Permanent Secretary
The Ministry of Digital Economy and Society
120 Moo 3, 6-9 floor, The Government Complex
Commemorating His Majesty, Chaeng Watthana,
Thung Song Hong, Laksi, Bangkok 10210

February 6, 2018

RE: BSA COMMENTS ON DRAFT PERSONAL DATA PROTECTION ACT

Dear Permanent Secretary,

BSA | The Software Alliance (BSA)[1] thanks the Ministry of Digital Economy and Society (MDES) for the opportunity to participate in MDES's public hearing on the latest draft of the Personal Data Protection Bill (Bill) in Bangkok on January 25, 2018.

As we have noted over the last several years, 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.

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 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.

The continued development of these technologies requires a legal framework that is clearly defined and reasonably flexible, and which protects consumer privacy while not creating unnecessary barriers to international data flows, the lifeblood of the 21st century economy.

We provide the comments below to assist MDES in achieving these objectives. The current version of the Bill contains significant improvements over previous drafts. However, we propose recommendations on several provisions that still threaten to create unreasonable burdens and legal uncertainty for the technology sector, specifically those concerning:

- Personal Data Processors;
- Notice and Consent and Other Legal Bases for Handling Personal Data;
- International Transfers of Data;

[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, Amazon Web Services, ANSYS, Apple, Autodesk, AVEVA, Bentley Systems, Box, CA Technologies, Cisco, CNC/Mastercam, DataStax, DocuSign, IBM, Informatica, Intel, Microsoft, Okta, Oracle, salesforce.com, SAS Institute, Siemens PLM Software, Splunk, Symantec, The MathWorks, Trend Micro, Trimble Solutions Corporation, and Workday.

- Data Breach Notification; and
- Powers of the Personal Data Protection Committee (PDPC) and Expert Committees

Personal Data Processors (Sections 29 and 70)

We welcome the definition of "personal data processor". This makes clear the distinction between (1) an entity playing the role of a personal data controller (data controller), which has the authority and duty to make decisions regarding the collection, use, or disclosure (collectively "handling") of personal data, and (2) an entity playing the role of a personal data processor (data processor), which processes personal data pursuant to the instructions of the data controller.

The Bill would be further improved by better differentiating these two roles. Specifically, because the data controller, and not the data processor, has the direct relationship with the personal data subject (data subject), the responsibility and liability for ensuring compliance with applicable personal data protection law 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 left to be governed by contract.

This clear allocation of responsibility and liability is critical and ensures that the increasingly widespread practice of outsourcing does not create confusion in the overall personal data protection regime. This allocation allows the data subject and the legal authorities to know to which organizations they should turn in case of a problem, and organizations that handle personal data to have clarity on their respective roles and responsibilities.

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 burdens. In addition, this could also have a negative effect on potential investments and innovation in data processing and outsourcing services.

In short, data controllers should have the primary obligation for ensuring compliance with applicable personal data protection law, whereas data processors should only be required to comply with data controller instructions (through contractual mechanisms) and to ensure the security of the data they process.

Recommendations

In line with the above, we urge MDES to amend **Section 29** as follows:

> ***Section 29*** *A personal data processor shall have the following duties:*
> *(1) to process collection, use or disclosure of personal data in accordance with the instruction of personal data controller only, ~~except where such instruction is illegal or violates the principles of personal data protection as described in this Act~~; and*
> *(2) to provide appropriate security measures to prevent the loss, access to, use, modification, amendment or disclosure of personal data without authorization or in a wrongful manner, ~~and to notify personal data controller of personal data breach incidents as occurred; and~~*
> *~~(3) to produce and save a record of data processing activities as prescribed by the Committee.~~*
> ***in each instance, as agreed in writing with the personal data controller.***

Our recommended amendment to **Section 29(1)** is designed to reflect that the primary means by which the data processor understands whether and how to handle the personal data provided to it by a data controller is through a contractual arrangement between the two parties. We propose 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 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.

Our recommended amendment to **Section 29(2)** reflects our view that the requirement for the data processor to notify personal data breaches to the data controller, and under which circumstances, should be established as part of the contractual arrangement between the two parties.

We recommend deleting **Section 29(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.

For similar reasons, we suggest that the legal penalties described in **Chapter 8** should be limited to the data controller, and that the current **Section 70** be deleted in its entirety.

In regard to other proposed changes to the Bill, we urge MDES to eliminate and to avoid adopting 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 effectives protection of personal data by data controllers, while not inadvertently restricting how such data can be processed for the benefit of data subjects.

Notice and Consent and Other Legal Bases for Handling Personal Data (Sections 16 – 24)

Legal Bases for Handling Personal Data

Sections 16 through 24 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.

We note the inclusion of a legitimate interest exception to the consent requirement in **Section 20(4)**. This is an extremely important and positive development.

Recommendation

Rather than specifying legitimate interest and other bases as "exceptions" to a consent requirement, BSA urges the MDES to amend the PDP Bill to recognize other legal bases, in addition to consent, for handling personal data.

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.

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 information presented to them.

In today's digital world, a large amount of data is created through individuals' interactions with Internet-connected devices, and express consent is not suitable or practical in all 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 the handling of sensitive health or financial data, affirmative express consent may be appropriate.

Recommendation

BSA urges that MDES consider the various contexts in which personal data may be handled, and allow sufficient flexibility in the 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 16** as follows:

> ***Section 16:*** *A personal data controller cannot collect, use, or disclose personal data without the prior consent or consent at the time of a personal data owner, unless permitted under this Act or by other laws;…*
>
> *Consent shall be requested in writing or through electronic systems, unless such method is not possible by nature,* ***or where consent is deemed or can be implied in the circumstances****;*

Specified Forms of Consent

The Bill also proposes in **Section 16** that the PDPC can "*require the personal data controllers to request consent from the personal data subject in accordance with the 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 such consent, it is also necessary to preserve flexibility in the form in which consent may be 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 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 MDES to delete the text in Section 16 that contemplates that specific forms for consent may be required, as follows:

> ***Section 16***
> *…*
> *To request consent from a personal data owner, a personal data controller shall notify the personal data owner of the objective for the collection, use, or disclosure of personal data. The request for consent shall not be deceptive or mislead the personal data owner in terms of the objectives.* ~~*The Committee may require the personal data controller to request consent from the personal data owner in accordance with the form and statement prescribed by the Committee;*~~

Ambiguities in Consent Requirements

We remain deeply concerned that the Bill may be interpreted to impose on data controllers a separate duty to obtain consent prior to using data that was lawfully obtained with the knowledge of the data subject. In addition to the **Section 16** obligation to provide notification to data subjects in connection with the *collection* of personal data, **Section 23** could potentially be interpreted to

impose a separate obligation to obtain consent prior to any *use or disclosure* of such data. Such a requirement is at odds with the APEC Privacy Framework and is, as a practical matter, untenable in the modern cloud environment.

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. To fulfill this "Notice Principle," data controllers that are online service providers generally maintain privacy policies that consumers may review before any personal data is collected. 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.

If **Section 23** of the Bill requires data controllers to obtain separate consent before making any use or disclosure of personal data (in addition to the prior notification regarding the intended collection and use of such data), this would impose significant and unnecessary burdens on data controllers as well as data subjects. This would also be inconsistent with the carefully struck balance in the APEC Privacy Framework. To avoid this ambiguity, **Section 23** 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. Indeed, there are a wide range of mechanisms that enable users to control and consent to collection and use of their information, and some of the more robust opt-out mechanisms provide stronger protection for consumer privacy (with fewer disruptions for Internet users) than weaker opt-in mechanisms.

Recommendation

To ensure that **Section 23** is interpreted consistently with the APEC Privacy Framework, we urge MDES to amend the provision accordingly as follows:

> ***Section 23*** *Personal data controllers* ***may use, transfer, or disclose personal data only to fulfill the purposes of collection and other compatible or related purposes, as disclosed to the personal data subject pursuant to Section 19, except where:***
> ***1. the personal data owner has granted consent;***
> ***2. the use or disclosure is necessary to provide a service or product requested by the personal data owner;***
> ***3. the use or disclosure is necessary to fulfill a legal obligation; or***
> ***4. the personal data collected was collected in accordance with Section 20.***
> ~~*are prohibited from using or disclosing personal data without consent from personal data owner, unless it is permitted to be collected under the exemption for consent Section 20 or Section 22, or except in the case of Section 21 (3) as the case may be.*~~

International Transfers of Data (Sections 13, 24, and 31 – 34)

The Bill proposes to empower the PDPC to "*prescribe rules regarding international data transfers*" (**Sections 13(5), 24(5), and 31 through 34**).

While such rules may be helpful, it is critical that the measures, guideline, and rules are aligned, to the extent possible, with international 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 global data transfers.

The "accountability model," established under the Organisation for Economic Co-operation and Development (OECD) *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*[2] and subsequently endorsed and integrated in many legal systems and privacy

[2] At www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

principles, including the APEC Cross-Border Privacy Rules (CBPR)[3], provides an approach to cross-border data governance that effectively provides the individual with protections and fosters streamlined, robust data flows.

This accountability model requires that organizations that collect and use data are responsible for its protection and appropriate use 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.

Recommendation

Therefore, we strongly encourage MDES not to impose burdensome restrictions on global data transfers and to clarify in the Bill that data controllers will be free to transfer data internationally so long as they continue to protect the data or otherwise comply with international practices, such as a commitment to abide by the APEC CBPRs. To achieve this, we suggest amending **Section 24** as follows.

Section 24 *Sending or transfer of personal data abroad by a personal data controller shall be in accordance with the rules concerning protection of personal data prescribed by the Committee under section 13(5), except in the following cases:*

…

*(5) if it is a transfer **by or** to **a** ~~the~~ person granted a mark certifying personal data protection standards under section 32 or section 34;*

Section 32 should be amended to make clear that compliance with internationally accepted cross-border data protection regimes (e.g. relevant ISO standards; APEC CBPR; EU General Data Protection Regulation (GDPR)) will meet the PDPCs requirements under **Section 24.**

Data Breach Notification (Section 28)

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. For instance, the obligation to provide notice should not apply to instances in which the breached data is unusable, unreadable or indecipherable to an unauthorized third party through practices or methods (e.g., encryption) that are widely accepted as effective industry practices or industry standards. Finally, to ensure users receive meaningful notification 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.

Recommendation

Based on the foregoing, we recommend the following revisions to **Section 28(5)**:

Section 28

…

[3] See http://www.cbprs.org/

(5) To notify the personal data owner of a breach of personal data ***that creates a material risk of harm*** *without* ***undue*** *delay. In case of a breach* ~~***of personal data owner***~~ ***that creates a material risk of harm for*** ~~*in the number of*~~ *personal data subjects in the number exceeding that prescribed by the Committee, a personal data controller shall notify the Committee of the breach of personal data and remedial measures without* ***undue*** *delay.* ~~*Notification shall be conducted as prescribed in rules and procedures by the Committee.*~~ ***Notwithstanding the foregoing, a personal data controller shall not be required to provide any notification if 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.***

Powers of the PDPC (Sections 7-15) and Expert Committees (Sections 60-66)

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 eventual personal data protection law.

However, we remain concerned that several provisions may confer overly-broad powers to the PDPC, and the expert committees appointed under **Section 60** (Expert Committees). This includes a variety of open-ended powers for the PDPC "*to stipulate measures and guidelines for personal data protection*" (**Section 13(3)**), and "*to interpret, make enquiries into, and address issues*" arising out of the law (**Section 13(9)**).

We also note, for instance, that **Section 61(2)** grants the Expert Committee undefined authority to "*inspect*" the actions of a data controller and its employees or contractors regarding personal data that "*adversely affects*" data subjects. **Section 65** authorizes the Expert Committee to exercise its subpoena authority not only in the context of investigating a complaint, but also in furtherance of "*any other matters*" that it deems appropriate.

In addition to inspection powers, etc., **Section 63** grants the Expert Committee 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 are too severe and could be abused. **Section 75** grants the PDPC broad authority to determine fines and penalties but provides no guidance on what factors the PDPC should consider and how the PDPC should assess mitigating factors.

By offering little direction to the PDPC and the 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 PDPC and the Expert Committees may inadvertently 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 measure, guideline, or rules adopted by the PDPC under such powers are aligned, to the extent possible, with international 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 growth and development of cutting-edge technologies, while providing no benefit, and in many cases harming, the goal of protecting privacy.

Recommendations

At a minimum, and consistent with principles of checks and balances and due process, we recommend that safeguards be put in place to ensure the proper exercise of the authorities' powers, including under **Sections 13, 61, and 65**, and that legitimate privacy interests are not violated. Among other possible safeguards, such as including limited and strict criteria for how such powers can be exercised, the Bill should provide an avenue of appeal for data controllers and their

employees and contractors, against the decisions and orders of the PDPC and the Expert Committees.

We also recommend that MDES provide additional criteria under **Section 75** on how the PDPC assess fines and penalties and mitigating factors.

Civil Liability (Section 67)

Section 67 appears to impose strict liability with no accommodation for acting reasonably or mitigating efforts.

Recommendation

We suggest adding an additional factor that may protect a data controller against strict liability, as follows:

> ***Section 67***
> *…*
> ***(4) the data controller can demonstrate that it was acting reasonably or undertaking efforts to mitigate the damage to the personal data subject.***

Conclusion

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

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

Thank you for your time and consideration.

Yours sincerely,

Jared William Ragland
Senior Director, Policy, APAC
BSA | The Software Alliance

CC: The Secretary General, Office of the Council of State