BSA Response to Public Consultation on the Draft Personal Data Protection (Amendment) Bill

May 28, 2020

BSA | The Software Alliance (**BSA**)[1] appreciates the opportunity to provide comments in response to the public consultation by the Personal Data Protection Commission (**PDPC**) and the Ministry of Communications and Information (**MCI**) on the *Personal Data Protection (Amendment) Bill 2020* (the **Bill**) amending the *Personal Data Protection Act 2012 (**PDPA**)*. The Bill is the culmination of several consultations on aspects of the proposed legislation over the last few years and for which BSA has provided comments previously.

Summary of major points

BSA generally supports the Bill and its objectives. In our comments below, we propose or reiterate recommendations that we hope will improve the Bill and increase the likelihood the amendments will further the Government of Singapore's objectives. Specifically, we have proposed comments and recommendations on:

- Strengthening accountability — notification criteria, reporting criteria and data intermediary notification obligations
- Enabling meaningful consent — deemed consent and legitimate interests of organisations
- Increasing consumer autonomy — data portability, derived personal data, user activity data and multiple consecutive requests for data
- Strengthening effectiveness of enforcement — penalties and statutory undertakings
- Continuing the robust consultation with industry stakeholders during subsequent rule making processes

Statement of Interest

BSA members are enterprise solutions providers that create the software-enabled products and services that power other businesses. They offer tools including cloud storage services, customer relationship management software, human resources management programs, identity management services, cybersecurity solutions, and collaboration software. These enterprise software companies are in the business of providing privacy protective solutions and their business models do not depend on monetizing

[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 30 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, Atlassian, Autodesk, AVEVA, Bentley Systems, Box, Cadence, Cisco, CNC/Mastercam, IBM, Informatica, Intel, MathWorks, Microsoft, Okta, Oracle, PTC, Salesforce, ServiceNow, Siemens Industry Software Inc., Sitecore, Slack, Splunk, Synopsys, Trend Micro, Trimble Solutions Corporation, Twilio, and Workday.

300 Beach Road
#25-08 The Concourse
Singapore 199555

P +65 6292 2072
F +65 6292 6369
W bsa.org

Regional Representative Office
UEN: S97RF0005K

users' data. BSA members recognize that companies must earn consumers' trust and act responsibly with their personal data.

As such, BSA advocates globally for the implementation of personal data protection laws that increase the transparency of personal data collection and use; enables and respects informed choices by providing governance over that collection and use; provides consumers with control over their personal data; provides robust security; and promotes the use of data for legitimate business purposes.[2]

BSA strongly supports the Government of Singapore's commitment to a national personal data protection regime that strengthens accountability and consumer trust in personal data management while enhancing flexibility for the responsible use of personal information to drive innovation and economic growth and recovery.

Comments

Strengthening Accountability — Personal Data Breach Notification

Organizations should notify consumers as soon as practicable after discovering a personal data breach involving the unauthorized acquisition of unencrypted or unredacted personal data that creates a material risk of harm to data subjects. BSA supports the introduction of mandatory breach notification systems that incentivize organizations to maintain robust protections for personal data while enabling individuals to take action to protect themselves when their data is compromised. BSA responded positively to the proposed mandatory data breach reporting requirements in the consultation[3] and remains generally supportive of proposed amendments to implement them in the Bill.

Notification criteria

According to the proposed amendments, in order to determine whether and to whom it needs to report, an organization that has experienced a data breach involving personal information must assess the risk of significant harm to the affected individual(s) or determine the number of individuals affected by the breach.

A sophisticated data breach framework should recognize that the mere act of notification itself may not necessarily yield better security or privacy for individuals. Instead, a risk-based trigger for the notification obligation recognizes that the number of affected individuals is less important than the nature of the personal data breached and the consequent risk of harm such a breach poses to the affected individuals.

Therefore, we are concerned that establishing notification requirements based on the number of affected individuals alone may unnecessarily complicate the breach notification regime by diverting the attention and resources of an organization away from remedying or mitigating the breaches in question. Moreover, it could also result in the individuals and the PDPC being overwhelmed with breach notifications in instances where there is no credible risk of harm or impact determined to the affected individuals.

Additionally, we urge the Government of Singapore 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.

[2] See BSA's Global Privacy Best Practices at: https://www.bsa.org/files/policy-filings/A4_2018_BSA_Global_Privacy_Best_Practices.pdf

[3] Public Consultation for Approaches to Managing Personal Data in the Digital Economy – 27 July 2017. BSA's submission may be found here: https://www.bsa.org/policy-filings/singapore-bsa-usabc-submission-to-consultation-part-i-on-personal-data-protection-act

To simplify the regime and provide clarity to organizations on when and to whom they need to provide breach notifications, **we recommend:**

i **eliminating the requirement in the proposed section 26B(1)(b) of the PDPA;**
ii **amending the requirement in the proposed section 26D of the PDPA such that notifications need to be made to both the PDPC and affected individuals only where the breach in question results in, or is likely to result in, significant harm to the affected individuals; and**
iii **clarifying that the term "affected individuals" refers to individuals who have a nexus to Singapore in the proposed section 26A of the PDPA.**[4]

We commend the Government of Singapore's inclusion of the "technological protection exception" under the proposed section 26D(5) of the PDPA. Applying the exception to all technical means of rendering breached data unusable, unreadable, or indecipherable to an unauthorized third party is an important clarification in the Bill. While encrypting data is one means for accomplishing that objective, it is commendable that the Government of Singapore ensures the exception is technologically neutral to allow and incentivize other mechanisms of data protection and prevent the exception from becoming obsolete.

However, we recommend that if an effective technological protection is in place or other remedial actions have been implemented, an affected organization should not be required to report to the PDPC.

We therefore recommend amending proposed section 26D(1) of the PDPA to be subject to the proposed sections 26D(4) and (5) of the PDPA.

In addition, for the sake of clarity, **we recommend that section 26D(2) of the PDPA explicitly state that it is subject to the proposed section 26D(5) of the PDPA.**

We commend the addition of a prescribed list of data to assist organizations in assessing significant risk to an individual. BSA assumes that such a list will be included in implementing regulations and suggests it should include such data types as the individual's name or other clear 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).

Reporting timeline

To ensure that the breach 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.

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.

[4] See clause 12 of the Bill.

Recognizing these variables, the Government of Singapore 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, including "all the information that is prescribed for this purpose" to the PCPC no later than three-days from the time it made the assessment that the data breach is reportable.[5] Again, requirements such as this unnecessarily divert attention and resources away from remedying or mitigating the breaches in question.

Therefore, **we recommend deleting "but in any case no later than 3 days" from the proposed section 26D(1) of the PDPA.** If the Government of Singapore nonetheless decides to maintain a three-day notification period, **we recommend that the proposed sections 26D(1) and 26D (3) should be amended to clarify that the initial notification, subject to the three-day period, does not require "all the information" prescribed to be provided at the same time, and instead allow the remaining information to be provided in phases without undue delay.** This approach would be consistent with that taken in Article 33 of the EU's General Data Protection Regulation (GDPR), and would allow an affected organization to focus limited resources on understanding and mitigating the breach rather than on immediately developing a full report to the PDPC within three days.

BSA also recommends that notification of an incident to the Commission be initially kept confidential to help prevent further breaches until appropriate mitigation measures are in place by the organization. Following the public announcement of an incident, malicious actors can take advantage of the situation by attempting to further compromise an organization publicly identified. Organizations will not always be able to determine the root cause of an incident within the three-day notification period and could still be vulnerable to further incidents, hence the need for confidentiality.

Data intermediary notification obligations

In the proposed section 26C(2) of the PDPA, a data intermediary (DI) is required to notify the organization it is processing data on behalf of "without undue delay" where it has "reason to believe that a data breach has occurred". This is an important provision, but the notification trigger is overly broad and risks confusing the responsibilities between the organization and the DI. As currently drafted, this section could be interpreted as a requirement for DIs to proactively monitor the systems and content of the organization they are processing data on behalf of to comply with notification obligations under the Bill.

This raises particular challenges in the cloud computing services context, where instructions to process data are frequently automated. Cloud services providers typically do not have information regarding the purpose of such instructions to be able to determine whether a particular instruction to, for example, copy, modify, or delete personal data is authorised.

To clarify that the DI's obligation to notify are to be limited to breaches to data or systems over which it exercises direct control, **BSA recommends the proposed section 26C(2) of the PDPA be amended as follows:**

> **"Where a data intermediary has reason to believe that a data breach has occurred <u>in systems under which it exercises direct control in</u> relation to personal data that the data intermediary is processing on behalf of and for the purposes of another organisation —"**

Data intermediary data obligations to public agencies

BSA is broadly supportive of the amendment to section 4(1)(c) of the PDPA removing the exclusion of organizations acting on behalf of public agencies. We note however that it could cause some uncertainty regarding a DI's data retention and protection obligations noted in sections 24 and 25 of the PDPA given that these requirements for public agencies are not publicly available.

[5] Proposed 26D(3) – see clause 12 of the Bill.

BSA recommends that sections 24 and 25 of the PDPA be 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 reasonable protection or retention requirements should be in accordance with their contractual arrangements.

Enabling meaningful consent

Deemed Consent

BSA agrees with the proposal to expand the scope of deemed consent for handling personal data to include deemed consent by contractual necessity and deemed consent by notification. We also support the proposal to introduce exceptions based on legitimate interest and business improvement. These proposals will enhance the protection of individuals' personal data while promoting responsible use of personal data by businesses. BSA supported the Government of Singapore's initial proposals to include additional legal bases for collecting, using, and disclosing personal data and we remain supportive of these proposals in the Bill.[6]

Privacy and data protection regulators around the world have long debated the challenges and limitations presented by consent-based models. We recognize that consent is a valid way of legitimizing the handling of personal data. However, consent should not be the primary mechanism. Additional mechanisms, where appropriate, should be recognized as equivalent legal grounds for processing rather than as exceptions to consent. In relation to this, the concept of deemed consent by contractual necessity would be more appropriately recognized as a separate, and equivalent, legal grounds for processing rather than as a subset of consent. We note that this is also the approach taken by the EU in Article 6.1(b) of the GDPR.

Legitimate interests of organizations

BSA supports the general idea that organizations should weigh the interests of data subjects in determining whether to process data on the grounds of legitimate interest. However, any such consideration should be undertaken based on the type of data at issue and should not require an individualized assessment for each data subject.

The proposed First Schedule (Part 3) of the PDPA under legitimate use and the proposed section 15A(3)(a) of the PDPA under deemed consent both propose a granular assessment based on each individual before collection, use, or disclosure of personal data about the individual. This type of assessment is more appropriately conducted at a higher level akin to the type of considerations attached to the GDPR's legitimate interest exception. The GDPR's legitimate interest exception allows processing necessary for purposes of the legitimate interests pursued by the controller or a third party where such interests are not "overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data."

Increasing consumer autonomy — Data portability

Data Portability

BSA promotes a user-centric approach to privacy that provides consumers with mechanisms to control their personal data in a safe and deliberate manner. As such, BSA supports encouraging data portability for consumers in privacy legislation. It is important to ensure that such a right may be flexibly implemented based on internationally recognized standards and practices and minimizes conflicting legal obligations on organizations.[7]

[6] Public Consultation on Managing Unsolicited Commercial Messages and the Provision of Guidance to Support Innovation in the Digital Economy – 27 April 2018. See BSA's joint filing with the US-ASEAN Business Council at: https://www.bsa.org/files/policy-filings/06072018BSA_USABC_Submission.pdf

[7] Public Consultation on Review of the Personal Data Protection Act 2012 – Proposed Data Portability and Data Innovation

Derived Personal Data

The Bill explicitly limits an organization's data portability obligations to individuals with an existing direct relationship with the organization. The Bill also limits the obligation to user provided and user activity data held in electronic form. We commend the Government of Singapore for appropriately excluding "derived personal data" from the obligation.

However, as currently written, the Bill raises a potential overlap between the definitions of "derived personal data" and "user activity data".

Therefore, **BSA recommends changing the proposed definition for "derived personal data" in the proposed section 2(1)(a)(b) of the PDPA to:**

> **"does not include personal data resulting from the individual's use of any product or service or derived by the organisation using any prescribed means or method;"**

Further, since the word "created" (which characteristically means to make something new) could imply that an organization is creating new data by virtue of individual's use of the product or service, thus blurring the lines with "derived data", **we recommend that the definition of "user activity data" in the proposed section 2(1)(b) of the PDPA be changed as follows:**

> **"'user activity data', in relation to an organization, means personal data about an individual that is ~~created~~ generated in the course or as a result of the individual's use of any product or service provided by the organisation;"**

Multiple consecutive requests for data

BSA suggests that the time and scope of the proposed section 26G of the PDPA should be limited. In the EU, several abuses under the GDPR's data portability provision occurred when individuals submitted multiple onerous requests within a short timeframe creating an operational burden on the organization inconsistent with the intention of the data portability provision. **BSA recommends that the proposed section 26G(3) of the PDPA be amended to limit data access requests to "reasonable intervals".**

Strengthening effectiveness of enforcement

Penalties

A central regulator should have the tools and resources necessary to ensure effective enforcement. Remedies and penalties should be proportionate to the harm resulting from violations of data protection laws.

We note the addition of extended criminal liability for knowing or reckless unauthorized disclosure of personal data. BSA's position is that criminal penalties are not proportionate remedies for violation of data protection laws.

We also note the increased financial penalty cap in the Bill. It is BSA's position that civil penalties should not be set arbitrarily or based on factors that lack a substantial connection to the context in which the underlying harm arose such as a regulated entity's annual turnover. To do so risks imposing undue hardship on an otherwise responsible entity. **Civil penalties should not be tied to a regulated entity's turnover but should instead be proportionate to the harm caused to the data subjects, and to any aggravating or mitigating factors.**

If the Government of Singapore nonetheless imposes the revenue-based maximum financial penalty, **BSA recommends the Bill state that the cap is based on turnover "in Singapore"**, reflecting the intention stated in paragraph 58 of the Public Consultation document.

Provisions – 22 May 2019. See BSA comments at: https://www.bsa.org/files/policy-filings/07172019pdpcdataportability.pdf

To avoid penalizing organizations that act in good faith, the Government of Singapore should also consider introducing a provision stating that it may impose a financial penalty only if the infringement has been committed intentionally or negligently, similar to section 69(3) of the Competition Act.

Statutory undertakings

BSA notes with interest the proposal in the Bill to introduce alternative resolution processes via a voluntary statutory undertakings regime As a general principle, it seems reasonable to apply more flexible and individually tailored approaches to resolving issues that reflects the existing obligations of organizations and powers of the PDPC. However, we recommend that there be an express clarification that where an organization chooses not to enter into a voluntary undertaking, this will be without prejudice to the organization's legal rights (including rights of defence against any action against the organization), particularly when there could be public release of information.

Conclusion

BSA is grateful for the opportunity to provide these further comments on the proposed amendments to the PDPA. We remain supportive of the Government of Singapore's efforts to continually review and update the personal data protection regime in Singapore, responding to the ever-evolving needs of the digital economy and data innovation. We hope that our comments will support the Government's efforts and to ensure that Singapore continues to be a hub of cutting-edge innovation and a leader for the creation of sound data innovation policy.

It is important to note that several of the proposed amendments, including those related to the data breach notification requirement, the data portability right, and other matters will require substantial rule making from the Government of Singapore to implement and provide necessary guidance to industry and other stakeholders. **It is critical that the Government of Singapore conduct thorough consultations with interested stakeholders when developing, and prior to finalizing, such rules and guidance. BSA looks forward to actively participating in such consultations.**

Please do not hesitate to contact us if you have any questions or comments regarding our suggestions. We remain open to further discussion and look forward to further opportunities to work with the Government of Singapore on the development of data protection and data policy issues in Singapore.

If you require any clarification or further information in respect of this submission, please contact the undersigned at brianf@bsa.org or +65 8328 0140.

Yours faithfully,

Brian Fletcher

Director, Policy – APAC

BSA | The Software Alliance