October 4, 2017

Personal Data Protection Commission
460 Alexandra Road
#10-02 PSA Building
Singapore 119963

PUBLIC CONSULTATION FOR APPROACHES TO MANAGING PERSONAL DATA IN THE DIGITAL ECONOMY

BSA | The Software Alliance[1] ("**BSA**") and the US-ASEAN Business Council[2] ("**US-ABC**") greatly appreciate this opportunity to comment on the changes to Singapore's Personal Data Protection Act ("**PDPA**"), as proposed by the Personal Data Protection Commission ("**Commission**") in its public consultation paper of July 27, 2017 ("**Consultation Paper**").[3]

The members of our organizations are at the forefront of data-driven innovation, including cutting-edge advancements in data analytics, machine learning, and the Internet of Things, among others. They have made significant investments in Singapore, which accounted for nearly 30 percent of all US investment into Asia in 2015. To ensure consumers and businesses alike can trust in and reap the maximum benefits from these innovations, our members remain deeply committed to protecting personal data across technologies and business models.

The continued development of modern and emerging technologies requires a legal framework that is clearly defined yet flexible enough to remain relevant long-term in a highly dynamic environment. In this regard, BSA and US-ABC commend the Commission for its leadership in developing and implementing the existing personal data protection regime in Singapore, which provides clear guidance and yet flexibility in how personal data is to be collected, used, or disclosed.

---

[1] BSA | The Software Alliance (www.bsa.org) is the leading advocate for the global software industry before governments and in the international marketplace. Its members are among the world's most innovative companies, creating software solutions that spark the economy and improve modern life. With headquarters in Washington, DC, and operations in more than 60 countries, BSA pioneers compliance programs that promote legal software use and advocates for public policies that foster technology innovation and drive growth in the digital economy.

BSA's members include: Adobe, Amazon Web Services, ANSYS, Apple, Autodesk, AVEVA, Bentley Systems, CA Technologies, Cisco, CNC/Mastercam, DataStax, DocuSign, IBM, Intel, Microsoft, Oracle, salesforce.com, SAS Institute, Siemens PLM Software, Splunk, Symantec, The MathWorks, Trend Micro, Trimble Solutions Corporation, and Workday.

[2] For over 30 years, the US-ASEAN Business Council has been the premier advocacy organization for US corporations operating within the dynamic Association of Southeast Asian Nations ("ASEAN"). Worldwide, the council's 150-plus membership generates over $6 trillion in revenue and employs more than 13 million people. Members include the largest US companies conducting business in ASEAN, and range from newcomers to the region to companies that have been working in Southeast Asia for over 100 years. The council has offices in Washington, DC; New York, New York; Bangkok, Thailand; Hanoi, Vietnam; Jakarta, Indonesia; Kuala Lumpur, Malaysia; Manila, Philippines; and Singapore.

[3] The Commission's public consultation paper titled "Public Consultation for Approaches to Managing Personal Data in the Digital Economy", issued on July 27, 2017 and available at https://www.pdpc.gov.sg/legislation-and-guidelines/public-consultations.

We further commend the Commission on its present efforts to review the data protection regime to ensure that it stays relevant to today's digital economy. In support of that effort, we offer comments on the Commission's proposals to amend the PDPA to introduce:

- two additional bases for collecting, using, and disclosing (collectively, "**handling**") personal data; and
- a mandatory data breach notification regime.

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**").

While we recognize that consent can be a valid way of legitimizing the handling of personal data, consent should not only be the only or primary way of doing so. Privacy and data protection regulators around the world have long debated the challenges and limitations presented by consent-based models.[4] We therefore welcome the Commission's thoughtfulness and leadership in this area, by contemplating alternatives 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.

Please also see our responses to Questions 1 through 4 of the Consultation Paper below.

Responses to Consultation Questions

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

BSA/US-ABC Response: Yes. We support the inclusion of the Notification of Purpose basis for handling personal data, for the reasons above and detailed by the Commission in the Consultation Paper.

Question 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)?

BSA/US-ABC Response: No. The Notification of Purpose approach should not be subject to conditions.

We strongly 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

[4] For instance, the FTC Report of 2012 already referred to the need to simplify consumer choices. Opinion 06/2014 of Article 29 Working Party clarifies that consent is one of several legal grounds to process personal data, rather than the main ground. In 2016, the Office of the Privacy Commissioner in Canada also published a discussion paper exploring potential enhancements to consent under the Personal Information Protection and Electronic Documents Act.

is practical or not to obtain consent in the first instance. In our experience, conditions will create ambiguity and will hinder reliance on the Notification of Purpose approach.

Regarding the two conditions proposed by the Commission, it is unclear what circumstances would render consent "*impractical*" (paragraph 3.8a of the Consultation Paper), or what criteria organizations can reasonably rely upon in determining the handling of personal data is "*not expected to have adverse impact*" (paragraph 3.8b of the Consultation Paper).

Instead, a requirement for organizations to perform a risk and impact assessment prior to relying on the Notification of Purpose, as proposed by the Commission in paragraph 3.10 of the Consultation Paper, is a superior approach that avoids unnecessary ambiguity. This should be sufficient to safeguard the interests of individuals, and organizations should then be able to confidently rely on the Notification of Purpose basis to handle personal data. That said, we note that the Commission has not set out what the risk and impact assessments would entail, and we would appreciate guidance in this regard. In addition, we would also like to clarify whether organizations may leverage risk and impact assessments conducted in other jurisdictions for purposes of relying on the Notification of Purpose basis for handling personal data.

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

BSA/US-ABC Response: Yes. We support the inclusion of the Legal or Business Purpose basis for handling data, for the reasons above and detailed by the Commission in the Consultation Paper.

Question 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)?

BSA/US-ABC Response: No. The Legal or Business Purpose approach should not be subject to conditions.

Consistent with our response to Question 2, we firmly 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 hinder reliance by organizations on it.

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 or 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*."[5]

We also note that the legitimate interest basis in the European Union's ("**EU**") General Data Protection Regulation ("**GDPR**"),[6] on which the Legal or Business Purpose was modeled,[7] is not subject to the two conditions the Commission is proposing and is a legal basis just as valid as consent.[8] The GDPR legitimate interest basis allows organizations to expand business opportunities and yet remain compliant with their overall data protection obligations.

We therefore recommend that the Legal or Business Purpose approach not be subject to any conditions. Similar to the Notification of Purpose approach, requiring organizations to perform a risk and impact assessment prior to relying on the Legal or Business Purpose approach, as proposed by the Commission in paragraph 3.17 of the Consultation Paper, should be sufficient to safeguard the interests of individuals. That said, and similar to the risk and impact assessments contemplated in paragraph 3.10 of the Consultation Paper, we note that the Commission has not set out what the risk and impact assessments would entail, and we would appreciate guidance in this regard. In addition, we would also like to clarify whether organizations may leverage risk and impact assessments conducted in other jurisdictions for purposes of relying on the Legal or Business Purpose basis for handling personal data.

Should the Commission decide to retain either or both of its proposed conditions, we recommend that the Commission expressly incorporate:

a. the legitimate interest of the organization as a factor to be weighed against the impact or risks to the individual; and
b. an exception to allow the handling of personal data by organizations, without consent, for the purposes of:
    i. fraud detection and prevention;
    ii. administration and analyses within a group of affiliated organizations for internal purposes (e.g., to improve operational efficiencies, provide internal training, etc.); and/or
    iii. ensuring network and information security.[9]

MANDATORY DATA BREACH NOTIFICATION

We favor the introduction of breach notification systems when they incentivize organizations to maintain robust protections for personal data, while enabling individuals 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. Such a definition ideally consists of an individual's name or other clear

[5] At paragraph 2.5 of the Consultation Paper.

[6] 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.

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

[8] 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.

[9] In relation to sub-paragraphs i., ii., and iii., the EU has expressly recognized that legitimate interests of an organization would include handling personal data for the purposes of preventing fraud, internal administration within a group of related organizations, and/or ensuring network and information security (see Recitals 47, 48, and 49 of the GDPR).

identifier in combination with information which if acquired creates the material risk that identity theft or other fraud will occur (e.g., financial account number, national identification number, home address).

A sophisticated data breach framework should recognize that the mere act of notification itself may not necessarily yield better security or privacy for individuals. A risk-based trigger for the notification obligation is necessary to ensure that individuals and the Commission are not overwhelmed with breach notifications in instances where there is no credible risk of harm. To ensure that the notification contains 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.

Responses to Consultation Questions

Question 5: 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?

BSA/US-ABC Response: The Commission is proposing that breach notifications must be given for "*any risk of impact or harm to the affected individuals*"[10] or "*even if the breach does not pose any risk of impact or harm to the affected individuals*"[11] (emphases added).

A better approach would be to require notifications of breaches only if there is a material risk of identity theft or economic loss. Otherwise "notification fatigue" may result, where the individual or the Commission is notified of data breaches when no serious harm is likely to occur from those breaches, and becomes unduly inconvenienced or overlooks taking appropriate action in cases where there is an actual risk of material harm.

Furthermore, establishing two different trigger criteria and different notification obligations to individuals and the Commission (depending on which criterion applies) unnecessarily complicates the breach notification regime. The more complicated the regime, the more resources an organization will need to expend on determining when the notification requirement is triggered and to whom notifications must be made. This unnecessarily diverts attention and resources away from remedying or mitigating the breaches in question.

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 and whose data is not handled in Singapore.

To simplify the regime and provide clarity to organizations on when and to whom they need to provide breach notifications, we recommend adopting a single notification requirement and criterion by:

i. eliminating the requirement in paragraph 6.2b of the Consultation Paper;

[10] Paragraph 6.2a) of the Consultation Paper.

[11] Paragraph 6.2b) of the Consultation Paper.

ii. amending the requirement in paragraph 6.2a of the Consultation Paper such that notifications need to be made to both the Commission and affected individuals only where the breach in question poses a material risk of identity theft or economic loss to affected individuals; and
iii. clarifying that the term "affected individuals" refers to individuals who have a nexus to Singapore.

Should the Commission decide to retain the two separate notification requirements and criteria, we recommend that the changes described in sub-paragraphs ii. and iii. above should still be made.

Question 6: What are your views on the proposed concurrent application of PDPA's data breach notification requirements with that of other laws and sectoral regulations?

BSA/US-ABC Response: In the immediate aftermath of a security incident, organizations should be focusing their time and resources on investigating and remediating the breach in question, rather than diverting them to making multiple notifications to multiple regulatory agencies.

We accordingly recommend that, regarding paragraph 6.3a of the Consultation Paper, it should be sufficient for the notification to be made only to the sectoral or law enforcement agency. Requiring concurrent notification to the Commission will divert resources without providing any additional safeguard for consumers. Therefore, notification to the Commission should be required only in circumstances where an organization is not already required to make such a notification to a sectoral regulator or to law enforcement.

Question 7: What are your views on the proposed exceptions and exemptions from the data breach notification requirements?

BSA/US-ABC Response: The proposed exceptions and exemptions in paragraphs 6.9 through 6.11 of the Consultation Paper are helpful.

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).

Question 8: What are your views on the proposed time frames for data breach notifications to affected individuals and to PDPC?

BSA/US-ABC Response: Our industry's experience informs us that specifying a fixed deadline in which to notify data breaches is impractical and does not acknowledge the sophistication of today's hackers nor the challenging nature of a forensic investigation. The time required to perform a thorough remediation effort varies with the size, severity, and complexity of the underlying security breach.

More importantly, it is our experience that imposing arbitrary deadlines may reduce the benefit to consumers of a breach notification law. Organizations that suffer a data breach should be encouraged to focus their resources on investigating the scope of the incident, preventing further disclosures, and restoring the integrity of any impacted data systems. Unless the vulnerability is

addressed prior to making the incident public, both the organization that experiences the breach and the affected individuals will be at risk of suffering further harm.

Recognizing these variables, the Commission has wisely proposed that organizations provide affected individuals with notification "*as soon as practicable*". However, we are concerned that this sound policy approach could be undermined by the requirement to provide notification to the Commission "*no later than 72 hours from the time it is aware of the data breach*". Consistent with our response to Question 5, a single notification timeframe should apply to notifications to individuals and notifications to the Commission. This is preferable to multiple notification timeframes which will result in the diversion of resources to determine which notification timeframe applies.

We accordingly recommend that the timeframe for breach notification, whether for a notification to an individual or a notification to the Commission, be "*as soon as practicable*" and not reference a specific number of hours.

To the extent that the Commission adopts a notification obligation that references a specific number of hours, we recommend that the Commission make it clear that the obligation:

i. is only applicable to the organization that originally collected the personal data (as compared to a service provider of that collecting organization); and
ii. is only triggered when that organization confirms and has actual knowledge that the breach necessitates notification to the Commission.[12]

Obligations of Data Intermediaries

Concerning the Commission's proposals in paragraphs 6.6 through 6.8 of the Consultation Paper, we welcome the Commission's clarification that where an organization uses a data intermediary, any arising obligation to provide breach notification to individuals and/or the Commission rests primarily on the organization (and not the data intermediary). However, we are of the view that this clarification itself would be sufficient, and that there is no need to impose an additional statutory requirement on the data intermediary to notify the organization it serves of a data breach. Such breach notification, and the timeframe for notification, should instead be left to contractual negotiations between the organization and the data intermediary.

Should the Commission decide to impose a mandatory notification obligation on data intermediaries, the requirement to notify immediately is impractical. It takes time for the intermediary to determine what happened, and which customers may have been affected by an incident. Instead of being required to send the notification immediately, data intermediaries should only need to notify the organizations they serve "*as soon as practicable*". This would allow the intermediaries sufficient time to investigate and determine the scope of an incident and necessary remedial measures.

Further, the notification requirement should only be triggered when a data intermediary has actual knowledge of the breach. For instance, a data intermediary should not be held liable for failure to provide timely notice if they are unable to access the data necessary to identify the occurrence of a breach (e.g., where the data intermediary is prohibited, under its contract with the organization in question, from investigating the attributes and characteristics of the data it is processing or hosting for the organization).

[12] We note the Commission has proposed in footnote 43 of the Consultation Paper that *"[i]n certain cases, an organisation may require more than 72 hours to confirm the breach and obtain the necessary details of the incident. In such a scenario, the organisation should still notify PDPC with as much information as possible within the 72 hours and provide PDPC with the remaining information as soon as possible.*" For clarity, we recommend that the Commission clarify that the 72-hour window for notification will not begin until such time as the organization has determined that notification to the Commission is necessary.

In view of the above, we recommend that:

i. the Commission not impose any mandatory breach notification obligations on data intermediaries; and
ii. if the Commission decides to impose such mandatory obligations, the data intermediary should only need to make the notification to the organization in question as soon as practicable after the data intermediary has actual knowledge of the breach.

CONCLUSION

Once again, BSA and US-ABC greatly appreciate the opportunity to provide these comments. We look forward to continuing to work with the Commission on its review of the PDPA, and we stand ready to answer any questions you may have.

Yours faithfully,

BSA | The Software Alliance and **the US-ASEAN Business Council**