To: Personal Data Protection Commission of Singapore
Re: Public Consultation for Approaches to Managing Personal Data in the Digital Economy
Date: October 5, 2017

To Whom It May Concern,

Amazon is grateful for the opportunity to provide comments on the Personal Data Protection Commissions' public consultation on "Approaches to Managing Personal Data in the Digital Economy."

The below answers to the questions posed in the consultation document reflect the combined view of both Amazon's retail and digital businesses and Amazon Web Services, our cloud computing business. Amazon is at the forefront of the digital economy globally and in Singapore, and our business depends on ensuring we have our customers' trust that we will protect their personal data.

We wish to commend Singapore for recognizing that – due to advancements in big data, Internet of Things, artificial intelligence, and machine learning – the historic model of "informed consent" is unsustainable. It is already the case that normal data subjects encounter more privacy notices in a day than there is time to actually read and digest that content. We therefore commend Singapore for "thinking big" (one of our core leadership principles) on how personal data can sustainably be managed in the age of digital economy and as Singapore truly becomes a Smart Nation. We strongly support the proposed introduction of "notification of purpose" and "business and legal purpose" as alternative frameworks under which personal data can be collected and processed.

With regards to the mandatory data breach notification, we favor the introduction of breach notification systems that incentivize organizations to maintain robust protections for personal data, while enabling data subjects to take action to protect themselves when their data is compromised. We believe any such system should be crafted based on the following core principles".

- ensure that users receive timely and meaningful notifications about data breaches that create material risk of identity theft or other economic loss;
- incorporate a risk-based trigger for the notification obligation to ensure consumers are not overwhelmed with breach notifications in instances where there is no credible risk of harm
- provide reasonable timeframe for organizations to fully investigate the scope and potential impact of a breach, take the steps necessary to prevent further disclosures, and undertake a risk analysis to determine the extent of exposure so as to ensure that consumers receive actionable information

Once again, we thank the Commission for the opportunity to respond to the Public Consultation. We hope to have an opportunity to discuss our submission in greater detail with the Commission.

Sincerely,

Quint Simon
Head of Public Policy, ASEAN
Amazon Web Services

simquint@amazon.com
+65 81515381

RESPONSE TO PUBLIC CONSULTATION DOCUMENT

Part 1: Additional Bases for Collecting, Using and Disclosing Personal Data

We agree with the Commission's proposal to expand the current consent-based regime for handling personal data to include two additional bases for handing personal data:

- notifying individuals of the purpose of the handling ("**Notification of Purpose**"); and
- handling personal data for a legal or business purpose ("**Legal or Business Purpose**").

We welcome the Commission's thoughtfulness and leadership in this area, by contemplating a modernized personal data protection regime that will ensure Singapore continues to have a modern, yet time-proof, privacy framework. As recognized by the Commission, these two additional bases for handling personal data will create more flexibility for organizations and will keep Singapore's data protection regime in step with developments in technology and global privacy regulation. This is especially important in fields such as the Internet of Things, data analytics and machine learning, where responsible personal data handling can result in vast societal and economic improvements and gains.

1. **Should the PDPA provide for Notification of Purpose as a basis for collecting, using and disclosing personal data without consent?**

   Yes. Notification of Purpose would be useful where it is not practical to obtain prior or contemporaneous consent. This approach will enable the adoption of advanced technologies and innovation, including big data, internet of things, machine learning and artificial intelligence, in line with Singapore's Smart Nation strategy.

   We further note that the Notification of Purpose is in line with privacy practices in other jurisdictions, as identified in the PDPC's Public Consultation Paper.

2. **Should the proposed Notification of Purpose approach be subject to conditions? If so, what are your views on the proposed conditions (i.e., impractical to obtain consent and not expected to have any adverse impact on the individual)?**

   No. Notification of Purpose should itself be a legitimate approach to collecting, using and disclosing personal information as an alternative to obtaining consent. This is in line with, for example, Australia's privacy regime.

   We believe all legal bases should be treated as equal legal grounds for handling personal data, and not as exceptions to one another. In particular, the ability of organizations to use the two new bases proposed by the Commission should not have to depend on whether it is practical or not to

obtain consent in the first instance. In our experience, conditions are likely to create ambiguity and this may limit the usefulness of the Notification of Purpose approach. Regarding the two specific conditions proposed by the Commission, it is unclear what circumstances would render consent "impractical", or what criteria organizations can reasonably rely upon in determining the handling of personal data is "not expected to have adverse impact".

3. **Should the PDPA provide for Legal or Business Purpose as a basis for collecting, using and disclosing personal data without consent and notification?**

   Yes. This is a welcome approach to collect, use and disclose personal data.

4. **Should the proposed Legal or Business Purpose approach be subject to conditions? If so, what are your views on the proposed conditions (i.e., not desirable or appropriate to obtain consent and benefits to the public clearly outweigh any adverse impact or risks to the individual)?**

   Consistent with our response to Question 2, we support the idea that all legal bases should be treated as equal legal grounds for handling personal data, as opposed to complicated exceptions to one another. Subjecting the use of the Legal or Business Purpose approach to conditions will create ambiguity and limit its usefulness for organizations.

   Regarding the two conditions proposed by the Commission, they are widely subjective and open to multiple interpretations. It is unclear what circumstances would make it "*not desirable or appropriate to obtain consent from the individual*" (paragraph 3.15a of the Consultation Paper) or when there would be "*benefits to the public (or a section thereof)*" (paragraph 3.15b of the Consultation Paper).

   With respect to the condition in paragraph 3.15b of the Consultation Paper, it is also unclear whether a private organization would be considered to be "*the public (or a section thereof)*." A private organization could be handling personal data for an internal legitimate purpose, including activities to detect or prevent fraud or cybersecurity incidents. It is also foreseeable that some applications of technology would only benefit a particular private organization (e.g., data analytics on the organization's employees' work processes to derive better ways to enhance organizational efficiencies). In such circumstances, the proposed conditions would make it unclear whether the organization can rely on the Legal and Business Purpose approach to handle the personal data in question.

   It follows that subjecting the Legal or Business Purpose approach to conditions could unintentionally stifle the use of modern and emerging technology like data analytics and machine learning, which would run counter to the Commission's stated intent of ensuring that "*the regulatory environment keeps pace with evolving technology in enabling innovation*."[1]

[1] At paragraph 2.5 of the Consultation Paper.

We also note that the legitimate interest basis in the European Union's ("**EU**") General Data Protection Regulation ("**GDPR**"),[2] on which the Legal and Business Purpose was modeled,[3] is not subject to the two conditions the Commission is proposing and considered as a legal basis just as valid as consent.[4] The GDPR legitimate interest basis allows organizations to expand business opportunities and yet remain compliant with their overall data protection obligations.

Part 2: Mandatory Breach Notification

We favor the introduction of breach notification systems when they incentivize organizations to maintain robust protections for personal data, while enabling data subjects to take action to protect themselves when their data is compromised.

Any such system should be carefully crafted to ensure that users receive timely and meaningful notifications about actual data breaches that create material risks of identity theft or other economic loss. To this end, the PDPA should clearly define the personal data that is subject to breach notification.

A sophisticated data breach framework should recognize that the mere act of notification itself may not necessarily yield better security or privacy for data subjects. A risk-based trigger for the notification obligation is necessary to ensure consumers are not overwhelmed with breach notifications in instances where there is no credible risk of harm. To ensure that consumers receive actionable information, reasonable time should also be given for organizations to investigate the scope and potential impact of a breach, take the steps necessary to prevent further disclosures, and undertake a risk analysis to determine the extent of exposure. Furthermore, the requirement to notify should apply when the relevant personal data is acquired, disclosed, lost, or destroyed, rather than merely accessed.

With this background, we offer our responses to Questions 5 through 8 of the Consultation Paper below, along with some additional comments on the Commission's proposed breach notification regime for data intermediaries.

1. **What are your views on the proposed criteria for data breach notification to affected individuals and to PDPC? Specifically, what are your views on the proposed number of affected individuals (i.e., 500 or more) for a data breach to be considered of a significant scale to be notified to PDPC**?

---

[2] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC.

[3] We refer in particular to paragraph 3.12 of the Consultation Paper where the Commission referred to the legitimate interest basis in the EU.

[4] It is worth noting that the equal validity of the different legal basis available in the European framework was validated in 2011 by a decision of the Court of Justice of the European Union, which required amendments to the Spanish implementation of the framework for overly restricting the use cases of the legitimate interest basis.

Individuals

We urge the PDPC to require notifications of breaches only if there is a material risk of identify, theft or economic loss.

In line with this approach, the PDPA should clearly define the personal data that is subject to breach notification. The types of personal data that trigger this requirement should also be limited to types of personal data that are more likely to cause significant harm if there is unauthorized disclosure, for instance, a data breach that involves personal data such as NRIC number, health information, financial information or passwords. For example, in the Philippines the data privacy laws require notification only if the data breach relates to "sensitive personal information" or data which could be used to commit identity fraud. In the US, as well, typically data breach notification requirements are triggered only upon exposure of information that can lead to fraud or identity theft, such as financial account information or medical / biometric information.

Additionally, we urge the Commission to clarify that the term "affected individuals" refers only to individuals who have a nexus to Singapore. Otherwise the breach notification requirement could be triggered even if, for example, the breach only affects foreign nationals who are all situated in a foreign country.

However, we do agree with and support the PDPC's recommendation that there be different criteria and different notification obligations to individuals and to the Commission. Amazon believes that the threshold for notifying individuals should be if there is material risk of identity theft or economic loss, no matter the number of individuals affected. The PDPC's suggestion to allow organization to notify individuals as soon as practicable after becoming aware of a data breach is welcome and appropriate.

PDPC

Meanwhile, notification to the PDPC should be limited to circumstances where at least 500 individuals are required to be notified from a single incident as above. The proposal by the PDPC that it be notified "even if the breach does not pose any risk of impact or harm to the affected individuals" is unduly burdensome on organizations and is inconsistent with notification practices elsewhere in the world, including several states in US. Without incorporating these two criteria, companies will be incentivized to over-notify PDPC which will both divert resources and likely create notification fatigue within PDPC.

2. **What are your views on the proposed concurrent application of PDPA's data breach notification requirements with that of other laws and sectoral regulations?**

During a data breach incident, the focus and resources of an organization should be dedicated to responding to or handling the security incident. Resources should not be directed into notifying multiple government agencies during that critical period.

As such, we urge the Government of Singapore to establish a single point of notification, perhaps within PDPC, which would then be in charge of disseminating the key information to the relevant ministries.

3. **What are your views on the proposed exceptions and exemptions from the data breach notification requirements?**

The PDPC's exemptions are welcome.

However, we recommend clarifying that the "technological protection exception" under paragraph 6.10b of the Consultation Paper applies to all technical means of rendering breached data unusable, unreadable or indecipherable to an unauthorized third party. While encryption of data at rest is one means for accomplishing that objective, we urge the Commission to keep the exception technologically neutral in order for it to allow and incentivize other mechanisms, and avoid becoming obsolete by focusing on a certain technology.

Consistent with our response to Question 5, we also request that the Commission explicitly include an exception that covers the situation where the organization that experienced the breach makes a determination that the risk of harm to the individuals in question is low (e.g., if the breached personal data is already publicly available information).

4. **What are your views on the proposed time frames for data breach notifications to affected individuals and to PDPC?**

Data Intermediaries

The requirement for data intermediaries / processors to notify the relevant organisation immediately regardless of the risk of harm or the scale of impact of the data breach is not practical and is out of line with international practice. Even in the EU's GDPR regime the requirement is of a lower standard being "without undue delay" and in several US states the applicable standard is "without unreasonable delay". This standard allows organizations to assess the risk of harm and impact of a security incident without creating impractical and overly burdensome reporting obligations on data intermediaries.

Affected individuals

The PDPC's suggestion to allow organizations to notify individuals as soon as practicable after becoming aware of a data breach is welcome and appropriate provided that this applies to a data breach where there is a material risk of identify, theft or economic loss.

Notification to the PDPC

The proposed notification timeframe is unduly burdensome and may result in resources being diverted towards notification and compliance and away from managing and mitigating the impact of the incident particularly as a different timeframe has been proposed for notifying individuals compared to the PDPC.

As noted by the Public Consultation Paper under other regulatory regimes there is a wide range of applicable timing for notification to the regulator. For example, in the US in California notification is required "as expediently as possible", and in other US states, entities are required to notify the regulator after undertaking an investigation to confirm the breach. In Australia, the regulations enable entities to undertake an assessment if they become aware that there are reasonable grounds to suspect that there has been an eligible data breach but do not have reasonable grounds to believe an actual data breach has occurred (and must take all reasonable measures to complete this assessment within 30 days). The requirement to notify the regulator is triggered in Australia if after that assessment the entity concludes that an eligible data breach has actually occurred.