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

Comments from BSA | The Software Alliance

June 30, 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 second 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 second group of draft subordinate regulations add to the points made in our earlier submission dated March 16, 2021. We 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:

- Recognizing Distinct Roles of Data Controllers and Data Processors
- Data Subject Rights
- Derogations under the Royal Decree
- Territorial Scope

[1] BSA's members include: Adobe, Akamai, Amazon Web Services, Apple, Autodesk, AVEVA, Bentley Systems, Box, Cadence, Cisco, CNC/Mastercam, DataStax, DocuSign, IBM, Informatica, Intel, MathWorks, Microsoft, Okta, Oracle, PTC, Salesforce, ServiceNow, Siemens PLM Software, Sitecore, Slack, Splunk, Symantec, Synopsys, Trend Micro, Trimble Solutions Corporation, Twilio, Workday and Zoom.

- Consistency in Data Protection Obligations

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.

Companies entrust some of their most sensitive information to BSA members, and our members work hard to keep that trust. Companies also rely on BSA members to provide technologies that can advance social and economic goals, from helping businesses transition to remote work and ensuring the continuity of their operations[2] to empowering researchers and first responders with new tools to address the spread of infectious diseases such as COVID-19.[3] We hope our comments will assist MDES in drafting subordinate regulations to implement the PDPA in ways that can enhance consumer privacy and personal data protection, ensure international interoperability with emerging global norms, and enable and facilitate innovative uses of data to drive economic growth and job creation in Thailand.

In the sections below, we provide recommendations in response to proposals in the consultation document for the draft subordinate regulations, to ensure they most effectively achieve the objectives of the PDPA and MDES and are in line with emerging policy developments and internationally recognized approaches to privacy and personal data protection.

Recommendations

Recognizing Distinct Roles of Data Controllers and Data Processors

As we emphasized in our March comments, a comprehensive data protection framework must create effective and enforceable obligations for all companies that handle consumer data. These obligations will only be effective in protecting consumer privacy and instilling trust if they reflect how a company interacts with consumer data. The distinction between data controllers and data processors is paramount because both data controllers and data processors have important, but different, roles in protecting personal information.

BSA welcomes the distinction between data controllers and data processors in the PDPA and in the consultation document, as this ensures that data protection obligations can be appropriately applied to entities that have very different roles in handling consumers' data. As MDES develops subordinate regulations to ensure that data processors remain accountable for handling personal data securely, it is important that the regulations take into account the unique role data processors play vis-à-vis data controllers and do not assign them obligations that do not fit their role as a provider of services to other businesses under contractual obligations.

[2] BSA's Response & Recovery Agenda at: https://www.bsa.org/files/policy-filings/05272020bsaresponserecoveryagendaa4.pdf

[3] COVID-19 Response: Software Solutions Enable Vaccine Research, Security, Safe Distribution at: https://software.org/news/covid-19-response-software-vaccine-research-security-distribution/

It is also important for MDES to allow data controllers and data processors the flexibility to negotiate agreements that befit the type(s) of data entrusted to the data processor for processing, and the protections that need to be accorded to such data, rather than prescribing prescriptive rules for what the agreement between the data controller and data processor should contain. To this end, we recommend ensuring the requirements in the subordinate regulations are principle-based and not overly prescriptive.

We wish to also highlight our concerns with the following proposals, which seek to implement Section 40 of the PDPA:

- Section 2.5, Paragraph 2.1: The consultation document indicates that the proposed subordinate regulations will contain an obligation for a set of "minimum requirements" to be included the agreement between a data controller and a data processor. We again question the need for the proposed subordinate regulations to be so prescriptive and would further highlight that several of these minimum requirements raise concerns – and may inadvertently undermine privacy and security of personal data intended to be protected by the PDPA, particularly with respect to subprocessor obligations. For example, while data processors should provide assistance to data controllers in order for them to meet their obligations, many data processors are contractually prohibited to access certain data and it may be more appropriate for data processors to provide assistance that is "*reasonably practicable*". A general authorization instead of a written permission should also suffice to allow data processors to engage sub-processors as long as the controllers' instructions and other commitments as set forth in the data processing agreement are maintained. In addition, the list of minimum requirements refers to requirements to demonstrate that a processor can perform its obligations, but should recognize that this demonstration may be done in a variety of manners, and not only by reference to agreements or the provision of specific systems or technical measures.

- Section 2.5, Paragraph 2.3: This section is intended to clarify the circumstances in which a data processor would be considered a data controller for a processing activity. We support the recognition that data processors are to process data as instructed by data controllers – and that an entity that is not acting on behalf of a controller can no longer be considered a processor. For example, data protection laws such as the European Union's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA), recognize that if a data processor begins determining the purposes and means of processing personal data, it becomes the controller for purposes of that processing. We support this result and urge you to ensure that the proposed subordinate regulations will be consistent with this approach as follows:

  2.3 ~~The data processor who fails to comply with a data processing agreement shall become the data controller for the non-compliant processing of personal **data**~~ **If a data processor infringes the data processing agreement by determining the purposes and means of processing, the data processor shall be considered a data controller in respect of that processing**.

- Section 2.5, Paragraph 2.4: This proposed requirement states that data processing agreements must be terminated within one year from the date of entry into force of the subordinate regulation. This arbitrary deadline would increase costs and administrative burdens on both data controllers and processors – requiring them to renegotiate all existing contracts – without providing any clear benefits to the privacy of personal data, particularly when those existing contracts may already comply with requirements in the PDPA. We recommend revising this requirement to recognize that existing data processing agreements shall remain valid between data controllers and processors unless inconsistent with PDPA.

> ***2.4*** The data processing agreements provided by the data controller before this Notification shall remain in force and be deemed to have complied with the provisions of this Chapter until the end of the agreement. Nonetheless, ~~such~~ **agreements that are inconsistent with the PDPA** must have the date of termination within 1 year from the date of when this Notification becomes effective.

- Section 2.5, Paragraph 2.8: This provision would require data processors to provide the data controller with a list of information, without delay, once it is aware of a personal data breach. As data processors in many cases are contractually prohibited from accessing the content of data controllers and may not have visibility on the data being processed by them, which could limit the types of information they may provide under Paragraph 2.8. We recommend amending Paragraph 2.8 as follows:

> ***2.8*** In the event of a personal data breach under the responsibility of the processor, the processor is obliged to provide the controller with the following details**, to the extent it is feasible** and without **undue** delay, ~~and~~ from the time the processor becomes aware of the incident so that the controller can inform the Office and the data subject as required by the law.[34]

- Section 2.5, Paragraphs 2.10 and 2.11: This provision would impose obligations on the use of sub-processors – but as currently written, these obligations could inadvertently undermine the privacy and security of personal data instead of strengthening those protections. The current text would require a processor to obtain the controller's approval for changes in sub-processing and to provide the controller with an opportunity to object to sub-processors. However, in many cases a processor may rely on dozens (or more) subcontractors to provide a single service – and will need to replace a sub-processor quickly if one is unable to provide services, including because of operational failures or potential security concerns.

  Requiring controllers be given an opportunity to object to new sub-processors can limit the ability of processors to provide secure and stable services in these circumstances, without a clear benefit to privacy. Instead, we suggest replacing Paragraphs 2.10 and 2.11 with this provision to ensure a controller is notified of a new sub-processor and to require the processor's privacy and security obligations are passed on to the sub-processor via contract, to ensure the personal data remains protected.

2.10 In case of a change, addition or replacement of the subprocessor, the processor must ~~first obtain permission from the data controller, giving an opportunity to the data controller to object to such changes.~~ notify **the data controller and engage the subprocessor pursuant** to a written contract that requires the subprocessor to meet the obligations of the processor with respect to personal data processed on behalf of the controller.

Data Subject Rights

BSA supports giving individuals more control over their data. The inclusion of additional consumer rights that align with international best practices, including the Right to Data Portability (Section 31 of the PDPA), the Right to Object (Section 32 of the PDPA), and the Right to Erasure (Section 33 of the PDPA), as well as the Right to Restrict Processing (Section 34 of the PDPA), serve to achieve this outcome. While these data subject rights lay the foundation for a robust data protection framework in Thailand, it is imperative that the proposed subordinate regulations retain flexibility and are not over-prescriptive. Otherwise, these obligations can cause practical operational challenges, increase the cost of compliance, and lessen the incentive for businesses in Thailand to use data and technology in innovative ways.

In particular, we wish to highlight our comments with regard to the following proposals that seek to implement Sections 31-36 of the PDPA:

- <u>Section 2.4, Paragraph 2.7</u>: Under the Right to Portability (Section 31 of the PDPA), we welcome the recognition that data controllers may be unable to comply with a data portability request due to technical limitations. The specific mechanisms for transferring data from legacy systems to cloud-based service providers and from one service provider to another will depend heavily on the specifics of each organization and their existing data structures. BSA members offering software and cloud computing services have developed a variety of solutions that can be tailored to their customers' needs for secure transfer of data from one system to another. In some cases, this may be straightforward. In others, it may be more difficult, such as where the data is tightly associated with particular applications and is not easily convertible to alternative systems. BSA further urges that the proposed subordinate regulations make clear that **<u>data controllers are allowed to determine the means and format that is practical and technically feasible</u>**. This will afford industry the flexibility required to comply with the data portability requirement.

- <u>Section 2.4, Paragraphs 2.14 and 2.16</u>: BSA notes the new requirement for data controllers to delete personal data *without the need for a data subject's request*, when it is "no longer necessary to process the personal data, or when the personal data have been unlawfully collected, used or disclosed." While we support the need for accountable privacy and data protection measures, it is important to clarify that it is the controller that determines when the processing of personal data is necessary, based on the products and services it provides. We are also particularly concerned by the proposal in Paragraph 2.16 for data controllers to arrange audits that would demonstrate the necessity of processing personal data. Given that an audit is only one example of demonstrating the necessity of processing personal data, and does not preclude other methods, such as a simple attestation by the data controller that processing remains necessary, we would encourage MDES to recognize that a controller may make a determination that processing is necessary through means other than audits.

Derogations under the Royal Decree

BSA welcomes the enactment of a Royal Decree which would provide exemptions from the PDPA for certain types of data and under specific scenarios. Given that data increasingly powers the modern, digital economy, and drives innovation in areas such as Artificial Intelligence and the Internet of Things, a flexible data protection regime that enables data innovation is necessary to guard against privacy risks whilst growing Thailand's digital economy.

BSA recommends the following exemptions in the Royal Decree:

- Anonymized, pseudonymized or de-identified data. We note that Section 33 of the PDPA and the consultation document currently provide for the use of anonymization and de-identification techniques as means to mitigate privacy risks. We encourage MDES to further incentivize the innovative use of anonymized, pseudonymized, or de-identified data by clearly excluding such data from the PDPA. Such de-identified data that has contractual controls, privacy and security controls, or both, and reasonably reduces the risk of re-identification, should not be covered data under the PDPA.

- Public health exemption. Section 24(2) of the PDPA currently allows the collection of personal data without consent for the purpose of "preventing or suppressing a danger to a Person's life, body or health;". While the public health exception is a well-established one, we encourage you to ensure the Royal Decree notes that Section 24(2) may be appropriately relied upon in public health emergencies where there are good grounds to collect of personal data of an individual to protect someone else's life or health, as opposed to the life or health of the individual.

- Other exceptions to data subjects' requests. A robust data protection framework should not only provide individuals with important rights to their personal data, it should also recognize certain exceptions to the exercise of these rights, so that individual rights requests do not undermine the privacy or security of an individual or a service, and do not prevent an individual from receiving a requested service. In this regard, we support the exemptions under Paragraph 2.4 and 2.5. However, additional exemptions should be incorporated. Specifically, we urge the proposed subordinate regulations to incorporate exemptions to allow data controllers to reject requests by data subjects in instances where: (1) the request is vexatious, frivolous, or duplicative of an earlier request; (2) fulfilling the request would create a security risk; (3) fulfilling the request would prevent the company from providing a service or product specifically requested by the individual; or (4) fulfilling the requests would create risks to the privacy of the individual or natural persons.

Territorial Scope

Section 5 of the PDPA extends the territorial scope of the PDPA to activities by data controllers and processors that are "outside the Kingdom", for activities related to "the offer of goods and services" and the "monitoring of… behavior" to any personal data owner who is in the Kingdom. For the extraterritoriality provision to be enforceable, BSA recommends that the scope of Section 5 of the PPDA should be limited to entities or activities that have a sufficiently close connection to Thailand where: (1) the personal data that is the object of the processing is purposefully collected from data subjects in Thailand at the time of collection, and (2) such collection is performed by an entity through a stable arrangement giving rise to a real and effective level of activity, or subject to Thai law by virtue of international public law. Under this standard, the mere accessibility of a website in Thailand or the use of the Thai language on a website would be insufficient, on their own, to establish the applicability of the Thai data protection law.

Consistency in Data Protection Obligations

Section 3 of the PDPA states that in the case there is any specific law governing data protection in any manner, the provisions of such law will apply. Additionally, the PDPA's provisions with respect to the collection, use, and disclosure of personal data and the provisions with respect to the rights of data subjects including relevant penalties will continue to apply. This could create conflicts and inconsistencies that may be difficult for organizations handling personal data to reconcile.

We note that the consultation document contains proposals for the Personal Data Protection Committee (PDPC) to cooperate and coordinate with the PDPC Office and other regulatory agencies to maintain consistency and compliance with the PDPA. We support such cooperation among various government agencies on matters of personal data protection. However, the process contemplated appears cumbersome and ad hoc, and could lead to a lack of up-front clarity for organizations on what obligations they need to meet when handling personal data. To allow organizations to better understand their data protection obligations in Thailand, we encourage MDES, prior to the implementation of the PDPA, to conduct an inter-agency exercise to identify and resolve inconsistencies and conflicts between the various laws that apply to data protection in Thailand. We also recommend including an explicit clarification in the proposed subordinate regulations that in the event of any unresolved inconsistency or conflict between a provision of the PDPA and a provision in another law pertaining to the collection, use and disclosure of personal data and the rights of data subjects, the PDPA provision will take precedence.

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 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

Eunice Lim
Senior Manager, Policy – APAC
BSA | The Software Alliance