data breach has occurred". The proposed language is overbroad and confuses the obligations of the Data Intermediary and the main Organisation on whose instructions the Data Intermediary acts. The Data Intermediary's obligation to notify should apply where the Data Intermediary has actual knowledge of a data breach and the breach extends to data or systems over which the Data Intermediary exercises control and

has visibility into the content. As currently drafted, Data Intermediaries could be required to not only monitor their own systems but also proactively monitor the systems and content of the main organisation in order to be able to comply with their obligations, which blurs the responsibilities between the parties and could create a situation where the main organisation fails to implement its own appropriate security measures and monitoring systems because it expects the Data Intermediary to carry out these obligations on its behalf. **We therefore 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.** This is particularly relevant in the cloud services context, where instructions to process data are automated and cloud services providers do not have visibility into the purpose of such instructions to be able to determine whether an instruction to, for example, copy, modify or delete personal data is authorised. **Our recommended revisions to the language in the PDP Amendment Bill, are reflected in the Appendix**.

- **Recommendation: revise section 26(D) to make it clear that DIs are not required to notify the Commission and Individuals of a "notifiable data breach"**. While we support the requirement for DIs to notify organisations of data breaches "without undue delay", it should however remain the responsibility of the organisation to assess whether a data breach constitutes a "notifiable data breach" and notify the Commission and/or individuals, as the case may be. The current drafting of section 26(D) is ambiguous is to whether such notification obligations would apply to DIs. We therefore propose amendments to the language to make it clear that this obligation **would not apply to data intermediaries**, as MCI/PDPC intends. **Our recommended revisions to the language in the PDP Amendment Bill, are reflected in the Appendix.**

2**. New Data Portability Obligation. Clauses 13 and 16 of the PDP (Amendment) Bill.** Amazon recognises the potential of data portability to provide individuals with greater autonomy and control over their personal data. However, **we continue to recommend that broad data portability requirements should *not* be mandated**. Instead, MCI/PDPC should work with industry to develop voluntary best practices that align to regional or international standards and codes of conduct. Data portability frameworks should also be flexible and allow industry to use commercially negotiated terms and conditions offering customers tools and methods to move their data; easy contract termination provisions and pay as you go pricing – which would help addressing any potential "lock-in" concerns. We believe that mandated data portability, when tied to a specific process or standard may threaten innovation and contractual freedom, which in turn may adversely affect market development and harm consumers.

If MCI/PDPC nonetheless proceed 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 preprocessed 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. 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.**

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.

While we commend the PDPC for aspiring to reduce the compliance burden for organisations, there remains a significant compliance workload for porting organisations, including the need to make certain subjective assessments (which require manual, labour-intensive processes). Under the PDP Amendment Bill, in order to qualify a data porting request, a porting organisation would need to verify whether the data porting request satisfies prescribed requirements, whether the porting organisation has an ongoing relationship with the individual, whether the receiving organisation is formed or resident in Singapore and whether it is on a blacklist, whether the transmission of the applicable data can be reasonably expected to threaten the safety/physical/mental health of any individual or be contrary to the national interest, whether transmitting applicable data about an individual (P) would transmit personal data about another individual (T), and if so whether the data porting request is made in P's personal or domestic capacity. The porting organisation would then need to follow the prescribed technical requirements for the dataset in question. This litany of criteria would require organisations to implement complicated and resource-intensive compliance programmes, which may not be outweighed by the benefits to the requesting individual. **We would strongly recommend that MTI/PDPC closely examine the provisions and remove or reduce mandatory assessments that porting organisations would need to make.** In particular, sections 26G(6) and 26(H)(2) place an undue burden on porting organisations. **We explain our concerns more fully, and recommend revisions to these provisions, in the Appendix.**

Separately, data portability requirements also create an increased risk of cybersecurity challenges as portability tools can increase attack surface by enlarging the number of sources for attackers to siphon user data. In addition, if the mechanism by which data is ported (typically an API) is not implemented securely, unauthorised parties could use it to access data under the guise of portability requests. **Amazon would only support a mechanism of data transmission that meets our information security standards.**

We welcome PDPC's stated intentions to work with the industry to develop Regulations to implement the Data Portability Obligation. We believe this consultative process will be essential, and **we seek PDPC's commitment that they will consult on the various aspects, including the classes of porting organisations, "whitelist" of data categories, and technical and process details for transmission.**

3. **Increased Financial Penalty Cap. Clause 17 of the draft PDP (Amendment) Bill.** The clause proposes that the maximum financial penalty be (i) for organisations with an annual turnover exceeding $10 million, 10% of the organisation's annual turnover; or (ii) in any other case, $1 million.

Amazon's view is that 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. **We therefore recommend reverting to a financial penalty cap of up to $1 million.**

Mitigating factors could include (a) how actively and promptly the organization has tried to resolve the matter with the data subject; (b) whether reasonable steps to prevent or reduce the harm caused by the breach; and (c) whether the organisation has provided affected data subjects with remedies. Aggravating factors can include (a) whether the breach was intentional or repeated, including where the organization knew or should have reasonably known of the risk of the breach but continued with its operations without taking measures to minimise the risk or remedy the breach; or (b) if the organisation is in the business of handling sensitive personal data (e.g. health data), but failed to put in place safeguards that were adequate or proportional to the harm that might be caused to the data subject, should the personal data be disclosed.

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. **Our recommended revisions to the language in the PDP Amendment Bill, are reflected in the Appendix.**

4. Further clarification to "voluntary undertakings" scheme including on due process and appeals mechanisms. Clause 18 of the PDP Amendment Bill. We support voluntary undertaking schemes as a way to improve enforcement mechanisms. However, this scheme should reflect existing obligations of organisations and powers of the Commission. To that end we have proposed some changes to clarify the scope and operation of this scheme in the Appendix.

5. Further clarification on the applicability of the PDPA obligations to DI acting on behalf of public agencies that are not covered by the PDPA. Clause 3(a) of the PDP (Amendment) Bill.

While we are broadly supportive of the need to ensure accountability of third-parties, including DIs, that are acting on behalf of public agencies – 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. In this regard, it is unclear, for example what constitutes "reasonable security arrangements" pursuant to Section 24 of the PDPA, as the requirements for "reasonable security arrangements" for public agencies, are not transparent. 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. Our recommended revisions to the language in the PDP Amendment Bill, are reflected in the Appendix.**

APPENDIX: LIST OF ISSUES AND RECOMMENDATIONS

Legend: strikethroughs represent proposed deletions; and red text represents proposed inclusions

PROVISION FROM PDP (Amendment Bill)	RECOMMENDATION/SUGGESTION	JUSTIFICATION
Section 24	Protection of personal data 24. An organisation shall protect personal data in its possession or under its control by making reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks. **24A. Where section 24 applies to a data intermediary acting on behalf and for the purposes of a public agency, such reasonable security arrangements should be in accordance with contractual arrangements.**	Changes proposed as public agencies are not covered under the PDPA.
Section 25	Retention of personal data 25. An organisation shall cease to retain its documents containing personal data, or remove the means by which the personal data can be associated with particular individuals, as soon as it is reasonable to assume that — (a) the purpose for which that personal data was collected is no longer being served by retention of the personal data; and (b) retention is no longer necessary for legal or business purposes. **25A. Where section 25 relates to a data intermediary acting on behalf and for the purposes of a public agency, the obligations outlined in Section 25 should be in accordance with contractual arrangements.**	Changes proposed as public agencies are not covered under the PDPA.
Section 26A	**26A.** In this Part, unless the context otherwise requires — "data breach", in relation to personal data, means — ~~**(a) the unauthorised access, collection, use, disclosure, copying, modification or disposal of personal data;**~~	The definition of "data breach" as the trigger for notification is not clear and inconsistent with data breach notification regimes elsewhere in the world. We propose the amendments, which are consistent with international practices.

PROVISION FROM PDP (Amendment Bill)	RECOMMENDATION/SUGGESTION	JUSTIFICATION
	~~or~~ ~~(*b*) the loss of any storage medium or device on which personal data is stored in circumstances where the unauthorised access, collection, use, disclosure, copying, modification or disposal of the personal data is likely to occur.~~ **a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed."**	
Section 26C(2)	(2) Where a data intermediary ~~has reason to believe~~ **becomes aware** that a data breach has occurred in relation to**: (i)** personal data **controlled by the data intermediary that it** ~~that the data intermediary~~ is processing on behalf of and for the purposes of another organisation**; or (ii) the systems controlled by the data intermediary that the other organization uses to store or process personal data** — (a) the data intermediary must, without undue delay, notify the other organisation of the occurrence of the data breach; and (b) the other organisation must, upon notification by the data intermediary, conduct an assessment of whether the data breach is a notifiable data breach in accordance with subsection (1).	Proposed amendments to clarify that the data intermediary would not be expected to monitor for security breaches that are within the main organization's control and responsibility.

PROVISION FROM PDP (Amendment Bill)	RECOMMENDATION/SUGGESTION	JUSTIFICATION
Inserted after Section 26C(3)	**(4) A data intermediary has no obligations under sub-section (2) in cases where the actual or possible access, collection, use, disclosure, copying, modification or disposal of personal data are a result of, or consistent with, instructions given to the data intermediary from the organization requesting the processing.**	Data intermediaries should not have an obligation to proactively monitor or verify whether the instructions of an organization, on whose behalf the data intermediary processes personal data, are authorized or lawful.
Section 26D(1)	Where an organisation**, other than a data intermediary,** assesses, in accordance with section 26C, that a data breach is a notifiable data breach, the organisation must 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.	The current language in Clause 26D(1) currently does not make it clear that the duty to notify **does not apply to data intermediaries**, which we understand is the intention of MCI/PDPC.
Section 26G(6)	A porting organisation **is not required to** transmit any applicable data about an individual under subsection (2) if –	It is extremely onerous and against data subjects' interests for a porting organisation to review applicable data to determine whether the content meets the specified scenarios. In some cases, it would be impossible for the porting organisation to make the determination in any meaningful way. We note that these criteria are more complicated to operationalise in the context of the Data Portability Obligation (which involves user activity data and third parties' data) as compared to the Access Obligation. Proposed changes therefore make it optional for organisations apply the criteria.
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 from *P* **satisfies any requirements prescribed. –** ~~**(a) is made in P's personal or domestic capacity; and**~~ (b) ~~**relates to P's user activity data or user-provided data.**~~	It is extremely onerous for the porting organisation to review applicable data to determine whether transmitting applicable data about an individual (*P*) would transmit personal data about another individual (*T*), and if so whether the data porting request is made in P's personal or domestic

PROVISION FROM PDP (Amendment Bill)	RECOMMENDATION/SUGGESTION	JUSTIFICATION
		capacity. It is also not clear why there is a separate concept of "user activity data or "user-provided data" to qualify this request. Proposed changes require porting organisations to only verify that the data porting request from *P* satisfies prescribed requirements. The prescribed requirements for the data porting request can include statements that the request is being made in P's personal or domestic capacity.
Section 29(d)(2A)	(2A) For the purposes of subsection (2)(*d*), **the Commission may impose a financial penalty only if it is satisfied that the infringement has been committed knowingly or recklessly, and** the amount of the financial penalty must not exceed — (*a*) where the direction is given to an organisation or a person with an annual turnover exceeding $10 million **in Singapore** (as ascertained from the most recent audited accounts of the organisation or person available at the time the direction is given), and the failure to comply that is the subject of the direction occurs on or after the date of commencement of section [17] of the Personal Data Protection (Amendment) Act 2020 — 10% of the annual turnover **in Singapore**; or (*b*) in any other case — $1 million.	Proposed changes to more clearly reflect that any annual turnover calculation is based on the turnover recorded in Singapore, and adding a "knowing" and "reckless" standard to avoid penalising organisations that act in good faith.
Section 31A(2)	Without limiting the matters to which the voluntary undertaking may relate, the voluntary undertaking may include any of the following undertakings by the organisation or person**, in order to comply with relevant provisions in the Act as outlined in subsection (1)**:	All actions reflected in 31A(2) should be tied back to actual obligations that the organization has under the Act.

PROVISION FROM PDP (Amendment Bill)	RECOMMENDATION/SUGGESTION	JUSTIFICATION
	(*a*) an undertaking to take specified action **to comply with a provision under Parts III to VI of the Act** within a specified time; (*b*) an undertaking to refrain from taking specified action **to comply with a provision under Parts III to VI of the Act**; (*c*) an undertaking to publicise the voluntary undertaking.	
Inserted after Section 31A(3)	**31A-3(X) Notwithstanding subsection (3):** **(a) an organisation or person may withdraw or vary the undertaking at any time, but only with the written consent of the Commission; and** **(b) the Commission may, by written notice given to the organization or person, cancel the undertaking.**	Propose an inclusion for a mechanism to cancel the voluntary undertaking otherwise it would be in effect for perpetuity.
Section 31A(4)	(4) Where an organisation or a person fails to comply with any undertaking in a voluntary undertaking, the Commission may give the organisation or person any direction that the Commission thinks fit in the circumstances to ensure the compliance of the organisation or person with that undertaking**, in accordance with the powers conferred onto the Commission pursuant to Part VII of this Act.**	To clarify pursuant to 31A(4), if an organization or person does not comply with the undertaking, the Commission should only have the same powers it has under the Act to enforce breaches of the PDPA. "The Commission may exercise any powers of Enforcement it has under this Act.
Section 31A(5)	(5) In addition, where an organisation or a person fails to comply with an undertaking mentioned in subsection (2)(*c*), the Commission may ~~**publicise the voluntary undertaking in accordance with the undertaking**~~ **exercise any powers of enforcement granted to the Commission under this Act**~~**and recover the costs and expenses so incurred from the organisation or person as a civil debt due to the Commission.**~~".	We propose deletion of this part, as these are not currently captured