Draft Notification of the Personal Data Protection Committee on Rules and Methods of Personal Data Breach Notification under the Personal Data Protection Act 2019

Comments from BSA | The Software Alliance

November 22, 2022

Introduction

BSA | The Software Alliance (**BSA**)[1] welcomes this opportunity to provide our comments to the Ministry of Digital Economy and Society (**MDES**) and Office of the Personal Data Protection Committee (**PDPC Office**) regarding the draft Notification on Rules and Methods of Personal Data Breach Notification under the Personal Data Protection Act (**Notification**). BSA is the leading advocate for the global software industry before governments and in the international marketplace. We have extensive experience engaging with governments around the world to promote effective, internationally interoperable legal systems that protect personal information and provide strong consumer rights while supporting responsible uses of data-driven technologies.

In the past few years, BSA has followed with great interest developments related to the Personal Data Protection Act (**PDPA**). We value our engagements with the PDPC Office and are glad to have met for an in-person discussion November 15, 2022. This submission adds to a list of recommendations BSA has provided on the PDPA and its draft subordinate regulations and implementing rules, with a listing of the submissions and the respective online links below:

- BSA Comments on the Draft Notification of Appropriate Personal Data Protection for International Transfer Under the Personal Data Protection Act 2019[2]
- BSA Comments on Thailand's Personal Data Protection Act 2019 Draft Implementing Rules[3]

[1] BSA's members include: Adobe, Alteryx, Altium, Amazon Web Services, Atlassian, Autodesk, Bentley Systems, Box, Cisco, CNC/Mastercam, CrowdStrike, Dassault, Databricks, DocuSign, Dropbox, Graphisoft, IBM, Informatica, Intel, Kyndryl, MathWorks, Microsoft, Nikon, Okta, Oracle, Prokon, PTC, Rockwell, Salesforce, SAP, ServiceNow, Shopify Inc., Siemens Industry Software Inc., Splunk, Trend Micro, Trimble Solutions Corporation, TriNet, Twilio, Unity Technologies, Inc., Workday, Zendesk, and Zoom Video Communications, Inc.

[2] https://www.bsa.org/policy-filings/thailand-bsa-comments-on-the-draft-notification-of-appropriate-personal-data-protection-for-international-transfer-under-the-personal-data-protection-act-2019

[3] https://www.bsa.org/policy-filings/thailand-bsa-comments-on-thailands-personal-data-protection-act-2019-draft-implementing-rules

300 Beach Road
#30-06 The Concourse
Singapore 199555

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

Regional Representative Office
UEN: S97RF0005K

- Third Group of Draft Subordinate Regulations under the Personal Data Protection Act 2019[4]
- Second Group of Draft Subordinate Regulations under the Personal Data Protection Act 2019[5]
- BSA's Comments on the Draft Subordinate Regulations under the Personal Data Protection Act 2019[6]
- BSA Comments on Dec 2018 Version of Thailand's Personal Data Protection and Cybersecurity Bill[7]
- Comments on Jan 2018 Version of Draft Personal Data Protection Act[8]
- BSA Comments to July 2017 Revisions of the Personal Data Protection Bill[9]
- Comments on Draft Personal Data Protection Act (2015)[10]

Definition of Personal Data Breach

Clause 3 of the unofficial translation of the draft Notification defines a "personal data breach" as one that involves "*a leak or breach of personal data security measures resulting from an intentional, willful, or negligent act or from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored, or otherwise processed without the consent of the data subject*".

This definition implies that a personal data protection violation — i.e., the processing of personal data without the consent of the data subject — is a data breach. However, this is not aligned with how a data breach is understood in personal data protection laws internationally. For example, Article 4(12) of the EU General Data Protection Regulation (**GDPR**) defines "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."* Section 26A of the Singapore Personal Data Protection Act (**Singapore PDPA**) defines "data breach", in relation to personal data, as *"the unauthorised access, collection, use, disclosure, copying, modification or disposal of personal data; or 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."*

[4] https://www.bsa.org/policy-filings/thailand-third-group-of-draft-subordinate-regulations-under-the-personal-data-protection-act-2019

[5] https://www.bsa.org/policy-filings/thailand-second-group-of-draft-subordinate-regulations-under-the-personal-data-protection-act-2019

[6] https://www.bsa.org/policy-filings/thailand-bsas-comments-on-the-draft-subordinate-regulations-under-the-personal-data-protection-act-2019

[7] https://www.bsa.org/policy-filings/thailand-bsa-comments-on-dec-2018-version-of-thailands-personal-data-protection-and-cybersecurity-bill

[8] https://www.bsa.org/policy-filings/thailand-comments-on-jan-2018-version-of-draft-personal-data-protection-act

[9] https://www.bsa.org/policy-filings/thailand-bsa-comments-to-july-2017-revisions-of-the-personal-data-protection-bill

[10] https://www.bsa.org/policy-filings/thailand-comments-on-draft-personal-data-protection-act

The definition of personal data breach in Clause 3 inappropriately combines a personal data protection violation with the occurrence of a data breach. Given that processing data without the consent of the data subject is a violation of personal data protection principles that should be covered separately rather than under the draft Notification for data breach notifications, **BSA recommends deleting the underlined section "or otherwise processed without the consent of the data subject."**

Introduction of Categories of Data Breaches

Clause 4 introduces categories of data breaches including Confidentiality Breach, Integrity Breach, and Availability Breach. Such categories are not listed in data protection laws and regulations of other jurisdictions. Instead, these categories may be described in non-binding guidelines or other measures. For example, these categories of data breaches are similar to those listed in the Guidelines 9/2022 on personal data breach notification under GDPR issued by the European Data Protection Board (**EDPB**) on October 10, 2022. However, Guidelines issued by the EDPB are suggestive, and not definitive nor are they mandatory. While we recognize that it is important to provide further context for data controllers and data processors to comply with the law, including this list of categories in the Notification is not consistent with international practice. **BSA recommends removing Clause 4 and, if desired, including the content in a guidance document that is not legally binding.**

Obligation of the Data Processor

Clause 6 sets out that if the data controller has an agreement or contract to delegate to the data processor the processing of personal data on its behalf, the data controller must also stipulate in a clause the data processor's obligation to notify the data controller of a personal data breach without undue delay (within 72 hours) after the data processor is aware of the breach. Certain data processors such as cloud service providers may not know if a data controller has stored personal data on the service, the estimated number of affected data subjects, or the potential risk of harm to data subjects. In many cases, a data processor's access to and knowledge of personal information collected by its enterprise customers are also limited by the privacy and security controls built into its product and enforced by contractual terms between the processor and its customers. In such situations, processors will be unable to provide such notification to the data controller, or such information related to the breach of personal information about which the data controller should notify PDPC.

Article 33(2) of the GDPR requires the processor to "*notify the controller without undue delay after becoming aware of a personal data breach*." Section 26C(3)(a) of the Singapore PDPA requires that a data intermediary "*processing personal data on behalf of and for the purposes of another organisation […] must, without undue delay, notify that other organisation of the occurrence of the data breach.*" Neither the GDPR nor the Singapore PDPA require the data processor to report specific information to the data controller. To align with international norms, **BSA recommends that the requirement in Clause 6 – "the data processor must notify the details of the personal data breach in Clause 5(2) of this Notification" should be deleted.**

Exemption from obligation to notify the PDPC Office

Clause 7 of the Draft Notification provides that the data controller may rely on the exemption from the obligation to notify the PDPC Office of a personal data breach if it can demonstrate that the personal data breach is unlikely to result in a risk to the rights and freedoms of data subjects. However, Clause 7 requires the data controller to submit the details of the reasons for the exemption to the PDPC, such as the details of security measures for personal data. The process

of seeking an exemption is not very different from submitting a notification of a personal data breach to the PDPC. The request for exemption must provide details of the personal data breach in order to provide context on the measures taken by the data controller for the protection of personal data.

Including the option of seeking an exemption from notification allows data controllers to determine that a personal data breach does not require such notification and therefore reduces the burden of unnecessary notifications on data controllers and the PDPC. Therefore, **BSA suggests replacing the requirement to submit exemptions to the PDPC with a requirement for data controllers to carry out an assessment of the potential personal data breach and keep an internal record of the assessment** that no notification to the PDPC Office is required. This would allow the PDPC Office to verify compliance with the personal data breach notification requirement where the need may arise. It would also reduce the regulatory burden on organizations and the PDPC Office.

Risk of notification fatigue

The Draft Notification requires that personal data breaches are reported to the PDPC Office with few exceptions. While there are two examples provided within the Attachment of the Notification that do not require notification to the PDPC Office, it appears that personal data breaches of low risk to data subjects nevertheless need to be reported. This may result in notification fatigue to both the PDPC Office and to data controllers, which erodes the effectiveness of the notification requirement. **BSA recommends that the threshold for notification to the PDPC Office be the unauthorized acquisition of unencrypted or unredacted personal data that creates a material risk of harm to data subject so that the PDPC Office and data controllers can appropriately focus their efforts on such breaches.**

Relying on public notices to notify data subjects

Clause 9 of the unofficial translation provides that the data controller may notify the data subject using public media and that the notification using public media "must not cause any damage to or impact on the data subject." This caveat is broad as it does not specify what constitutes "damage or impact on" the data subject. BSA suggests to either remove the caveat completely or to rephrase it as "The notification using public media must take into account the rights and interests of data subjects."

Examples of data breaches

To address the PDPC Office's question in the consultation website of whether the examples should be provided in a separate document, BSA is of the view that they should indeed be placed in a separate guidance document together with the categories of data breaches currently listed in Clause 4 of the Draft Notification. This will enable the non-binding examples to be separate from the Notification and allows the PDPC Office to amend and update the examples as necessary.

Conclusion

BSA appreciates the opportunity to provide our comments and recommendations on the draft Notification of the PDPA. We support the Government of Thailand's efforts in implementing the PDPA successfully and look forward to continue working with the MDES and the PDPC Office on privacy and personal data protection policies. Please do not hesitate to contact the undersigned at waisanw@bsa.org if you have any questions or comments regarding our suggestions.

Yours faithfully,

Wong Wai San

Senior Manager, Policy – APAC