Proposed Additional Amendments to the Personal Data Protection Bill

BSA Comments

August 4, 2017

On behalf of BSA | The Software Alliance (BSA),[1] we thank the Personal Information Protection Task Force of the Ministry of Digital Economy and Society (MDE) for providing us with the opportunity to review the most recent amendments to the Personal Information Protection Bill.

Priority Issues:

Having reviewed the current Personal Information Protection Bill (Close Case No. 1135/2558) which includes the most recent proposed amendments (July 2017 Amendments), BSA would like to highlight the following issues and recommendations.

A. Definition and Obligations of Personal Data Processor

We welcome the addition of a definition for "personal data processor" as it is meant to differentiate data controllers from data processors. However, we recommend clarifying the definition in line with global practice. We suggest the definition be modified to read:

> "Personal data processor" means a person, juristic person, public authority, agency, or any other body which processes personal data on behalf of the data controller.

Furthermore, we are concerned that the current Bill applies undue obligations on personal data processors. We recommend deleting references to personal data processor in Sections 25, 29/1, and 44.

Data controllers should have the primary obligation for ensuring compliance with applicable privacy laws (including laws pertaining to the transfer of data abroad), while data processors should be required only to comply with data controller instructions. Data processors process data at the instruction of data controllers and typically have very little insight into the data owner, the data controller's objectives for collecting data, or even the nature of the data provided by the data controller. Similarly, a data processor would typically not initiate a transfer of data abroad on its own, and would act in response to a request by the data controller to do

[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, CA Technologies, Cisco, CNC/Mastercam, DataStax, DocuSign, IBM, Intel, Microsoft, Oracle, salesforce.com, SAS Institute, Siemens PLM Software, Splunk, Symantec, The MathWorks, Trend Micro, Trimble Solutions Corporation, and Workday.

300 Beach Road
#25-08 The Concourse
Singapore 199555

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

Regional Representative Office
UEN: S97RF0005K

so. Additionally, as between data controllers and data processors, data controllers are best positioned to ensure that appropriate security measures are implemented to protect the data as they retain control over the data.

Placing the primary obligation for privacy law compliance on data controllers, instead of on data processors, and allowing the relationship between the data controller and the data processor to be governed by contracts or other legally binding mechanisms would result in a clear allocation of responsibility and liability. This allocation allows the data subject and the legal authorities to know who to turn to in case of a problem, and companies have clarity on roles and responsibilities.

B. Express or Implied Consent

We are encouraged that Section 17 recognizes both express (explicit) and implied consent, and believe its drafting can be further improved. In this regard, in circumstances where consent may be necessary, it is important that the legislation focuses on the ends and not the means by which consent is provided. As long as consent is given freely, specifically, and in an informed and unambiguous way, it should be accepted.

To this end, we recommend modifying paragraph 2 of Section 17 to read as follows:

> "In circumstances where consent may be necessary, any form of consent will be accepted as long as it is given freely, specifically, and in an informed and unambiguous way."

C. Legitimate Interest for the Collection, Use and Disclosure of Personal Data

The Bill has improved significantly over the last two years of deliberation and we thank the Government of Thailand for its willingness to listen to BSA and industry stakeholder input. We note, in particular, the exceptions in Section 21 to the consent requirement, and appreciate the Government's recognition that there are other ways (besides consent) to legitimize the collection, use, and disclosure of personal data.

We believe the Bill can be further improved by establishing a "legitimate interest" exception to the consent requirement. This would create the flexibility that businesses may need to ensure personal data is handled as necessary and in a timely fashion, even if the reason for the action is not specifically enumerated as an exception in the Act or regulation.

For example, if a financial institution is seeking to recover an outstanding debt and needs to collect, process, and/or disclose (e.g., to debt-collecting agencies) personal data as part of the debt-collection process, it may not be suitable to request the data owner's consent to do so but there is a legitimate interest that would justify the handling of the data.

We accordingly respectfully reiterate our recommendation for the explicit inclusion of a "legitimate interest" exception in the Bill.

D. Definition of Personal Data Owner

It is important to clearly define the term "data owner" as this definition impacts the definition of personal data, which is central to this Law.

We strongly recommend Section 5 be modified as follows:

> "Personal Data Owner" means a person identified or identifiable by the personal data.

The proposed language would prevent uncertainties that could arise from the term “source of data” that could create conflicting interpretations.

E. Detailed Recommendations

Below we provide a summary of preliminary BSA reactions to proposed amendments to the Bill on a Section-by-Section basis.

Yours Sincerely,

Jared W. Ragland, Ph.D.
Senior, Director, Policy - APAC

300 Beach Road
#25-08 The Concourse
Singapore 199555

P +65 6292 2072
F +65 6292 369
W bsa.org

Regional Representative Office
UEN: S97RF0005K

Detailed Recommendations:

Section	BSA Recommendation
Section 2: This Act shall come into force ***the day next to the date of publication*** in the *Government Gazette*	We recommend that the Act provide ***at least 2 years*** between the moment the Bill is enacted and the time when the obligations come into force. This will allow business operators time to adjust to new requirements and provide the Government of Thailand to work out implementing mechanisms, in coordination with interested stakeholders. We note that proposed Section 52/1 creates a 180-day transition period from the time of enactment of this Act to the time provisions related to the collection, use, or disclosure of personal data and related penalties come into force. We recommend that this be extended to at least 2 years.
Section 4(7): This Act shall not apply to: … ***(7) personal data that has been collected for a minimum of one hundred years***.	We recommend deleting this proposed additional exception to the application of this Act. It is unclear the intent or effect of this proposed addition.
Section 5: "personal data controller" means a person or juristic person with the power and duty to make decisions regarding the collection, use, or disclosure of personal data;	**BSA Note to Members:** In past submissions, we urged the government to explicitly exclude data processors from the definition of data controller. With the introduction of a definition of data controller in Section 5 (see below), ***are there in further concerns with the proposed definition of data controller?***
Section 5: "personal data owner" ***means a person who is a source of data and*** include***s***: (1) legal representatives acting on behalf of a minor; (2) guardians acting on behalf of an incompetent person; or (3) curators acting on behalf of a quasi-incompetent person.	We recommend specifying that the "personal data owner" is the person identified or identifiable by the personal data. This would avoid the need to include the unclear concept of "person who is a source of data" in the definition.
Section 5: *"Personal data processor" means a person or juristic person who is not hired by the personal data controller and who performs regarding personal data under this Act either in an automatic*	We recommend that the definition of personal data processor better follow international models. For example:

manner or other manners as instructed by the personal data controller.	"Personal data processor" means a person, juristic person, public authority, agency, or any other body which processes personal data on behalf of the personal data controller.
Section 5: "Office" means the Office of the ***Personal Data Protection Committee***;	**Note to Members:** The change from National Cybersecurity Committee to Personal Data Protection Committee seems unobjectionable. ***No comment.***
Section 5: "Secretary-general" means the secretary-general of the Office of the ***Personal Data Protection Committee***; and	**Note to Members:** The change from National Cybersecurity Committee to Personal Data Protection Committee seems unobjectionable. ***No comment.***
Section 17: ...When asking for consent, it shall be made in write or through electronic systems, ***except in case of:*** *(1)* ***expressed or implied consent;*** *(2)* ***encrypted personal data with mathematic process.***	Please see Section C in our cover note above. We support the proposed exception to requiring written request in cases where the subject has implied or expressed (explicit) consent. We propose clarifying Section 17 by stating that: "In circumstances where consent may be necessary, any form of consent will be accepted as long as it is given freely, specifically, and in an informed and unambiguous way." **Note to Members:** It seems unclear what may be intended by the exclusion of "encrypted data" as an exception to requiring written consent, but it seems unobjectionable. ***No comment.***
Section 17: … The request for consent shall not be deceptive or mislead the personal data controller in terms of the objectives or ***conditions of services***.	**Note to Members:** This proposed addition seems unobjectionable. ***No comment.***
Section 21: The personal data controller shall not collect personal data without the consent of the personal data owner, except in the following cases: … *(2)* ***(added) for the benefit of fraud and corruption prevention, and the personal data is kept confidential;***	We recommend that the Bill include an exception to "legitimate interest" of the data controller. While we appreciate the inclusion of another important enumerated exception to the requirement to obtain consent prior to, or at the time of, personal data collection, it is important to build in flexibility for data controllers to determine justifiable circumstances to collect data absent

	consent that may not be specified in the Act or ministerial regulations.
Section 24: The personal data controller is prohibited from using or disclosing personal data without consent from the personal data owner, except the following cases: … *(2)* ***It is the personal data as a result of the processing by government agencies for the purpose of public interests.*** (3) ***It is the personal data disclosed according to disclosure procedures in case of law enforcement for the personal data owners' interests, and such use or disclosure of the personal data shall be conducted appropriately in a fair manner to the personal data owner according to the rules under this Act.***	We recommend that the Bill include an exception to "legitimate interest" of the data controller. We note that if this concept were incorporated into Section 21 (see above), there would be no apparent need to explicitly include this important exception in Section 24. As above (see recommendation to Section 21), we appreciate the inclusion of additional exceptions to the requirement to obtain consent in order to use or disclose personal data. However, also as above, it is important to build in flexibility for data controllers to determine justifiable circumstances to use or disclose personal data absent consent that may not be specified in the Act or ministerial regulations.
Section 24: If a personal data controller uses and discloses personal data which is exempt from obtaining consent under the first paragraph, the personal data controller shall enter the use and disclosure in the record under Section 30, ***except for Section 24(2) it shall comply with rules as prescribed by the Committee***.	**Note to Members:** This provides an alternative reporting mechanism for the use or disclosure of personal information by government agencies (Section 24(2) activities). Does this affect member interests?
Section 25: Sending or transfer of personal data abroad by the personal data controller ***or the personal data processor*** shall be in accordance with the rules concerning protection of personal data prescribed by the Committee under Section 13(5), except…	We recommend deleting "personal data processor" from this provision. It should be up to the data controller to determine whether the requirements for transfer of personal information abroad are met – the processor must simply comply with the instructions of the data controller according to contractual arrangements with the data controller. A data processor typically would only respond to a request to transfer data abroad made by the data controller rather than initiating a transfer abroad on its own. The data processor will also not control which country is selected by the data controller for the transfer, it may not know the reasons for the transfer, or whether the transfer abroad request complies with the requirements of Section 25 as

	the data processor typically does not have a direct relationship with the data owner (contractual or otherwise). Furthermore, the proposal to limit the transfer of personal information abroad, for which consent or other requirements have been met to allow collection, use and disclosure, is counter-productive, unnecessary and should be removed from the Bill (see Sections 13(5), and 25). As described in more detail in previous comments, territorial restrictions on data storage undermine the promise of the modern information economy by unnecessarily increasing costs, undermining efficiency, and threatening data integrity. In a world where cross-border data flows are the rule rather than the exception, the legal framework must remain flexible. For more, see APEC Privacy Framework, Item 32: A personal information controller should be accountable for complying with measures that give effect to the Principles stated above. When personal information is to be transferred to another person or organization, **whether domestically or internationally,** the personal information controller should **obtain the consent** of the individual **or exercise due diligence and take reasonable steps to ensure that the recipient person or organization will protect the information consistently with these Principles.**
Section 29: The personal data controller shall have the following duties: ***(1) (added) to evaluate the implication on the privacy of personal data on a regular basis.***	We recommend deleting this additional proposed obligation. It is not clear and appears redundant with the other duties of the data controller enumerated in this Section.
Section 29/1: The personal data processor shall have the following duties: ***(1) to perform data processing according the instruction of the personal data controller only in compliance with the objective of the personal data controller;***	To the extent that including a section on the obligations of data processors is deemed valuable, only sub-item (1) is appropriate. The data processor should be required to process personal data according to the instructions and contractual arrangements of the data controller.

(2) to provide appropriate security measures to prevent loss, access, use, alteration, modification or disclosure of personal data without authority or in an unlawful manner, and to notify the personal data controller of any incident of data breach; ***(3) to prepare and store a record relating to data processing activities as prescribed by the Committee.***	The data controller should ensure that the data processor has the capability to secure and manage the personal data according to the data controller's requirements. Sub-item (2), therefore, is already addressed by sub-item (1), except for the data breach notification requirement. First, the processor should notify the controller according to the agreement between the controller and the processor. Second, it is unreasonable to require notification for ***any*** incident, as many incidents may present no risk to data owners, such as when the incident is unsuccessful, or the data is encrypted or otherwise rendered unusable. Sub-item (3) is also unnecessary. It is highly impractical and would be an undue economic burden on data processors to require them to keep records relating to their data processing activities, particularly where the data processing activities are wholly automated and/or in respect of big data processing requests. Additionally, data processors may be managing data from many different controllers in many different jurisdictions. It will be impractical for the data processors to follow distinct reporting and recordation requirements depending on where the data controller resides. Instead, as described above, the data processor should be obligated to manage the data according to the instructions and requirements of the data controller, as established in the agreement between the two entities.
Section 31: The Committee may set out a personal data protection practice code as guidelines for personal data controllers ***and the personal data processor*** to follow.	It is important that any code of practice or guideline is consistent with emerging international practices and does not propose unique requirements for controllers or processors in Thailand.
Section 36: The expert committees shall have the following power and duties: … (2) to inspect any action of the personal data controllers or their employees ***or the personal data processor of the personal data controller*** regarding	We recommend eliminating sub-section (2) in its entirety. The committee should not have arbitrary inspection powers over either data controllers or data processors, as the utilization of such powers could be severely, unnecessarily and unfairly disruptive to the businesses involved.

personal data that adversely affects the personal data owners;	
Section 37: A personal data owner has the right to file a complaint with the expert committee if a personal data controller or its employees ***or the personal data processor of the personal data controller*** violate or fail to comply with this Act, ministerial regulations, or notifications issued hereunder.	We recommend eliminating the specific reference to data processor in this Section, since the data controller should be the entity accountable to the data owner. This clear allocation of responsibility allows the data owner and the legal authorities to know who to turn to in case of a problem, and companies have clarity on roles and responsibilities.
Section 41: in the execution of this Act, the competent officer shall have the following powers and duties: (1) to send a notice summoning the personal data controller ***or the personal data processor*** or any person to provide information or submit any document or evidence regarding performance or violation of this Act; (2) to examine and gather facts, and notify the expert committee of the same, in the case that a personal data controller ***or the personal data processor*** or any person commits an offense or causes damage due to violation f or non-compliance with this Act, ministerial regulations, or notifications issue hereunder. When taking actions under (2), if it is necessary for the protection of the personal data controller or for the public interest, ***files a request with a court with jurisdiction for an order for the competent officer to enter the premises of the personal data controller or a person related to the offense hereunder*** ~~the competent officer may enter the premises of the personal data controller or a person related to the offense hereunder any time from sunrise to sunset, or during the working hours of the premises~~, in order to inspect and gather facts, and forfeit or seize documents and evidence, as well as other items related to the offense or suspected to have been used or	References to the personal data processor should be eliminated from Section 41, as the data controller is the entity with the relationship with the data subject and should be accountable for the handling of personal data, whether is it processed by a personal data processor or not. In paragraph 2, while we appreciate that the competent officer must now file a request with a court before entering premises to inspect and gather facts, forfeit or seize documents, etc., it is important that the conditions under which such requests are granted are narrowly tailored and it is critical that any information gathered during such activities, especially sensitive proprietary information and trade secrets, must be strictly protected from unauthorized disclosure.

possessed for use in the commission of the offense.	
Section 44: … ***Any personal data processor violates or does not comply with Section 29/1 shall be subject to a fine of not exceeding Baht 200,000.*** Any person who performs an action under the first ***and second paragraph*** to seek unlawful benefits for that person or other persons or to the detriment of other persons shall be subject to imprisonment for a term not exceeding six months or a fine not exceeding Baht 500,000 or both.	We recommend removing the new paragraph relating to personal data processors from Section 44. The data controller should be accountable for the handling of personal data. As described above in our comments on Section 29/1, we recommend that the data processor be obligated to comply with the instructions and requirements of the data controller according to the contractual arrangements between the two entities.
Section 46: Any person who fails to comply with the order of the expert committee or fails to provide facts under Section 40, or fails to accommodate the competent officers under the third paragraph of Section 41 shall be subject to a fine not exceeding Baht 100,000 ***and a fine of Baht 500 a day of the period of violation.***	***No Comment.***
Section 52/1: ***The provisions related to collection, use or disclosure of personal data and the penalties related thereto shall come into force one hundred eighty days after this Act comes into force.***	We recommend that the 180-day transition period between the entry into Force of this Act and the imposition of obligations be extended to at least two years. It is important to provide relevant stakeholders with the opportunity to understand the law and adjust their operations as necessary.
Section 53: Any person who is a personal data controller under this Act before the Act comes into force ***can use or disclose personal data in accordance with the objectives existing prior to the implementation of this Act, and in a manner that does not violate the principles of personal data protection as stated in this Act, and in manner that the personal data owner is provided with the choice to revoke consent, and*** shall comply with the provisions of this Act, ministerial regulations, or notifications issued under this Act, except Section 29(1) hereunder which shall be	***No Comment.***

complied with within 90 days form the effective date hereof.	

300 Beach Road
#25-08 The Concourse
Singapore 199555

P +65 6292 2072
F +65 6292 369
W bsa.org

Regional Representative Office
UEN: S97RF0005K