



March 16, 2021

Ms. Acharin Pattanaphanchai
Permanent Secretary
Ministry of Digital Economy and Society, Thailand
Chaeng Watthana Government Complex, Building B
Chaeng Watthana Road, Lak Si
Bangkok

BSA COMMENTS ON THE DRAFT SUBORDINATE REGULATIONS UNDER THE PERSONAL DATA PROTECTION ACT 2019

On behalf of BSA | The Software Alliance (BSA) and our members,¹ we write to provide our comments to the Ministry of Digital Economy and Society (**MDES**) regarding the 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 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
- Security of Personal Data Processing
- Expanding Legal Bases for Processing Personal Data
- Facilitating Cross Border Data Transfers
- Thresholds for Data Breach Notifications
- Flexibility in Appointing Data Protection Officers
- Accountability-based Approach Towards Notification

¹ BSA's members include: Adobe, Amazon Web Services, Atlassian, Autodesk, AVEVA, Bentley Systems, Box, Cadence, Cisco, CNC/Mastercam, DocuSign, IBM, Informatica, Intel, MathWorks, Microsoft, Okta, Oracle, PTC, Salesforce, ServiceNow, Siemens Industry Software Inc., Slack, Splunk, Synopsys, Trend Micro, Trimble Solutions Corporation, Twilio, and Workday.

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 operations² 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 information 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 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

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 companies that decide when and how to collect and use data about individuals (**data controllers**) and companies that only process data on behalf of other companies (**data processors**) is important because both data controllers and data processors have important, but distinct, roles in protecting personal information.

BSA welcomes the distinction between personal data controllers and personal data processors in the PDPA and the draft subordinate regulations, especially where it relates to consumer-facing obligations such as the requirement for data controllers to establish measures that ensure data subjects can access, amend, or request a copy of their personal data and data breach notifications. We urge MDES to ensure future regulations continue to recognize the very different roles these entities play in handling consumers' data.

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/>

In particular, we wish to highlight our concerns with regard to the proposals in Section 2.4 of the draft subordinate regulations: Criteria and Policies on the Protection of Personal Data that is Sent or Transferred Overseas. These proposals conflate the roles of the data controller and data processor by:

- Introducing joint liability on both data controllers and processors: This will be problematic as it brings about significant and unwarranted risk. As a general principle, parties should only be liable for what they are responsible for per their contractual arrangements or regulatory responsibilities. We suggest clarifying that processors are only liable where they have not complied with their statutory obligations specifically directed to processors or where they have acted outside of or contrary to lawful instructions of the controller.
- Allocating disproportionate responsibilities between a data controller and data processor: For example, under the subordinate regulations, data controllers appear to be required to include contractual provisions with data processors allowing the data subject to exercise his or her rights against the data exporter (controller), data importer (processor), and any sub-processor. This conflates the roles of controllers and processors, as the data controller is the party that both determines how and why to collect a consumer's data and is responsible for the transfer of personal data overseas. The controller should accordingly be the main party held accountable to the data subject. A data processor is unlikely to be able to identify a data subject or verify her identity — and requiring the processor to disclose data to an unidentified person can create significant privacy and security risks. Rather, the controller should be obligated to respond to all data subject rights requests and the processor should remain accountable to the data controller as per their contractual agreement. This is equally the case for sub-processors. We accordingly urge MDES to revise the draft subordinate regulations so that controllers remain responsible for honoring data subject rights requests and processors and sub-processors are accountable to those controllers via contract.
- Imposing obligations on data processors which do not fit their role as providers of services to other businesses: For example, the draft subordinate regulations state that data processors are required to provide a summary of the details on data protective measures and sub-processing service agreements to data subjects if the data subject fails to obtain those documents from the data exporter (controller); data processors are also required to “ask the data exporter (controller) about processing of the sent or transferred personal data”. As noted above, data processors do not have a direct relationship with data subjects and may be unable to determine when such requests should be honored. It is also unclear what information regarding transferred personal data processors should be requesting from data exporters (controllers). Moreover, in many cases a data processor may be contractually prohibited from accessing data on its services except in certain circumstances, a prohibition often explicitly designed to increase privacy protections afforded to that data. The requirement to allow data subjects to request specific information directly from a data processor is thus not suited for data processors and may inadvertently undermine privacy protections afforded to data subjects.

Security of Personal Data Processing

Personal data controllers and data processors should be held accountable for the safe and secure handling of personal data. This is already provided for under Sections 37(1) and 40(2) of the PDPA where both personal data controllers and processors are required to put in place “appropriate security measures” to prevent the unlawful loss, access, use, modification, editing, or disclosure of personal data.

Under the draft subordinate regulations, the Personal Data Protection Committee (**PDPC**) and the Office of the PDPC (**Office**) will now be able to monitor and inspect both personal data controllers and processors to ensure that adequate personal data processing security measures have been established by these entities. In addition, the PDPC may also require both personal data controllers and personal data processors to submit assessment reports for their review, in accordance with the details and methods set by the PDPC. This appears to depart from Sections 39 and 40 of the PDPA, where only controllers are required to maintain specific records to be checked upon by the Office. BSA accordingly urges the review mechanism established by the draft subordinate regulations to adopt the same scope as the PDPA and not be applied to data processors.

Additionally, it is currently unclear whether the security measures detailed in the draft subordinate regulations are voluntary or mandatory. We urge MDES to avoid mandating prescriptive security approaches and instead recommend providing organizations with the flexibility to implement security measures that meet the intended data protection outcomes against the background of an ever-changing threat landscape. For example, MDES can consider a voluntary review mechanism where an organization can choose to opt-in for a review by the PDPC as a means to obtain the assurance that it has implemented a data management framework appropriately. The PDPC and/or the Office could provide feedback and suggestions for improvement in the organization’s processes thereby helping organizations that have volunteered to build capacity and improve their data protection procedures.

Expanding Legal Bases for Processing Personal Data

Section 19 of the PDPA makes clear that the collection, use, and disclosure of personal data will be primarily governed by consent, while Section 24 of the PDPA contains a list of “exceptions” to the consent requirement which personal data controllers can rely on to collect personal data. The draft subordinate regulations further aim to provide clarity on how organizations in different sectors can obtain explicit consent from data subjects through sectoral-specific consent forms.

Due to evolving advancements in technology and new and innovative ways in which personal data can be used to enhance societal and economic benefits, many data controllers today develop mechanisms for gaining and assessing consent based on a variety of factors. Prescribed forms of consent could quickly be rendered obsolete and could instead hamper such developments and the accrual of benefits to consumers. Other jurisdictions, such as Singapore, are acknowledging that the reliance on obtaining explicit consent is not practical in every context. To that end, in addition to enumerated exceptions to requiring consent, such as processing to allow the performance of a contract, or to protect the life or health of the individual, etc., it is also important to provide companies with additional legal bases for processing data, such as to achieve legitimate interests of the

enterprise or to promote business improvement.⁴ We urge MDES to consider allowing organizations to rely on deemed, indirect, or implied consent based on differing contexts, and to explicitly introduce such additional legal grounds for collections and processing as seen in other well regarded personal data protection systems. While organizations should provide the appropriate mechanisms for individual control over how personal data is being processed, it should not require consent at each juncture or for each activity that uses personal data.

Facilitating Cross Border Data Transfers

The ability to transfer data, including personal data, across international borders is the lifeblood of the modern digital economy. For this reason, it is critical that the subordinate regulations should enable and allow companies to responsibly transfer data internationally. While differences exist among data protection regimes, BSA encourages the draft subordinate regulations to create mechanisms to bridge those gaps in ways that both protect privacy and facilitate global data transfers.

BSA appreciates the proposed inclusion of several data transfer mechanisms such as adequacy recognition, policies that facilitate transfers within a corporate group (akin to binding corporate rules), and the use of minimum safeguards identified in the draft subordinate regulations. These mechanisms are incorporated in data protection frameworks such as the European Union's General Data Protection Regulation (**GDPR**) and Japan's Act on the Protection of Personal Information (**APPI**) to promote cross-border data flows. BSA further recommends recognizing other data transfer mechanisms, such as international trustmarks and regional certifications, as additional acceptable mechanisms to support international data transfers. These mechanisms are recognized in the Asia-Pacific region, including through the APEC Cross Border Privacy Rules, Singapore's Personal Data Protection Act, and the APPI. BSA urges the subordinate regulations to clarify that there are multiple independent and equally compliant legal bases for transferring personal data across borders, and that entities are free to determine which basis they will rely upon to transfer data.

We also offer specific recommendations to facilitate the development of transfer mechanisms within corporate groups, and the development of minimum safeguards that may support data transfers:

- *Transfers within a corporate group:* The draft subordinate regulations make clear that sending or transferring personal data within a group of affiliated companies to a destination country or international organization that is not yet regarded as having adequate personal data protection standards is permitted when the affiliated companies have a privacy policy that has been inspected and certified by the Office. The draft subordinate regulations also include a list of "minimum requirements" that the Office will use when "inspecting and certifying" the privacy policy of company groups.

The requirement for the Office to assess and approve a group of companies' privacy policy appears similar to how the European Union handles the approval and use of binding corporate rules (**BCRs**) under the GDPR. Although such binding group policies can be an effective way to allow organizations to transfer data overseas while ensuring that an adequate level of protection is achieved, it may result in a lengthy and onerous process that can require significant resources from both the Office and the regulated entities. We recommend that MDES establish processes that incorporate more flexibility, such as by making the inspection

⁴ See Article 6(1)(f) of the European Union's General Data Protection Regulation and Sections 15A and Section 17 of the Singapore's Personal Data Protection Act.

and certification of such group policies voluntary rather than mandatory and allowing companies to submit independent third-party audits and supporting documentation in lieu of additional or duplicative audits conducted by the Office.

- Transfers pursuant to minimum standards recognized by the PDPC: The draft subordinate regulations recognize that companies may also transfer personal data pursuant to minimum safeguards recognized by the PDPC when they seek to transfer personal data to a destination country that has not received an adequacy determination and no policies are in place to support transfers between affiliated companies. This concept appears similar to standard contractual clauses, and we encourage it to be implemented in a manner that ensures the standards recognized by the PDPC align with globally recognized contractual provisions designed to provide such safeguards.

At the outset, we support the recognition in the draft subordinate regulations that these minimum standards should be applied in distinct ways to personal data controllers and personal data processors. We accordingly agree with the draft subordinate regulations' approach of identifying minimum standards for transferring data to a data controller separately from the minimum standards for transferring data to a data processor. We urge MDES to clearly recognize that businesses may rely on contracts that contain these identified minimum standards to facilitate transfers — without requiring pre-approval by the Office. In contrast, if pre-approval of each contract were required, it would likely inundate the Office with requests to approve contracts that incorporate the terms it has already established — resulting in a duplicative and burdensome process.

- Certifications and trustmarks: In addition, we recommend the PDPC recognize certifications or trustmarks that are consistent with the minimum standards, which would establish a clear and easy-to-use mechanism for companies to facilitate transfers.

The draft subordinate regulations contain a specific reference to cloud system services which implies that the use of cloud computing services is considered as an international data transfer. Not all uses of cloud computing services involve moving data outside a given country and there are many circumstances in which data is transferred overseas and the use of cloud services is only one such method. As such, it is neither necessary nor helpful to specifically reference any particular technology platforms or services, such as cloud computing. Therefore, we respectfully urge MDES to remove the specific reference to “cloud system services” in the subordinate regulations and instead ensure the regulations appropriately describe the situations in which data may be transferred under the PDPA.

Thresholds for Data Breach Notification

BSA supports the creation of a personal data breach notification system that is consistent with global best practices and that includes requirements that are reasonable and appropriately crafted. This will provide incentives to personal data controllers to be transparent about data breaches that are likely to harm the interests of their customers and enable data subjects to take actions to protect themselves from serious harm should the need arise. To achieve these goals, it is critically important to set the correct threshold for reporting breaches based on risk of harm to individuals, to allow sufficient time for data controllers to report, and to provide appropriate exceptions to the notification requirement.

To ensure that neither consumers nor the Office are inundated with notices about situations that pose little or no risks to consumers, the notification obligations in the draft subordinate regulations should

implement the risk-based approach reflected in the PDPA. In particular, the standard for notification should be when an incident involves the unauthorized access to or loss of unencrypted or unredacted personal data that creates a material risk of harm to the data subject. This will help ensure that consumers and regulators alike focus their attention on meaningful incidents.

Currently, under Section 37(4) of the PDPA, personal data controllers are required to notify both the Office and data subjects if a breach “is likely to result in a high risk” to the rights and freedoms of the data subject. We recommend the draft subordinate regulations provide further guidance to organizations on what is likely to constitute a “high risk” and what does not meet this threshold. For instance, guidance can specify that “high risk” incidents are understood to be those creating a “material risk of actual harm to the data subject, such as identity theft or financial fraud.” In addition, the guidance can state that an incident is not “high risk” when the breached data is unusable, unreadable, or indecipherable to an unauthorized third party through practices or methods (e.g., encryption).

Furthermore, to ensure users receive meaningful notification in the event of a breach, it is critical that personal data controllers are afforded adequate time to perform a thorough risk assessment to determine the scope of the security risk and prevent further disclosures that could negatively impact data subjects. Section 37(4) of the PDPA recognizes this by requiring personal data controllers to notify the Office of a personal data breach that meets the notification threshold “without delay” and, “where feasible, within 72 hours” after having become aware of the breach. This flexibility, recognizing that in some cases 72 hours may not be a feasible timeframe for submitting the initial report, is helpful. We also urge the subordinate regulations clarify that the timeline for notification begins when the notifying company establishes with a reasonable degree of certainty that a material data breach that meets the notification threshold has occurred. While the PDPA is clear that the notification is triggered after a controller “becomes aware of” the breach, the subordinate regulations should clarify that the triggering event is becoming aware of an incident that meets the threshold covered by the notification requirement — rather than requiring notice of a potential breach when companies are unsure if the event meets the notification threshold. This approach will help avoid overwhelming the Office with immaterial notifications and will prevent the diversion of company resources from activities that foster data security to the preparation of notifications that are unlikely to meet the notification threshold. It will also reduce “notification fatigue” where data subjects begin to disregard such notifications is the majority pose no real risk to their rights or interests.

Flexibility in Appointing Data Protection Officers

Data protection officers (**DPOs**) are now an established part of global data protection programs and can play a valuable role in helping businesses maintain compliance with their data protection obligations. However, companies vary in size, complexity, and volume of personal data processing. In light of these differences, BSA recommends that organizations should be permitted to appoint their DPOs based on their suitability and their organizations’ structure. In particular, we recommend avoiding overly prescriptive thresholds for companies to appoint DPOs, minimum qualification requirements, or specific certifications mandated by the Office.

Accountability-Based Approach Towards Notification

BSA recognizes the need for data controllers to provide adequate notice to data subjects regarding purpose for which they are collecting personal data and that controllers should use that data in a manner that is consistent with that explanation, the context of the transaction, or the reasonable expectations

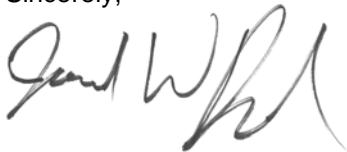
of the data subject, or in a manner that is otherwise compatible with the original purpose for which the data was collected. We encourage MDES to allow organizations to determine the best way of providing such notice so that the data subject is provided with the required information, such as by making their privacy policies available on their organizations' websites, and to avoid specifying overly prescriptive methods for such notifications.

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 us if you have any questions or comments regarding our suggestions.

Thank you for your time and consideration.

Sincerely,

A handwritten signature in black ink, appearing to read "Jared W. Ragland". The signature is fluid and cursive, with the first name "Jared" and last name "Ragland" clearly distinguishable.

Jared William Ragland, Ph.D.
Senior Director, Policy – APAC

BSA | THE SOFTWARE ALLIANCE