Third Group of Draft Subordinate Regulations under the Personal Data Protection Act 2019

Comments from BSA | The Software Alliance

24 September 2021

Introduction

BSA | The Software Alliance (**BSA**)[1] welcomes this opportunity to provide our comments to the Ministry of Digital Economy and Society (**MDES**) regarding the third group of draft subordinate regulations under the Personal Data Protection Act (**PDPA**). 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.

Our comments on the consultation document for the third group of draft subordinate regulations build on the points made in our earlier submissions dated March 16 and June 30, 2021 on the proposed first and second groups of subpordinate regulations. These comments focus on measures designed to protect consumer privacy and personal data while supporting an internationally interoperable approach to data protection that enables companies to deliver global services that benefit the individuals and businesses they serve, creating local jobs and adding value to the Thai economy.

Our recommendations, discussed in greater detail below, address the following topics:

- Data Protection Impact Assessments (**DPIAs**) for High-risk Processing
- Obligations on Data Controllers Regarding Automated Processing
- Certifications

[1] BSA's members include: Adobe, Altium, Atlassian, Autodesk, AVEVA, Amazon Web Services, Bentley Systems, Box, Cisco, Dassault Systems, DocuSign, IBM, Informatica, Intel, Mastercam, MathWorks, Microsoft, Nikon, Okta, Oracle, PTC, Rockwell Automation, Salesforce, ServiceNow, Siemens PLM Software, Splunk, Synopsys, Trend Micro, Trimble Solutions Corporation, Twilio, Workday, Zendesk, and, Zoom.

300 Beach Road
#30-06 The Concourse
Singapore 19955

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

Regional Representative Office
UEN: S97RF0005K

- International Cooperation

BSA members create the technology products and services that power other businesses. Our members offer tools including cloud storage services, customer relationship management software, human resources management programs, identity management services, security solutions, and collaboration software. BSA members are enterprise software companies that are in the business of providing privacy protective technology products and services and their business models do not depend on monetizing users' data. BSA members recognize that companies must earn consumers' trust and act responsibly with their personal data.

Our comments are aimed at ensuring the draft subordinate regulations can effectively achieve the objectives of the PDPA and MDES, in a manner in line with emerging policy developments and internationally recognized approaches to privacy and personal data protection.

Recommendations

DPIAs for High-risk Processing

BSA recognizes that DPIAs are an important component of a company's data protection program and can support enhancing responsible data stewardship based on the principles of transparency and accountability. As such, DPIAs may be one of many tools that companies can choose to utilize to demonstrate accountability and their ability to comply with Section 37(1) of the PDPA. While we support such uses of DPIAs, it is important to clarify that even though the implementation of DPIAs is strongly encouraged, it should not be a mandatory requirement, particularly because the PDPA does not expressly provide for DPIAs.

Paragraphs 2.2 and 2.5 of Section 2.2 outline types of processing activities and data that may be considered high-risk and would be subject to a DPIA. While we appreciate the guidance on what would constitute high-risk processing activities and broadly agree that processing activities "affecting the freedoms" of data subjects would generally constitute a "high-risk" processing activity, examples presented in Paragraphs 2.2 and 2.5 should be provided as illustrative rather than exhaustive. In particular, numerous items on the list in Paragraph 2.5 may not necessarily lead to high risks to data subjects. For example, the processing of personal data (e.g., email addresses) using artificial intelligence for anti-fraud and anti-spam purposes should not lead to a high risk for data subjects – indeed, these uses may reduce the privacy and security risks for individuals using a service. Similarly, it is unclear why the collection of personal data from sources other than directly from the data subject without privacy notice should always be considered high-risk, especially when Sections 24-26 of the PDPA recognize a number of circumstances in which processing of data is appropriate without notification to an individual.

Instead of a prescriptive and exhaustive list like the one in Paragraph 2.5, **we recommend adopting a principles-based approach towards what would constitute "high-risk processing activities" and to state clearly that *"data controllers should be aware that where a processing activity is likely to affect the freedoms or rights of a data subject, regardless of the technology being used to process the data, conducting a DPIA prior to processing the data is highly recommended*.**" Adopting a principles-based approach would

ensure the guidance remains flexible and technology-neutral which would allow for the PDPA to remain relevant as new technologies are developed and applied.

Further, given that one "high-risk data processing activity" set out in Paragraph 2.5 is "processing sensitive personal data as reasons to deny access to services", we recommend clarification on the definition of "sensitive personal data", a term that is currently undefined in the PDPA.

Because DPIAs are important internal tools for assessing risks, they help companies to identify important decisions about data protection and operationalize privacy-protective design and implementation choices. Those benefits may be reduced when companies are required to publish DPIAs, which can convert the internal assessment process into public-facing. We are therefore concerned by the statement in Paragraph 2.3 that data controllers are to publish the result of DPIAs and notify the Office of the Personal Data Protection Committee (**Office**) of its publication. This requirement may reduce the incentive for companies to conduct and rely on DPIAs, as opposed to other tools for monitoring risks and ensuring accountability under the PDPA. Instead, **we recommend that data controllers who have chosen to conduct DPIAs be allowed to voluntarily publish the results of their DPIAs, but that publication not be mandatory**. In addition, these data controllers should also keep a record of their DPIAs and provide them to the Office upon request as per Section 39(8) which requires data controllers to maintain records explaining their security measures.

Obligations on Data Controllers Regarding Automated Processing

The draft subordinate regulations also address obligations around automated processing. Specifically, Paragraph 2.4 of Section 2.2 requires a data controller to implement processes enabling human intervention or human processing in the event a data subject exercises the right not to be subject to "*a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her*."

We recognize the importance of putting in place guardrails that can safeguard consumers' interests given the widespread use of automated decision-making processes in digital services across many industry sectors. However, the draft subordinate regulations go beyond the PDPA, which currently does not provide explicit data subject rights with respect to automated processing. Rather than issuing subordinate regulations on automated processing, we would recommend that the **Office issue guidelines to encourage data controllers that use automated processing to inform data subjects about the use of such means and how the system operates**.

Certifications

BSA is supportive of the voluntary nature of the proposed certification scheme set out in the draft subordinate regulations. Such certification schemes can provide companies with an additional mechanism to demonstrate their compliance with the PDPA. However, in designing and implementing any domestic certification scheme, we encourage the Office to ensure the domestic certification scheme be interoperable with other regional and global schemes, such as ISO/IEC 27001 and 27001, and the APEC Cross Border Privacy Rules (CBPR). Interoperable certification schemes will help promote industry participation in the domestic certification scheme, allow certified organizations to build trust with their customers and ensure meaningful

protections for consumers, and facilitate international exchanges of data with other countries relying on similar certifications.

In addition to developing a domestic certification scheme, we urge the Office to recognize other regional and global certification schemes that are consistent with its domestic certification scheme as data transfer mechanisms in the subordinate regulations addressing cross-border data transfers. These mechanisms are also recognized in the in the GDPR,[2] Singapore's Personal Data Protection Act,[3] and Japan's Act on the Protection of Personal Information.[4] As we had highlighted in our March 2021 submission under the section pertaining to cross border data transfers, recognizing international Trustmarks, and regional certifications will align the PDPA with global best practices and help provide businesses with interoperability and the flexibility to determine which mechanism(s) will be better suited for each situation.

International Cooperation

BSA welcomes the Office's efforts to participate actively in international and regional fora related to data protection and privacy, with a view to improve regulatory coherence. While the individual contexts and perspectives around privacy and personal data protection may appropriately vary from economy to economy, based on cultural expectations, legal traditions, and other factors, it is important that countries are aware of, and strive to ensure interoperability with, emerging international norms and practices around core aspects of personal data protection. The emergence of fragmented policies on core issues of data protection raises the cost of business, especially for under-resourced small- and medium-sized enterprises (SMEs) and can often undermine personal data protection and consumer privacy.

We note that MDES is currently participating in the APEC Data Privacy Subgroup and the ASEAN Working Group on Digital Data Governance. Thailand will also be taking over as Chair of the ASEAN Data Protection and Privacy Forum in late 2021 and the host of APEC in 2022, creating timely opportunities for Thailand to contribute to international cooperation on these data protection issues. In addition to APEC and ASEAN, other regional and international fora which the Office could consider taking part in could include the OECD Working Party on Security and Privacy in the Digital Economy, the Global Privacy Assembly and the Asia Pacific Privacy Authorities.

We note MDES' plans to pursue an adequacy decision with the EU and, also support organizations' participation in regional cross-border data transfer mechanisms such as APEC CBPR. BSA is supportive of efforts to develop different data transfer mechanisms and urges the subordinate regulations to clarify and recognize that there are multiple independent and equally compliant legal bases for transferring personal data across borders, and that organizations are free to determine which basis they will rely upon to transfer data.

Conclusion

BSA is grateful for the opportunity to provide these comments and recommendations on the draft subordinate regulations of the PDPA. We support the Government of Thailand's efforts in

[2] European Union General Data Protection Regulation https://gdpr.eu/tag/gdpr/
[3] Personal Data Protection Act 2012, https://sso.agc.gov.sg/Act/PDPA2012
[4] Act on the Protection of Personal Information (English), https://www.ppc.go.jp/files/pdf/Act_on_the_Protection_of_Personal_Information.pdf

implementing the PDPA successfully and look forward to continuing working with the Ministry of Digital Economy and Society and the Office of the Personal Data Protection Committee on privacy and personal data protection policies. Please do not hesitate to contact the undersigned at eunicel@bsa.org if you have any questions or comments regarding our suggestions.

Yours faithfully,

Eunice Lim

Senior Manager, Policy – APAC
BSA | The Software Alliance