



January 30, 2019

Mrs. Saowanee Suvarnacheep
Chair of the Ad-Hoc Committee on the Personal Data Protection Bill B.E. ...
The National Assembly of Thailand
Authong Nai Road, Dusit,
Bangkok 10300
Thailand

BSA RESPONSE TO THE PERSONAL DATA PROTECTION BILL AND THE NATIONAL CYBERSECURITY BILL

Dear Chair Saowanee,

We refer to our previous correspondence dated January 11, 2019 titled "*Request for a Meeting to Present BSA Recommendations on the Personal Data Protection Bill and the National Cybersecurity Bill*". On behalf of BSA | The Software Alliance (**BSA**)¹ and our members, we write to express our sincere gratitude to the National Legislative Assembly (**NLA**) for the opportunity to submit our comments and recommendations on the proposed Personal Data Protection Bill ("**PDP Bill**") and National Cybersecurity Bill ("**Cybersecurity Bill**").

BSA commends the Royal Thai Government (**RTG**), the NLA, the Ministry of Digital Economy and Society (**MDES**), and the Electronic Transactions Development Agency (**ETDA**) for undertaking this important effort to ensure that Thailand has robust legal frameworks for protection of personal information and personal privacy, and effective management and deterrence of cybersecurity threats. Effective cybersecurity and personal data protection frameworks, which are sufficiently flexible, will strengthen the trust necessary to promote full participation in the digital economy and encourages innovative services and technologies which will directly contribute to the Thailand 4.0 goals and priorities.

We previously filed submissions with the MDES and Council of State describing our concerns and recommendations with the Cybersecurity Bill and have already enclosed copies of the submissions with our January 11, 2019 letter to the NLA. These submissions are also accessible online via the following links:

- [BSA Comments on National Cybersecurity Bill \(November 30, 2018\)](#);²

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, Akamai, Amazon Web Services, Apple, Autodesk, AVEVA, Bentley Systems, Box, Cadence, Cisco, CNC/Mastercam, DataStax, DocuSign, IBM, Informatca, Intel, MathWorks, Microsoft, Okta, Oracle, PTC, Salesforce, Siemens PLM Software, Slack, Splunk, Symantec, Synopsys, Trend Micro, Trimble Solutions Corporation, Twilio, and Workday.

² <https://www.bsa.org/~media/Files/Policy/Data/en11302018BSACommentsCybersecurityBill15November2018.pdf>

- BSA Comments on National Cybersecurity Bill (October 12, 2018);³
- Joint Industry Comments on the Cybersecurity Bill – Supplemental (May 21, 2018);⁴
- Joint Industry Comments on the Cybersecurity Bill (April 17, 2018);⁵ and
- BSA Comments on the Cyber Security Bill (May 6, 2015).⁶

While the comments described in the submissions listed above remain relevant for the current version of the Cybersecurity Bill, we would like to draw the NLA’s attention to the following key issues that remain a significant concern to BSA and our members:

1. **Framework for due-process and appeals can be further improved.** Any obligations on private organizations, and the investigatory powers of a government agency (or other body), must require a valid and binding court order or warrant. Private organizations must have the right to appeal or challenge the court order or warrant. The court order or warrant must only be applicable to companies that operate or control critical infrastructure in Thailand. Any obligation on private organizations, and any powers of a government agency (or other body), must be clear, subject to appeal, and proportionate to the intended aims of the legislation. The Cybersecurity Bill would therefore benefit from the inclusion of provisions that support the following:
 - a. Court orders should be served to the entities (whether public sector or private) managing critical information infrastructure (**CII**) rather than their service providers;
 - b. The right to appeal an authoritative instruction should be extended to all cyberattacks, regardless of level of impact;
 - c. An independent body should have oversight over the National Cyber Security Committee’s (**NCSC**’s) powers.

In addition, any broad, all-encompassing provisions (for example Section 66) that gives unfettered powers to a government agency, or other body, should be deleted. Any power, obligation, or right under the Cybersecurity Bill should be clear, subject to checks and balances, and be proportionate to the intended aims of the legislation.

2. **Certification, standards, or codes of conduct must leverage existing best practices and internationally recognized industry-led standards.** There are a range of guidelines, codes of conduct, codes of practice, standards, and other “guidance-like” documents referred to in the Cybersecurity Bill (for example new language in Section 53, collectively “Standards”). Standards and best practices are most effective when developed in collaboration with the private sector, adopted on a voluntary basis, and recognized globally. Thailand should align any practices and standards it issues with industry-backed approaches to risk management, including the ISO/IEC 27000 family of standards or the National Institute of Standards and Technology (**NIST**) Framework for Improving Critical Infrastructure Cybersecurity (NIST Cybersecurity Framework).⁷
3. **Categories of information which are exempted from disclosure,** such as privileged information or information which would violate other rights, such as personal information, or would be inconsistent with protecting intellectual property rights or trade secrets should be included in the law.
4. **Concept of “critical infrastructure” and “critical cyber-attack” should be consistent with international practice.** Instead of defining “Critical Information Infrastructure”, “Critical Information Infrastructure Agency”, and “Cyber-attack” in their current forms, NLA should ensure the definitions in the

³ https://www.bsa.org/~media/Files/Policy/Data/10122018EN_BSACommentsCybersecurityBillwith%20Annexes.pdf

⁴ https://www.bsa.org/~media/Files/Policy/Data/05212018enJointBSA_USABC_SupplementalCommentsThaiCybersecurityBill.pdf

⁵ https://www.bsa.org/~media/Files/Policy/Data/05212018enJointBSA_USABC_SupplementalCommentsThaiCybersecurityBill.pdf

⁶ https://www.bsa.org/~media/Files/Policy/Data/05062015SubmissionCybersecurityBill_EN_DeputyPrimer.pdf

⁷ <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf>

Cybersecurity Bill are consistent with international practice and consider adopting the following definitions or conceptions:

- a. **Critical Infrastructure:** “those assets, services, and systems, whether physical or virtual, which, if destroyed, degraded, or rendered unavailable for an extended period, would have a large-scale, debilitating impact on national security, public health, public safety, national economic security, or core local or national government functions.” Specific critical infrastructure should be identified by the NCSC based on an analysis of criticality, interdependency, and risk.
 - b. **“Agencies” for CII,** should be identified only as those which have effective control over the critical infrastructure or are responsible for the CII, and these would be the legal owners of the CII assets. The Cybersecurity Bill must also be clear that “computers” and “computer systems” located wholly outside of Thailand should not be designated as CIIs. For example, multinational organizations with offices in Thailand may be supported by infrastructure and IT systems located wholly outside of Thailand. Designation of such computers or systems as CII could lead to potential conflicts with other countries’ regulatory regimes.
 - c. **Significant Cybersecurity Incident:** defined as “a cybersecurity incident resulting in:
 - o The unauthorized or denial of access to or damage, deletion, alteration, or suppression of data that is essential to the operation of critical infrastructure; or
 - o The defeat of an operational control or technical control that is essential to the security or operation of critical infrastructure.”
5. **The transition period between the enactment of the law and its effective date should be at least two years.** The law should also apply only prospectively.
6. In addition to the points we previously raised, we also recommend that the Cybersecurity Bill should only apply to organizations and CII providers that are **operate or control critical infrastructure in Thailand.**

Separately, in relation to the PDP Bill, BSA previously filed submissions with the MDES and Council of State describing concerns and recommendations with previous versions of the PDP Bill which were also enclosed with our January 11, 2019 letter to the NLA. These submissions are also accessible online via the following links:

- BSA Comments on Draft Personal Data Protection Act (February 6, 2018);⁸
- Proposed Additional Amendments to the Personal Data Protection Bill – BSA Comments (August 4, 2017);⁹ and
- BSA Comments on Draft Personal Data Protection Act (March 23, 2015).¹⁰

The current version of the PDP Bill contains improvements over previous drafts, strengthening privacy protections for the Thai people. However, the PDP Bill also includes several provisions that continue to create unreasonable burdens and legal uncertainty for the technology sector. In this regard, we have appended an additional set of comments to this letter (**Annex**) outlining in detail our comments and recommendations for the December 28, 2018 version of the PDP Bill.

To ensure consumers and businesses alike can trust in and reap the maximum benefits from data driven innovations like artificial intelligence and the Internet of Things, BSA’s members greatly prioritize the protection of consumers’ personal data and the need for effective cybersecurity. Our members also provide essential technologies that safeguard the information security of systems, networks, and individuals.

⁸ <https://www.bsa.org/~media/Files/Policy/Data/02062018BSASubmissionThaiPersonalDataProtectionBill.pdf>

⁹ <https://www.bsa.org/~media/Files/Policy/Data/08042017BSACommentsrePersonalDataProtBill.PDF>

¹⁰ https://www.bsa.org/~media/Files/Policy/Data/03232015BSASubmissiononThaiPersonalDataProtectionAct_EN.PDF

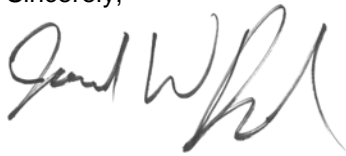
BSA appreciates the RTG's open and consultative process for the development of the PDP and Cybersecurity Bills. BSA has worked closely with governments around the world on cybersecurity and data protection policy and legislative developments. We strongly encourage Thailand to align to international best practices when developing, implementing, and operationalizing cybersecurity and personal data protection-related rules and requirements.

We hope that our comments will help to support the Committee and the National Assembly members as you debate of the Bills and prepare them for enactment.

Please do not hesitate to contact our representative for Thailand, Ms. Varunee Ratchatapattanakul at +66-8-1840-0591 or varunee@bsa.org with any questions or comments which you might have.

Thank you for your time and consideration.

Sincerely,

A handwritten signature in black ink, appearing to read 'Jared W. Ragland', written in a cursive style.

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

ANNEX: BSA COMMENTS ON PERSONAL DATA PROTECTION BILL

BSA thanks the RTG and the NLA for the opportunity to provide our comments on the PDP Bill. We have closely monitored the development of the PDP Bill and worked with the MDES and the ETDA. We appreciate the transparent manner in which the PDP Bill has been developed.

BSA members are at the forefront of data-driven innovation, including cloud-based technologies, data analytics, machine learning, and other cutting-edge technologies and services that promote economic development. Hence, BSA members recognize the importance of fostering trust and confidence in the online environment and are therefore deeply committed to protecting personal data across technologies and business models.

Indeed, BSA and our members view the enactment of an effective omnibus personal data protection law as an important step in Thailand's efforts to leverage the digital economy to drive economic growth and job creation. The continued development of these technologies requires a legal framework that is clearly defined and reasonably flexible and which protects consumer privacy without creating unnecessary barriers to international data flows, the lifeblood of the 21st century economy.

BSA provided comments on an earlier version of the PDP Bill in February 2018 with a view to achieving these objectives. The current version of the Bill contains improvements over previous drafts that would improve privacy protections for the Thai people. However, the PDP Bill also includes several provisions that still threaten to create unreasonable burdens and legal uncertainty for the technology sector. The following summarizes our key concerns and our comments in this submission:

1. The PDP Bill should establish a clear, default allocation of liability between data controllers and data processors, while allowing them to reallocate liability through contracts. Specifically, the primary obligation should rest with data controllers, with data processors following instructions pursuant to contractual agreement.
2. The definition of personal data should be clear. Business contact information and data de-identified through robust technical and organizational measures to reasonably reduce the risk of re-identification should not be considered to be personal data under the PDP Bill.
3. Specifying the principles by which data controllers can provide notice and obtain consent can provide certainty, but the PDP Bill should also provide flexibility for controllers to determine how best to operationalize such principles.
4. Restrictions on the international transfer of personal data do not advance personal data protection goals. Instead, they disrupt companies' operations and make it costlier to provide services. An adequacy requirement and other conditions on international data transfers, if imposed, should maximize consistency with existing mechanisms under data protection frameworks in other important markets.
5. Personal data breach notification requirements should focus on helping data principals avoid harm and should not interfere with businesses' responses to security incidents. In addition, the law should provide positive incentives, e.g. exemption from breach notification requirements if the data fiduciary has taken adequate organizational and technical measures (such as strong encryption) to make the data unusable.
6. Children deserve heightened data protections but setting the threshold for those additional protections at the age of 20 is inconsistent with other global approaches to ensuring children's privacy. Defining children, for purposes of heightened personal data protection, to be individuals under 13 provides sufficient protections for younger, more vulnerable children, while allowing older minors to more easily benefit from data-related services.
7. Including consumer rights, such as the right to data portability and the right to object to processing their personal data can enhance consumer protection, but for the operationalization of these rights to be practical, the formulation of guidelines, clarifications, and subsidiary legislation, must involve close consultation with the private sector.

8. The requirement to appoint a data protection officer (**DPO**) should be aligned with other privacy laws and apply only to data controllers or processors whose core activity requires regular and systematic monitoring of data subjects on a large scale. In addition, the PDP Bill should make it clear that the DPO does not need to be a resident of Thailand, and that corporate groups can appoint a single centralized DPO.
9. It is essential that the Personal Data Protection Committee (**Committee**) and the Office of the Personal Data Protection Committee (**Office**) operate in a manner that is fair, transparent, and predictable; the powers of the Committee and the Office should be appropriately limited, particularly when related to implementation of the Bill and conducting investigations.
10. Effective penalties and remedies are important elements of a personal data protection framework but imposing criminal penalties and individual liability is disproportionate to the risk of harm addressed in this context, inconsistent with internationally recognized best practices, and likely to chill legitimate data processing activities.
11. The scope of the Bill should be limited to entities or activities that have a sufficiently close connection to Thailand to ensure effective enforcement.
12. A reasonable time period between the enactment of the PDP law and its effective date of not less than two years should be provided to ensure smooth transition for individuals, businesses, and government agencies.

The following paragraphs provide a detailed explanation of our comments and recommendations for further review.

Clearer Distinction between Data Controllers and Data Processors (Sections 37, 39, 75-76 and 83-86)

At the outset, we highlight a key conceptual issue that remains a primary concern to us. The PDP Bill remains unclear on the distinction between a “personal data controller” (**data controller**) and a “personal data processor” (**data processor**). It is necessary that the allocation of responsibility and liability between a data controller and data processor is clear to ensure that the widespread practice of outsourcing does not create confusion in the overall personal data protection regime.

The data controller, and not the data processor, has the direct relationship with the personal data subject (**data subject**). Furthermore, the data processor collects, uses, or discloses personal data pursuant to orders given by or on behalf of the data controller, instituted via contractual obligations between the data processor and the data controller. Hence, the responsibility and liability for ensuring compliance with applicable personal data protection laws and requirements should fall primarily on the data controller. The data processor should only be concerned about complying with the instructions of the data controller and ensuring the security of the personal data it processes on behalf of the data controller. The relationship between the data processor and data controller should be governed by contract.

Imposing direct, joint, or several liabilities or other obligations on data processors would have a range of unintended consequences, would undermine the relationship between these actors, and would create unnecessary compliance and enforcement issues. In addition, this could also have a negative effect on potential investments and innovation in data processing and outsourcing services.

Recommendations

In order to make the distinction between the responsibilities of the data controller and the data processor clear, we recommend the following changes:

- Further amendments to the “duties” of the data processor in **Section 39** to clarify the allocation of liability between the data controller and data processor.
- Remove requirements on “data processors” that are applicable instead to “data controllers” from the Bill.

The following paragraphs provide specific reasons for the recommendations above.

I. Proposed Amendments to Section 39

Section 39 of the Bill introduces additional confusion between the roles of a data controller and data processor and suggests joint-liability between both the data controller and data processor by stating:

“...The data processor who fails to comply with (1) for the collection, use or disclosure of any Personal Data shall be regarded as the Personal Data Controller for the collection, use or disclosure of such Personal Data.”

Furthermore, the current drafting also suggests a direct contradiction with the definition of a data processor, as articulated in **Section 6** of the Bill “... whereby such person or juristic person is/are not the Personal Data Controller”.

We therefore urge NLA to amend **Section 39** as follows:

- (a) **Deleting the latter half of sub-section (1)** to reflect the fact that data processors may not be aware of the nature of the data provided to them, the previous consent or communications with the data subject sought by data controllers, or the particular legal requirements attached to such data. The data controller should be responsible for ensuring that the instructions it provides to the data processor do not violate any legal obligations. It is not reasonable or feasible for the data processor to investigate and confirm whether the data controller’s instructions are lawful. For example, typically if a data controller instructs a data processor to process the data that the controller has collected, the data processor has no way of independently verifying whether the appropriate consents were sought and that the subject was adequately notified.
- (b) **Amending sub-section (2)** to make clear that the requirement for the data processor to secure the data. We propose to remove “*loss of personal data and no unauthorized or illegitimate access, use, alteration, modification or disclosure of personal data*” as it is unnecessarily prescriptive. In addition, this sub-section should not create a separate data breach notification regime in addition to the requirement set out in Section 36(4). Therefore, we propose to delete “and notifying the data controller of personal data breaches”.
- (c) **Deleting sub-section (3)** since it would be unreasonable to expect a data processor to produce specific and distinct records for the different types of data it may handle. Again, to reiterate, many data processors may have very little insight into the specific nature of the data they process on behalf of others, and in fact many take active steps to ensure they have minimal awareness of such data as part of their commitment to the privacy and security of their customers and clients and their data.
- (d) **Deleting, paragraph 2**, as it introduces contradiction and confusion into the definition of a data processor. By way of **Section 6**, data processors are not data controllers, and act “*pursuant to the orders by or on behalf of*” data controllers.
- (e) **Including, at the end of Section 39, “*in each instance, as agreed in writing with the personal data controller.*”** to make clear that liability between data controller and data processor can be reallocated through contracts.

In sum, our proposed amendments to Section 39:

Section 39: The data processor shall have the following duties:

- (1) processing activities in relation to the collection, use or disclosure of personal data in accordance with the instructions of the data controller only ~~unless the instructions are not allowed by laws or the provisions of this Act in relation to the protection of personal data;~~

~~(2) implementing reasonable appropriate safeguards to secure the data, ensure no loss of personal data and no unauthorized or illegitimate access, use, alteration, modification or disclosure of personal data, and notifying the data controller of personal data breaches.~~

~~(3) prepare and maintain a record of data processing activities according to the regulations as set forth by the Committee; and~~

~~The data processor who does not act in compliance with (1) in relation to the collection, use or disclosure of personal data shall be regarded as the data controller for the collection, use or disclosure of personal data.~~

~~in each instance, as agreed in the contract with the personal data controller.~~

II. Removal of Other Personal Data Processor Requirements (including Sections 83-86)

As articulated above data processors do not have a direct relationship with data subjects and often do not have knowledge of or control over data processed pursuant to the orders given by or on behalf of a data controller. Given so, there may be no way for the data processor (e.g. a cloud service provider) to ascertain whether data it is processing is personal data, whether it pertains to sensitive data (per Section 26), or is a “large amount” of data (per Section 40(2)). Likewise, it would be disproportionate, for example, to impose civil liability on data processors given that they would be processing data pursuant to orders from, or on behalf of, a data controller, and may not have knowledge of the data processed. Hence, a data processor may not be able to determine the “reasonable” level of care to be afforded to the data. Therefore, we suggest that the following: **Amend sections 75-76 to remove reference to data processors and delete Sections 83-86,** as the civil and administrative penalties described in **Chapter 6 and Chapter 7** should be limited to the data controller and should not apply to the data processor.

The proposed changes in this submission to clarify and limit the requirements on data processors do not represent an exhaustive list. In general, we recommend that the NLA review all the proposed requirements on data processors and urge the NLA to avoid imposing unreasonable, unnecessary, and impractical requirements on data processors where the personal data protection obligations should rest more properly with data controllers. This will ensure that the law promotes effective protection of personal data by data controllers, while not inadvertently restricting how such data can be processed for the benefit of data subjects

Clarifying the definition of Personal Data (Section 6) and Anonymized and Pseudonymized Data (Sections 26, 33)

A. Business Contact Information and Anonymized/ Pseudonymized Data Should Not Fall Within the Definition of Personal Data

Section 6 contains a broad definition of “Personal Data” that encapsulates all data pertaining to a person that enables the identification of such person. We note that the revised PDP Bill no longer excludes from the definition of personal data “*data which specifies only the name, title, work place, or business address of an individual*”.

The transfer of business contact information is integral to many business processes, and the use of such information for business contacting purposes is often implied through the process of exchanging business contact information. Furthermore, it is unclear whether such business contact information belongs to the data subject or the organization by which the data subject is employed. Hence the inclusion of such business contact information under the definition of personal data could significantly impede business to business activities.

Recommendation

We urge the NLA to **reinstate the exclusion of business contact information from the definition of personal data** in **Section 6** as follows:

*“personal data means ... **but not including data which specifies only the name, title, work place, business contact information or business address of an individual, when used for contacting the individual solely for business purposes**”.*

B. Anonymized and Pseudonymized Data

Sections 26(5)(d) and 33 refer to Anonymized and Pseudonymized data. The PDP Bill does not adapt legal requirements in circumstances where other de-identification techniques, including anonymization and pseudonymization techniques, are used to mitigate privacy risks, including with respect to data breach notification obligations and risk assessments.

Recommendation

Incentivizing the use of de-identification techniques to protect personal data would benefit individuals and the economy since greater use of such techniques would reduce privacy and security risks. At the same time, the ability to use anonymized, pseudonymized, or de-identified data outside the framework of a data protection law will encourage innovative uses of data.

BSA therefore urges NLA to **clearly exclude data de-identified through robust technical and organizational measures that reasonably reduce the risk of re-identification from the definition of personal data**. Such de-identified data that has contractual controls, privacy and security controls, or both, and reasonably reduces the risk of re-identification, should therefore not be covered data under the PDP Bill, with the exception of security, or accountability requirements.

In addition, BSA recommends that NLA **adapt legal requirements in circumstances where anonymization, pseudonymization, or other de-identification techniques are used to mitigate privacy risks**, for example with respect to data breach notification obligations and risk assessments, to incentivize use of these practices.

Notice and Consent and Other Legal Bases for Handling Personal Data (Sections 19 – 29)

Sections 19 through 29 create a framework under which data controllers must provide notice to data subjects regarding the nature of their personal data handling efforts and acquire explicit consent from the data subjects, except in specified circumstances.

A. Deemed or Implied Consent

The standard for determining the level of consent that is appropriate should be contextual. In circumstances that do not implicate heightened sensitivity, implied consent may be appropriate.

Relying solely on explicit written consent as a legal basis for handling personal data would create the risks of: (1) stymying growth and innovation in the digital economy; and (2) not meeting consumer privacy expectations by leading consumers to “click fatigue,” where users simply accept whatever terms are presented to them without fully reviewing or understanding the presented information.

In today’s digital world, a large amount of data is created through individuals’ interactions with Internet-connected devices. Express consent is not suitable or practical in many instances, especially in circumstances that do not give rise to heightened sensitivity. For example, the future of public transportation services may be affected if an individual must provide express consent to allow an electronic gate to generate data every time he or she swipes a public transportation

card. In such circumstances, implied consent may be appropriate. In other circumstances, such as when handling sensitive health or financial data, affirmative express consent may be appropriate.

Recommendation

BSA urges the NLA to consider the various contexts in which personal data may be handled and allow sufficient flexibility in the PDP Bill for data controllers to determine the timing, standard, and mechanism for obtaining consent. In this regard, BSA recommends that the concept of “deemed or implied” consent be explicitly added to the Bill by amending **Section 19** as follows:

Section 19: *The personal data controller shall not collect, use or disclose personal data in case of no consent of the data subject is or has been given ~~in advance~~, except permitted to do so by the provisions of this Act or other laws.*

*The request for consent shall be made in writing or via electronic means, except the request by its nature cannot be done in the aforesaid manners **or where consent is deemed or can be implied in the circumstances;***

B. Legal Bases for Handling Personal Data

BSA remains supportive of the inclusion of a legitimate interests-like exception in **Section 24(6)** of the PDP Bill. We note that this inclusion was modeled on the “legitimate interest” basis in the European Union (EU) General Data Protection Regulation (GDPR),¹¹ and urge the NLA and the Committee in its implementation of **Section 24(6)** to offer a level of flexibility that is consistent to that of the EU-GDPR’s implementation of legitimate interests. The EU-GDPR’s legitimate interest basis allows organizations to expand business opportunities and yet remain compliant with their overall data protection obligations.

Furthermore, we recommend that rather than specifying legitimate interest and other bases as “exceptions” to a consent requirement, the PDP Bill recognize other legal bases, in addition to consent, for handling personal data.

Recommendation

BSA urges the NLA to amend the PDP Bill to provide for additional bases for processing personal data, in addition, rather than as an exception, to consent. These additional bases for processing include the legitimate interest of companies handling the data, the performance of contracts with the data subject, and compliance with legal obligations. The data protection framework need not identify a primary ground for processing. Instead, legal grounds should be generally applicable, and it should be up to the data controller to determine the relevant ground(s) — and to ensure that its processing activities comport with such grounds.

C. Specified Forms of Notice and Consent

The PDP Bill continues to propose in **Section 19** that the Committee can “*require the data controller to request consent from the personal data owner by using a form and statement prescribed by the Committee*”.

In cases where express consent may be required, while it may be useful to provide guidance to data controllers on what to include in their notifications to data subjects when seeking consent, it is also necessary to preserve flexibility in the form in which consent may be requested and given.

Due to constant 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

¹¹ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC.

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 such benefits.

Recommendation

We accordingly urge again the NLA to delete the text in Section 19 that contemplates that specific forms for consent may be required, as follows:

Section 19

...

In requesting consent from the data subject, the data controller must inform the purpose of collection, use or disclosure of personal data; and the request for consent must be clear and shall not be made to deceive the data subject or cause the data subject to misunderstand the purpose of collection, use or disclosure of personal data.; ~~and the Committee may require the data controller to request consent from the personal data owner by using a form and statement prescribed by the Committee.~~

D. Notification of Retention Time Period

The PDP Bill also introduces new notification requirements in **Section 23(2)** for data controllers to inform data owners either prior to or at the time of collection, “*personal data that will be collected and the period of collection*” or where that is not possible, the “*expected period of collection can be indicated based on the standard of collection*”.

Given the iterative nature by which data is collected and the new and innovative ways that personal data is used, as articulated in previous paragraphs, it would not always be practicable for data controllers to articulate at the onset of collection the time period for which collected data would be retained. It is also unclear based on the current drafting of Section 23(2) how data controllers would be able to state the “*expected period of collection*” as well as how “*the standard of collection*” would be assessed in order to indicate an expected retention period.

Recommendation

There may be circumstances where it would be impracticable for data controllers to articulate a time period for retention, whether actual or “expected”. Given so, we urge the NLA to amend Section 23(2) to provide more flexibility. Rather than providing notification of an “expected” time period, instead require data controllers to provide notification of the criteria and principles governing its retention policy. For example, data controllers could include in their retention policies that “personal data will only be retained for up to six months after there ceases to be a legal or business purpose to do so”. We recommend the following changes:

Section 23(2)

...

*personal data that will be collected and the period of collection; and in the event that the period of collection cannot be precisely indicated, **for organizations to provide information on their retention policies or principles.*** ~~*an expected period of collection can be indicated based on the standard of collection;*~~

E. Ambiguities in Consent Requirements

We remain deeply concerned that the PDP Bill may be interpreted to impose a separate duty on data controllers to obtain consent prior to using data that was lawfully obtained and with the knowledge of the data subject. In addition to the **Section 19** obligation to provide notification to data subjects in connection with the *collection* of personal data, **Section 27** remains ambiguous and could potentially be interpreted to impose a separate obligation to obtain consent prior to any *use or disclosure* of such data.

To avoid this ambiguity, **Section 27** should be amended to clarify that a data subject can provide consent for future uses of his or her personal data by agreeing to, or electing not to opt out of, the data controller's privacy policy. In addition, it should be made clear that data controllers are able to use personal data in a manner that is consistent with that explanation, the context of the transaction, or reasonable expectation of the consumer, or in a manner that is otherwise compatible with the original purpose for which the data was collected.

Without clarifying this ambiguity, such a requirement could seem at odds with the APEC Privacy Framework and, as a practical matter, would be untenable for modern data-intensive services, such as cloud computing. The APEC Privacy Framework sets forth a reasonable system that ensures consumers receive notification about the type of data an online product or service will collect *and* how that data will be put to use. The Notice Principle enables consumers to make informed decisions about whether they are comfortable with an online service's data collection practices. The APEC Privacy Framework further recognizes that the operator of an online service may use data it has collected from consumers to the extent such uses are consistent with the terms described in the notification.

Indeed, there are a wide range of mechanisms that enable users to consent to and control the collection and use of their information, and some of the more robust opt-out mechanisms provide stronger protections for consumer privacy (with fewer disruptions for Internet users) than weaker opt-in mechanisms.

Recommendation

To ensure that **Section 27** is interpreted consistently with the APEC Privacy Framework, we again urge the NLA to amend the provision accordingly as follows:

Section 27

~~The data controller shall not use or disclose the personal data without consent from the data subject, except the personal data permitted to be collected without consent under Section 24 or Section 26;~~ **may use, transfer, or disclose personal data only to fulfill the purposes of collection, in a manner that is consistent with that explanation disclosed to the data subject pursuant to Section 23 and the context of the transaction, or reasonable expectation of the consumer, or in a manner that is otherwise compatible with the original purpose for which the data was collected, except where:**

- 1. the data subject has granted consent;**
- 2. the use or disclosure is necessary to provide a service or product requested by the data subject;**
- 3. the use or disclosure is necessary to fulfill a legal obligation; or**
- 4. the personal data collected was collected in accordance with Section 24.**

International Transfers of Data (Sections 16(5) and 28 – 29)

A. Further Clarification to the Framework and Processes for International Transfers

I. Incorporating Accountability Approaches into the Framework for International Transfers

The current PDP Bill suggests an adequacy approach as the linchpin for international data transfers. Requiring the Committee to establish adequacy arrangements with other jurisdictions, would be significantly burdensome for the Committee. For example, experience with the adequacy requirement in the EU's Data Protection Directive (now included in the GDPR) points to several significant drawbacks in instituting such a requirement. Adequacy reviews are time-consuming and extremely resource intensive. The result is that the EU has concluded few adequacy determinations. Adequacy reviews also focus heavily on formal legal standards, which may not provide a complete picture of the safeguards in a country. Stated another way, the mere existence of formal legal protections in a country does not necessarily guarantee a high level of personal data protection in practice.

The NLA should instead consider how accountability concepts can be incorporated into the framework for international transfers. The “accountability model”, first established under the Organisation for Economic Co-operation and Development (OECD) *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*,¹² and subsequently endorsed and integrated in a variety of data protection frameworks around the world, provides an approach to cross-border data governance that effectively protects the individual and fosters streamlined, robust data flows. The accountability model requires organizations that collect and use data to be responsible for the protection and appropriate use of the data no matter where, or by whom, it is processed. It also requires that organizations transferring data must take appropriate steps to be sure that any obligations — in law, guidance, or commitments made in privacy policies — will be met.

Hence, instead of an adequacy-focused approach, the NLA should consider introducing accountability concepts into **Sections 28 and 29**, making **it clear that data controllers who are transferring data internationally are ultimately responsible for the protection and appropriate use of that data in any third country or international organization**. Relying on this accountability model would effectively protect and promote the responsible use of personal data.

Furthermore, while rules to be established pursuant to **Section 28 and 16(5)** may be helpful generally, it is critical that the measures, guidelines, rules, and approaches to exemptions are aligned, to the extent possible, with internationally recognized best practices and standards. The global nature of the digital economy makes it imperative that governments continue to ensure the free flow of data across borders and avoid requirements that impose unnecessary or burdensome restrictions on international data transfers. Hence, BSA strongly discourages the NLA from imposing burdensome restrictions on international data transfers and to clarify in the PDP Bill that data controllers will be free to transfer data internationally so long as they continue to protect the data or otherwise comply with internationally recognized practices, such as a commitment to abide by the APEC CBPR.

II. Do Not Require Prior Approval by the Committee and the Office before Personal Data Can Be Transferred

Sections 28 and 29 appear to require “prior approval by the Office” for transfers to third countries and international organizations, as well as intra-organization transfers overseas.¹³ In particular:

- **Section 28, paragraph 1** requires that personal data be transferred with an “adequate level of protection” based on “*the determination of the Committee*”. It is unclear based on the current PDP Bill whether this “determination” would be made on a case-by-case basis and if organizations would require prior approval for the international transfer of data generally.
- In addition, **Section 29, paragraph 1** requires organizations to subject their personal data protection policies to the Office for review and prior approval for intra-organizational international transfers.
- **Section 29, paragraph 2** requires a determination by the Committee of the nature of “group of undertakings”, “group of enterprises”, and criteria and process for review.
- Furthermore, **Section 29, paragraph 3** states that in the absence of an approval, data controllers and data processors can send or transfer data abroad on condition that the enforcement of data subject rights and remedies are based on a Committee-determined set of criteria and methods. It is unclear based on the current PDP Bill whether this

¹² At www.oecd.org/sti/economy/oecdguidelinesonthe protectionofprivacyandtransborderflowsofpersonaldata.htm

¹³ Section 29, paragraph 1, describes “intra-organization transfers” as transfers of “...*Personal Data to the Personal Data Controller or Personal Data Processor who is in a foreign country and in the same affiliated undertaking or affiliated business...*”

determination likewise must be made, and approval given, on a case-by-case basis, prior to a transfer.

Requiring the Committee to approve individual requests for international data transfers, or approving policies “of the protection of personal data” for intra-organization transfers, would be significantly burdensome on the Committee. It would also create an onerous and unnecessary layer of compliance. In practice, it would be infeasible for data controllers and processors that rely on Internet- or cloud-based solutions to seek approval for every country or organization to which data is transferred. Such a requirement would severely impede the ability for companies to deliver digital services to consumers in Thailand.

III. Clarification of Applicability of Section 29 Paragraph 3

Pursuant to **Section 29**, Intra-organization transfers are exempt from the **Section 28** adequacy requirements provided that such transfers meet the requirements outlined in **Section 29**. However, **Section 29, paragraph 3** provides a means for international transfers in the absence of a Committee decision of **Section 28 and Section 29, paragraph 1**. This has introduced potential inconsistency in the PDP Bill and confusion on whether **Section 28** committee decisions would apply to intra-organization transfers that meet the requirements set out in Section 29.

Likewise, the language in **Section 29, paragraph 3** inadvertently creates confusion on whether an obligation is introduced for data processors to ensure that data transferred internationally is done so in compliance with **Section 28** and the rules to be established pursuant to **Section 16(5)**. This is inconsistent with the language in **Section 28** itself, which clearly places responsibility on the data controller rather than the data processor. Imposing direct, joint, or shared liability on data processors would insert confusion into the accountability model. In addition, data processors do not generally have direct relationships with data subjects or may not have knowledge of the kinds of data being processed on their service on behalf of their customers. As such, data processors may not be able to establish whether an international transfer of data contains personal data and would therefore require approval or review from the Office and Committee.

Given so, it is imperative that the NLA make clear that:

- a. **Section 28** Committee decisions do not apply to intra-organization international transfers that meet the requirements in Section 29; and
- b. **Section 29, paragraph 3**, applies to both decisions that are made in relation to Section 28 international transfers, and Section 29, paragraph 1.

Recommendation

In line with internationally recognized best practices and the concerns we have raised, we urge the NLA to implement a full accountability-based model for international data transfers, and further clarify the framework for international data transfers by making the following changes:

- (a) Amend **Section 28** to make it clear that data controllers who are transferring data internationally are ultimately responsible for the protection and appropriate use of that data in a third country or international organization, and for international intra-organization transfers. Therefore, data controllers that take appropriate steps to ensure an adequate level of protection or have provided appropriate safeguards that provide an equal level of protection, can transfer personal data internationally.
- (b) Make clear that no prior approval is required by the Office for the processes identified under part II of this section:
 - Specifically, for intra-organization transfers, we urge the NLA to delete Section 29 paragraphs 1 and 2 in their entirety and implement a full accountability-based model for international data transfers. The NLA can instead recognize intra-organization transfers that meet the requirements under **Section 28**.

- Nonetheless, if the NLA decides to retain a review and determination framework for intra-organization transfers, we propose the NLA make clear that **this framework exists as an additional option for international transfers, in addition to the mechanisms under Section 28. This framework should not be made mandatory for intra-organization transfers.**

- (c) Amend **Section 28** to clarify that in the absence of a Committee decision, data controllers are permitted to transfer data consistent with methods determined by the Committee, which themselves should be consistent with internationally recognized standards of data protection.

In order to achieve these outcomes, we recommend the NLA make the following changes to **Section 28** of the PDP Bill and delete **Section 29**:

Section 28

*In the event that the data controller sends or transfers the personal data abroad, **the data controller shall take appropriate steps to ensure that** a third country or an international organization to which the personal data will be sent or transferred must ensure an adequate level of protection based on the determination of the Committee under Section 16 (5), **or if the data controller has provided appropriate safeguards that provides a standard of protection to personal data so transferred that is comparable to the protection under this act, except:***

...

In case that there is a problem with the adequacy of the level of protection in a third country or an international organization to which the personal data is sent or transferred, the Committee shall consider the problem; the decision of the Committee may be changed upon a request with new information that reveals developments in a third country or an international organization that prove the adequacy of the level of protection.

In absence of a decision of the Committee in Section 28, the data controller may send or transfer the personal data abroad if the data controller has provided appropriate safeguards without requiring any specific prior authorization from the Committee.

B. Provide Additional Avenues for Transferring Personal Data that Explicitly Recognize Internationally Recognized Standards and Best Practices

BSA is supportive of privacy laws that do *not* impose material restrictions on international transfers of data, and that provide clear and flexible mechanisms for transfers that are aligned to internationally recognized best practices and standards. International data transfers are often made with commitments assumed in international cooperation agreements — including industry codes of conduct or frameworks developed through open, multi-stakeholder processes — which provide additional assurances that companies will appropriately safeguard personal data.

Proposed revisions to **Sections 28-29** of the PDP Bill provide some additional mechanisms for international transfers of data. Nonetheless, no single data transfer mechanism alone is likely to meet the needs of modern technologies and services.

Recommendation

BSA continues to urge that the PDP Bill explicitly recognize additional data transfer mechanisms that would allow companies to adopt alternative, legally binding protections including:

- (a) **Internationally recognized best practices, certifications, and standards.** Companies that subscribe to global best practices and/or are certified to internationally recognized standards signal their commitment to appropriately safeguarding internationally

transferred personal data. Therefore, the PDP Bill should recognize that organizations meeting such best practices or certified to such standards, comply with the international transfer requirements under the Bill. These internationally recognized standards should include the EU GDPR Binding Corporate Rules and Standard Data Protection Clauses,¹⁴ and the APEC CBPR certification;

- (b) **Additional bases for transfer:** The NLA could also consider including the bases set out in GDPR Article 46 as permitted means to transfer personal data outside of Thailand. In particular, we would recommend the PDP bill to recognize GDPR permitted standard contractual clauses, binding corporate rules and approved codes of practices as a bases for international transfer.

Data Breach Notification (Section 36(4))

BSA supports the creation of a personal data breach notification system applicable to all businesses and organizations. Appropriately crafted data breach provisions incentivize the adoption of robust data security practices and enable individuals to take action to protect themselves in the event their data is compromised. When developing data breach notification provisions, it is critical to recognize that not all data breaches represent equal threats. In many instances, data breaches pose no actual risks to the individuals whose data was compromised.

To ensure that consumers are not inundated with notices regarding immaterial data breaches, the notification obligation should be triggered only in circumstances that pose credible risks of harm to users.¹⁵ However, the PDP Bill currently does not provide for any exceptions to notification. This is not in line with international practice and could lead to over notification and notification fatigue and ultimately diminish the usefulness of the requirement for breach notification to data subjects. The PDP Bill can consider including appropriate exceptions to the data breach notification requirement in line with international practice. In particular, the PDP Bill should include at least the following exceptions to the notification requirement:

- a. where the data controller or data processor has implemented appropriate technical and organizational measures, for example to render the personal data unintelligible to any person who is not authorized to access it;
- b. where the data controller or data processor has taken subsequent measures which ensure that the risk of harm is no longer likely to materialize;
- c. where the notification would involve disproportionate effort. In such a case, instead of notification to an individual there should be a public communication or similar measure whereby the data subjects are informed in an equally effective manner;
- d. where there is inconsistency with obligations contained in other applicable law; or
- e. where notification would compromise an ongoing or potential a law enforcement investigation carried out by authorized law enforcement agencies.

Finally, to ensure data owners receive meaningful notifications in the event of a breach, it is critical that data controllers are afforded adequate time to perform a thorough risk assessment to determine the scope of the security risk and prevent further disclosures. It is therefore counterproductive to include within the data breach provision a fixed deadline for providing notification.

¹⁴ Issued pursuant to EU GDPR Article 47 and Article 93(2) respectively.

¹⁵ Examples of international approaches to ensuring breach notification requirements only apply in circumstances where there is a credible risk of harm include:

- Australia's Privacy Act 1998 (Amended 2017), Section 26WA: "likely to result in serious harm"
- Canada's Personal Information Protection and Electronic Documents Act (2015), Section 10.1 (1): "real risk of significant harm to an individual"
- Philippines Data Privacy Act of 2012, Section 20: "likely to give rise to a real risk of serious harm to any affected data subject",
- EU GDPR, Article 33: notification required unless the breach is "unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons"

Recommendation

We urge the NLA to amend **Section 36(4)** to ensure that the proposed personal data breach notification framework: (1) enables data owners to receive meaningful notices; (2) allows data controllers to focus on dealing with the immediate security risks and preventing further disclosures, and (3) makes clear the allocation of liability and responsibilities in the event of a data breach. The proposed revisions to **Section 36(4)** will achieve the following outcomes:

- (a) **Include a risk-based measure, such that data breach notification requirements are only triggered where the breach “creates a material risk of harm”** in order to better balance the amount and types of notifications data owners receive and avoid data owners being inundated with notifications. In addition, **data breaches that involve encrypted or indecipherable data should not be subject to breach notification requirements.**
- (b) **Qualify the requirement for immediate notification with no “undue delay”** to provide flexibility for data controllers to manage resources and priorities in the immediate aftermath of a breach.
- (c) Include **other exceptions to data breach notifications** as outlined above.

We propose to revise **Section 36(4)** as follows:

Section 36

...

(4) *notifying the data subject of a personal data breach **that creates a material risk of harm** without undue delay; if **the breach creates a material risk of harm and the number of persons affected is higher than what is as** announced by the Committee, the data controller shall notify the Committee of the personal data breach and measures to be taken to address the personal data breach without undue delay, and the notification of personal data breach shall comply with the regulations set out by the Committee.*

Notwithstanding the foregoing, a data controller shall not be required to provide any notification if:

- a. **the compromised data was stored in a manner that renders it unusable, unreadable, or indecipherable to an unauthorized third party through practices or methods that are widely accepted as effective industry practices or industry standards;**
- b. **the data controller or its data processor has taken subsequent measures which ensure that the risk of harm is no longer likely to materialize**
- c. **the notification would involve disproportionate effort. In such a case, instead of notification to an individual there should be a public communication or similar measure whereby the data subjects are informed in an equally effective manner**
- d. **there is inconsistency with obligations contained in other applicable law; or**
- e. **notification would compromise an ongoing or potential a law enforcement investigation carried out by authorized law enforcement agencies.**

Consent Requirements for Minors, Incompetent Persons, and Quasi-Competent Persons (Section 20)

Consistent with the GDPR and the United States’ Children’s Online Privacy Protection Act (COPPA),¹⁶ BSA supports considering the personal data of children to be sensitive and providing

¹⁶ See generally 15 U.S.C. § 6501 *et seq.* and 16 C.F.R. Part 314.

heightened data protections for their data. However, the Bill's upper age limit of 20 years¹⁷ clashes with other standards for protecting children's data. For example, COPPA applies to children under 13 years old, providing appropriate protections to individuals at the most vulnerable ages. The GDPR sets the upper age limit of children at 16 but allows EU member states to lower the age to 13.¹⁸ The inconsistency of the PDP Bill with COPPA and the GDPR, especially the inclusion of much older minors as requiring the higher protections, could prevent some children — particularly middle and older teenagers — from accessing services that will be beneficial to them. In BSA's view, defining children, for purposes of heightened personal data protection, to be individuals under 13 provides sufficient protections for younger children who are particularly vulnerable, while allowing older minors to more easily benefit from data-related services.

Other Consumer Rights and Accountability Mechanisms (Sections 31, 32, 33, and 38)

BSA strongly supports giving individuals more control over their data. The inclusion of additional consumer rights that align to internationally recognized best practices, including the right to data portability (Section 31), the right to object to the collection, use, or disclosure of personal data (Section 32), and the right to destroy or temporarily suspend on processing of personal data (Section 33), as well as the introduction of accountability mechanisms, such as requirements for controllers to maintain records of processing activities (Section 38), serve to achieve this outcome. While these rights and accountability mechanisms lay a strong foundation for a robust data protection framework in Thailand, it is imperative that the implementing regulations or clarifications retain flexibility and are not overly prescriptive. Otherwise, these obligations can cause practical operational challenges, increasing the cost of compliance and lessening the incentives for businesses in Thailand to use data and technology in innovative ways.

In addition, certain rights, for example the requirement that a personal data owner (or data subject) is entitled to obtain personal data in a format that is generally readable or usable by automatic machines and tools (**Section 31**) should be tempered by allowing the data controller to determine the means and format that is practical and technically feasible. Furthermore, the requirement for data controllers to directly send personal data to other controllers (**Section 31(2)**) could inadvertently create cybersecurity risks and have an adverse impact on the protection of personal data.

We urge the NLA to consider the inclusion of these rights carefully, and for Committee to carry out open engagement with industry as guidelines, clarifications, and subsidiary legislation is developed.

Data Protection Officer (Section 40)

The criteria that triggers the requirement to appoint a DPO should be consistent with other privacy laws. In addition, the PDP Bill should clarify that a DPO does not need to be a resident of Thailand and that a corporate group (or group of undertakings) can appoint a single DPO to enable such companies to centralize and operate their intra-group privacy standards consistently in a world of increasingly overlapping privacy laws. The current language in the PDP Bill does not provide for this. This change would bring this requirement in line with other privacy laws such as the GDPR.

The PDP Bill stipulates that the contact details of the DPO of both the data processor and data controller need to be informed to the data owner and the data owner should be able to contact both the data processor and the data controller in respect of its rights. This is not appropriate for data processors (e.g. cloud providers) that have limited to no knowledge of whether their systems are being used to process personal data within the scope of the PDP Bill and have no contact or relationship with the data subjects. The obligations of the data processor should be focused on implementing reasonable and appropriate security measures for their systems.

¹⁷ Thai Civil and Commercial Code Section 19.

¹⁸ See GDPR art. 8(1).

Powers of the Committee (Sections 8-18, 88), Office, and Expert Committees (Sections 69 - 74)

BSA supports Thailand's effort to create a centralized personal data protection authority to promote privacy and the protection of personal data and to oversee the enforcement of the personal data protection law.

However, we remain concerned that several provisions may confer overly-broad powers to the Committee and the Expert Committees appointed under **Section 69**. This includes a variety of open-ended powers for the Committee "*to determine a measure or guideline in relation to personal data protection in order to ensure compliance with this Act*" (**Section 16(3)**).

We also note, for instance, that **Section 70(2)** grants the Expert Committees undefined authority to review or consider "*all personal data processing activities*" of a data controller or data processor and its employees or contractors regarding personal data. **Section 73** authorizes the Expert Committees to exercise subpoena authority not only in the context of investigating a complaint, but also in furtherance of "*any other matter*" that they may deem appropriate.

In addition to inspection powers, etc., **Section 72** grants the Expert Committees the power to impose harsh and potentially disproportionate penalties against entities found to be non-compliant with orders to (1) take corrective action or (2) avoid or mitigate causing harm to the data subject. While it is indeed important to have mechanisms to encourage compliance, we are concerned that the proposed penalties for non-compliance are too severe and could be abused. **Section 88** grants the Secretary General of the Office broad authority to determine fines and penalties but provides no guidance on what factors will be considered and how assessment of mitigating factors will be determined.

By offering little direction to the Committee, Office, and Expert Committees, and without any explicit provisions in this Bill to ensure there will be proper systems of checks and balances and due process, we are concerned that the Committee, Office, and Expert Committees may issue overly broad orders or overly harsh penalties that may have an adverse effect on data controllers, their employees, and/or their contractors.

It is also critical that any measures, guidelines, or rules adopted by the Committee under such powers are aligned, to the extent possible, with internationally recognized best practices and standards. The global nature of the digital economy makes it imperative that governments avoid creating country-specific rules that will only serve to stymie investment in the development and deployment of cutting-edge technologies, while providing no benefit, and in many cases harming, the goal of protecting privacy.

Incorporating appropriate checks and balances will ensure that it is commercially practical for organizations to comply with requests for information and investigations. Organizations should also have an appropriate and clear avenue to have decisions requiring disclosure of documents reviewed and to appeal decisions that are not reasonable. The Bill could for example draw from the Ninth Schedule of the Singapore Personal Data Protection Act that sets out the parameters and the manner in which the Personal Data Protection Commission's powers are to be exercised.

Recommendations

At a minimum, and consistent with principles of checks and balances and due process, we recommend that the NLA put in place safeguards to ensure the proper exercise of the authorities' powers, including under **Sections 16, 70, 73, and 88** and that legitimate privacy interests are not undermined.

Among other possible safeguards, such as including limited and strict criteria for how such powers can be exercised, the PDP Bill should provide an avenue of appeal for data controllers and their employees and contractors against decisions and orders, and in particular allow them to seek judicial review of such decisions. For an open and transparent process when determining measures or approaches and issuing or announcing notifications, rules, or guidelines, it is also

necessary that Committee solicits the input of interested stakeholders and takes into consideration industry's views.

We also recommend the NLA provide additional criteria under **Section 88** on how the Secretary General assess fines and penalties and mitigating factors.

Civil and Criminal Liability (Sections 75-79)

A. Civil Liability

Section 75 appears to impose strict liability with no accommodation for acting reasonably or undertaking mitigating efforts.

In addition, the compensation regime set out in the PDP Bill is not consistent with privacy laws elsewhere in the world including the GDPR. A data processor should not be liable to a data subject unless the data processor has acted contrary to the lawful instructions of the data controller. Data processors typically do not make the decisions about collection, use, or disclosure of personal data and have limited or no information regarding these decisions. It is therefore not reasonable to subject them to the same liability for compensation as a data controller.

Recommendation

In addition to our suggested changes in part 1(II) of this submission, that the references to "Data Processor" in **Sections 75 and 76** should be removed, we also recommend additional amendments to bring this provision in line with the GDPR, specifically, that data processors would be liable for damage caused by processing only if such activity was not in compliance with the Act.

In addition, **Section 76** should include more transparent criteria for the imposition of this administrative penalty by, for example, incorporating the considerations that are set out in Article 83 of the GDPR. As it stands, broad discretion is granted to the court but without clear criteria to assist the court to exercise this discretion in a fair and transparent manner.

We also suggest adding an additional factor that may protect a data controller against strict liability. Our proposed changes to **Section 75 and 76** are reflected as follows:

Section 75

*The data controller ~~or the data processor~~ who carries out personal data processing activities that infringe or do not act in compliance with this Act shall compensate for any damage the data subject suffers, regardless of whether the activities are performed purposefully unless the data controller ~~or the data processor~~ can prove **or demonstrate** that:*

...

(3) it was acting reasonably or undertaking efforts to mitigate the damage to the data subject.

The compensation as referred to in paragraph one shall include all expenses the data subject pays, as necessary, to prevent and mitigate the damage.

A data processor shall be liable for the damage caused by processing only where it has not complied with obligations of this Act specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller.

Section 76

The court shall have the power to order the data controller ~~or data processor~~ to pay an additional amount of compensation...benefits the data controller ~~or the data processor~~ gains, financial status of the data controller ~~or the data processor~~, efforts the data controller ~~or the data processor~~ has to mitigate the damage or responsibility of the data subject for the damage.

The claim for damages caused by processing that infringes this Act...about the data controller ~~or the data processor~~ who shall be responsible for processing...

B. Criminal Liability

BSA is very concerned with the PDP Bill's proposed application of criminal penalties, including individual criminal liability, to violations of the law. Criminal penalties do not have a useful role to play in data protection laws and, while present in some jurisdictions, are far outside of international norms. Such remedies are therefore disproportionate to the risks addressed in a data protection framework.

The substantive requirements of the PDP Bill, combined with monetary relief and conduct remedies provided through administrative or civil judicial processes, are sufficient to effectively protect individuals' privacy interests. In contrast, the risk of criminal liability can chill beneficial and harmless data practices, as illustrated in the following section of this submission. Furthermore, the bar for criminal liability is disproportionately low — **Section 77, paragraph 1**, provides for criminal penalties to be imposed if the failure to comply with the specified sections of the Act is merely *likely* to cause another person damage, reputational harm, etc.

Moreover, the PDP Bill's imposition of individual criminal liability in **Section 78** for “*Any person who access other person's personal data caused by performing of his or her duties under this Act and disclose the personal data to a third party*” as well as **Section 79** where “*the infringement of this Act is caused by ... any person who fails to instruct or perform, the board member, management or such person shall be subject to penalties as provided in this Act*”, is even more concerning.

Establishing liability for “any person” is inappropriate given the nature of data governance and data management practices. For example, if the offence consists of the violation of the obligation to collect, use, or disclose data in line with an exception under **Section 24**, then the number of persons that may be involved in this violation can be very large — across functions and potentially geographies — and implicate people with little actual responsibility. This is one of the reasons why liability for such offences should lie with the company and not with individuals. The high fines for the company and other non-compliance risks, including reputation damage and loss of business, encourage companies to deter employees from violating policies that the company needs to establish in order to ensure compliance with relevant laws and requirements.

Recommendation

We therefore strongly urge the NLA to eliminate the imposition of criminal liability for breaches of the Bill, **by deleting Sections 77-79 in its entirety.**

Territorial Scope of the PDP Bill (Section 5)

Section 5 of the PDP Bill has been revised to extend the territorial scope of the Bill 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... behaviors*” to any data subject who is in the Kingdom. BSA recommends limiting the scope of the PDP Bill to entities or activities that have a sufficiently close connection to Thailand in order to ensure effective enforcement of orders against foreign entities.

BSA recommends that the NLA limit application of the data protection law to data processing performed by an individual or legal entity, whether public or private, provided that: (1) Thai residents are specifically targeted; (2) the personal data that is the object of the processing is purposefully collected from data subjects in Thailand at the time of the collection, and (3) such collection is performed by an entity established in Thailand 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 would be insufficient, on their own, to establish the applicability of the Act.

Transition Period of the Law (Section 2)

It is critical for the NLA to ensure that the Act does not apply retroactively and to provide a reasonable period of time between the enactment of Act and its effective date. Individuals, businesses, and the Government will benefit from an orderly transition that does not impose abrupt changes to practices and risks and does not require the implementation of such changes in practices under threat of enforcement. **Section 2** currently states that the law will come into effect one hundred and eighty days from the date of publication in the *Royal Gazette*. One hundred and eighty days is an extremely short transition period and will be an insufficient amount of time for many organizations to implement the requirements of the Act. Furthermore, it is not in line with international practices. We note that other jurisdictions have allowed a two-year transition period. Given so, **we urge the NLA to provide in Section 2 a transition period of not less than two years.**

Conclusion

BSA appreciates the NLA's efforts in developing a modern personal data protection law to protect the privacy of Thailand's citizens. As properly drafted legislation leads to effective enforcement, BSA respectfully requests that serious consideration be given to the above comments and recommendations to achieve the best solution for all stakeholders.

We remain open to further discussion with the NLA or its designated representatives at any time. Please feel free to contact **Ms. Varunee Ratchatapattanakul, BSA's Thailand Country Manager**, at varunee@bsa.org or **+668-1840-0591** with any questions or comments which you might have.

Thank you for your time and consideration.