September 7, 2018

Department of Data Protection
Aras 6, Kompleks Kementerian Komunikasi dan Multimedia,
Lot 4G9, Persiaran Perdana,
Presint 4 Pusat Pentadbiran Kerajaan Persekutuan,
62100 Putrajaya, Malaysia

PUBLIC CONSULTATION FOR THE IMPLEMENTATION OF DATA BREACH NOTIFICATION

BSA | The Software Alliance[1] ("**BSA**") and the US-ASEAN Business Council[2] ("**US-ABC**") greatly appreciate this opportunity to comment on Malaysia's Department for Data Protection's ("**JPDP**") PUBLIC CONSULTATION PAPER NO.1/2018 on the Implementation of Data Breach Notification ("**Consultation Paper**").[3]

Our member companies are at the forefront of data-driven innovation, including cutting-edge advancements in data analytics, machine learning, and the Internet of Things, among others. 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 regulatory frameworks that are clearly defined yet flexible enough to remain relevant long-term in a highly dynamic environment. In this regard, BSA and US-ABC commend the Commissioner for its leadership in developing and implementing the existing personal data protection regime in Malaysia.

GENERAL

The adoption for a framework for data breach notification ("**DBN Framework**") can promote trust in the digital economy by establishing expectations for data stewardship that will reduce

[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 data user 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 JPDP's public consultation paper titled "PUBLIC CONSULTATION PAPER No. 1/2018: THE IMPLEMETATION OF DATA BREACH NOTIFICATION", available at http://www.pdp.gov.my/images/pdf_folder/PCP-1-2018-DBN-Ver2.pdf.

the risk of future breaches and ensure that data subjects receive timely and meaningful information about whether their personal information has been compromised. We favor the introduction of breach notification systems when they incentivize data users 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 incentivize data users to notify, whilst ensuring that data subjects receive timely and meaningful notifications about actual data breaches that create material risks of identity theft or financial fraud. To achieve these objectives, we support a breach notification system that is consistent with the following key principles:

- The notification standard should be risk-based so that data users can take steps to mitigate the potential impact of data breaches that create significant risks of material harm. The standard should promote good data storage practices by clarifying that data rendered indecipherable to unauthorized entities through use of encryption or other obfuscation technologies does not create such risks.
- In the immediate aftermath of a data breach, data users should be encouraged (and afforded adequate time) to focus their resources on performing a thorough investigation and restoring the integrity of potentially compromised systems.
- Data subjects should generally expect to receive notification from the organization with whom they have a direct relationship, the data user. Such a principle promotes good data stewardship, ensuring that data users who collect confidential personal information take a life cycle approach to managing the associated privacy and security risks. Contracts between a data user and its third-party data processers should remain enforceable, allowing an efficient allocation of risks.

More information on the key principles can be found in the BSA International Cybersecurity Policy Framework.[4]

With this background, we offer our responses to the Commissioner's proposed operational "Elements in Data Breach Notification" as well as three additional considerations to the proposed data breach notification, namely:

- Implementation of the data breach notification system under existing legal frameworks and interaction with other laws and legislation.
- Scope of application and criteria for breach notification.
- Operational elements in data breach notification.

Responses to the Consultation

BSA/US-ABC Clarification: How will the proposed data breach notification system be implemented under existing legal frameworks? How does the proposed data breach notification system interact with other domestic laws and legislations?

The Commissioner has stated that the implementation of the DBN Framework is aimed at assisting data users in personal data breach management and provides a framework to help data users take proactive steps to contain the damage caused by a breach incident. In addition, the DBN Framework is intended to enable enforcement authorities and regulators to conduct investigations thoroughly, transparently, and fairly.

To achieve these aims, it is imperative that the Commissioner clarify how the proposed DBN Framework would be implemented under existing legal frameworks. The Public Consultation Paper suggests that the Commissioner intends to implement the DBN Framework by "imposing conditions to the certificate of registration issued by the Commissioner to the data users." We seek clarification about the mechanisms by which registered data users will be required to

[4] More information can be found under the section "Ensure a Consistent, Reasonable Standard for Personal Data Breach Notification", on page 10. The document can be found here: http://bsacybersecurity.bsa.org/wp-content/uploads/2018/04/BSA_cybersecurity-policy.pdf

demonstrate that they have met the DBN Framework conditions. The Commissioner may also wish to clarify how the data breach notification system interacts and operates with other laws. In addition, it is very important that any information that is disclosed to the Commissioner as part of a DBN Framework should be kept strictly confidential and should not be disclosed to other regulators, enforcement agencies, or third parties.

BSA/US-ABC Clarification: What is the scope of application and criteria for breach notification?

We urge the Commissioner to maintain a streamlined set of criteria for data users to determine whether to notify the Commissioner and data subjects. The more complicated the determining criteria is, the more resources a data user 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.

As the Commissioner contemplates how to structure the DBN Framework, we offer the following recommendations:

Risk-Based Trigger for Notification: The DBN Framework should recognize that the mere act of notification itself may not necessarily yield better security or privacy for data subjects. In this regard, DBN obligations should be limited to breaches that create a "material risk of identity theft or financial fraud." Such a risk-based trigger for the notification is necessary to ensure that data subjects and the Commissioner are not overwhelmed with breach notifications in instances where there is no credible risk of harm. Furthermore, the requirement to notify should apply when the relevant personal data is acquired, disclosed, lost, or destroyed, rather than merely accessed. For example, the requirement to notify should not apply in situations where the data user takes action to remedy the breach prior to such breach resulting in a material risk of identity theft or financial fraud. Finally, to promote the use of best-in-class data storage practices, the risk-based standard should clarify that breaches involving data rendered indecipherable to unauthorized entities through use of encryption or other obfuscation technologies does not create "material risks" to data subjects.

Timeline for Notification: To ensure that the notification contains actionable information, reasonable time should also be given for data users 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. Affording companies a reasonable time frame for such efforts (as opposed to a fixed deadline for notification) helps to prevent additional collateral damage and ensures that affected data subjects receive the information they need protect themselves from identity theft and financial fraud.

Scope of Covered Entities: The Commissioner should also clearly define the scope of applicable data users to which the data breach notification system would apply. For example, it is not clear whether only registered data users[5] need to comply with the DBN Framework or whether the obligations would apply to all data users, whether they are registered or not.

In addition, when a data user uses a data processor, breach notification to data subjects and/or the Commissioner should rest on the data user (and not the data processor). This is because data processors generally do not have visibility over the data users' data and would not be in a position to provide the relevant information requested by the DBN Framework. Data processors also do not generally have direct relationships with data subjects and are therefore unable to meaningfully or effectively communicate matters relating to a personal data breach to data subjects directly. For example, cloud service providers ("**CSPs**") may not know if a data user has stored personal data on the service, the estimated number of affected data subjects or the

[5] Pursuant to *Division 2* of the *PDPA 2010* and by way of *Gazette* by the Minister.

potential risk of harm to data subjects. Given so, CSPs would not be in a position to provide relevant data requested by the DBN Framework

Exceptions from DBN Obligations: The Commissioner should also consider if there are any circumstances where data users *must not notify individuals*. For example, in circumstances where notification to affected individuals is likely to impede law enforcement investigation, or where notification would result in a breach of a legal obligation under any other law.

Operational Elements in Data Breach Notification

Section C: Notification
C(2): Have the other Regulatory bodies/Law enforcement agencies been notified?

BSA/US-ABC Response: In the immediate aftermath of a security incident, data users 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 Element C2 of the Consultation Paper, it should be sufficient for the notification to be made by the data user only to the sectoral regulator or law enforcement agency, consistent with the reporting obligations (including notification templates and timelines) of the sectoral regulatory authority. Concurrent notification to the Commissioner will divert resources without providing any additional safeguard for consumers. Therefore, notification to the Commissioner should be considered only in circumstances where a data user is not already required to make such a notification to a sectoral regulator or to a law enforcement agency.

Section C: Notification
C(5): Notification to the Commissioner must be made not later than 72 hours after having become aware of the breach.

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 data subjects of a breach notification law. Data users that suffer a data breach should be encouraged to focus their resources on investigating the scope of the incident, preventing further breaches, and restoring the integrity of any impacted data systems. Unless the vulnerability is addressed prior to making the incident public, both the data user that experiences the breach and the affected data subjects will be at risk of suffering further harm.

Recognizing these variables, we are concerned that the requirement to provide notification to the Commissioner "*not later than 72 hours after having become aware of the breach*" would not be practicable and accordingly result in a misallocation of time and resources, when data users should be focused on investigating and remediating the breach in question.

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

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

i. is only applicable to the data user that originally collected the personal data (as compared to a service provider of that data user); and

ii. is only triggered when that data user confirms and has actual knowledge that the breach meets the criteria for notification to the Commissioner.
iii. Lastly, we recommend a flexible approach be adopted that does not preclude data users from voluntarily notifying data subjects prior or in parallel to the DBN Framework notification requirements in order to minimize the impact of a breach.

Section D: Training and Guidance in Relation to Data Protection
D(1): Does the organization provide training/awareness program to staff members prior to the incident?

BSA/US-ABC Response: The proposed DBN Framework should also define "staff members / employees" subject to training and awareness programs as being employees directly involved in the handling and processing of personal data only.

CONCLUSION

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

Yours faithfully,

Dr. Jared W Ragland
Senior Director, Policy – APAC
BSA | The Software Alliance

Amb. Michael W. Michalak
Senior Vice President & Regional Managing Director
US-ASEAN Business Council