20 September 2018

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

(sent via email)

Dear Ms Pattanapanchai,

RE: Comments on the draft Personal Data Protection Bill (PDPB)

The Asia Internet Coalition (AIC) is an industry association comprising leading internet and technology companies. The AIC seeks to promote the understanding and resolution of Internet policy issues in the Asia Pacific region. Our members are AirBnB, Amazon, Apple, Expedia, Facebook, Google, Line, LinkedIN, Rakuten, Twitter and Yahoo (Oath).

We have learned from www.lawamendment.go.th that the latest version of the revised PDPB Personal Data Protection Bill ("**PDPB**") as of September 2018 is currently open for public hearing. We thank the Thai Government for seeking comments. Following our previous submission (dated 21st February 2018), we would like to provide these comments on the current draft.

Overview

We understand that the government wishes to align Thai data protection standards with the EU General Data Protection Regulation ("**GDPR**"). We feel this is premature and not the best approach, given that Thailand doesn't have an existing Data Protection Act in place, has not conducted a gap analysis and/or impact assessment on key areas, nor considered the costs of forcing compliance across all sectors. Importantly, compliance with the obligations under this version of the PDPB could not only hurt Thai SMEs and local businesses (especially smaller innovation firms that base their business on data analysis e.g. big data businesses), but also not meaningfully achieve its objective of protecting personal privacy. We encourage the revisions to the PDPB to protect the rights of data subjects, however urge that the bill not be drafted in an overbroad manner that could result in roadblocks to innovation and technological advancement.

We strongly feel that an industry consultation (and submissions) focused on a phased approach needs to take place in order to put a new data protection regime in place, one that works in the Thailand context, instead of applying a cut-paste approach with untested EU obligations. We fully appreciate the urgency of the situation due to recent data breaches, which is why our recommendation for a Thai-centric regime is relevant and warrants serious consideration.

We'd like to submit these specific comments

1. **Applicability of the PDPB should be limited to data controllers located within Thailand (Section 5)**

Section 5 of the PDPB:

"This Act shall apply to the collection, use, or disclosure of personal data by a personal data controller or a personal data processor, regardless of whether or not the collection, use, or disclose occurs in or outside the Kingdom.

In case the data controller and data processor are located outside the Kingdom, this Act shall be applicable to the collection, use, or disclosure of personal data of a data subject in the Kingdom by the activities performance of such data controller or data processor, for the following activities:

(1) The offer of goods or services to data subject in Thailand, whether there is a payment of the data subject or not;

(2) The behaviour monitoring of data subject occurs in the Kingdom."

The PDPB applies to the collection, use, or disclosure of personal data undertaken by data controllers and processors in Thailand, as well as those who offer goods or services to "personal data subjects" in Thailand or monitor personal data subjects' behavior in Thailand. This is a very broad application and seemingly does not require any affirmative action on behalf of a data controller or processor to operate in Thailand. Simply "monitoring" the data subject's "behavior" in Thailand is enough to come under the law. This strikes us as broader than the GDPR, which uses similar language but defines "monitoring" in a narrow manner in its recitals. The definition of "personal data subject" is also not clear, and introduces significant uncertainty in determining to whom this law applies.

The PDPB applies to processing of personal data by controllers or processors not present within Thailand if the processing involves offering goods or services to data subjects within the territory of Thailand or in connection with any activity which involves monitoring of the behavior of data subjects within the territory of Thailand. Again, this approach uses language from the GDPR, but has taken that language out of the context of the accompanying recital and EU case law, both of which limit the applicability of this concept to local-language and local-currency sales efforts that actually target the country. In the modern data economy, companies should be able to freely provide information without concern that in doing so, they might inadvertently collect information about individuals with whom they had no intention of establishing a relationship. The GDPR recognizes this by limiting this concept, and we recommend that the PDPB follow that lead.

If not altered, this approach may also violate basic international law principles. Privacy rules should not impact legal norms for determining jurisdiction by self-proclaiming their quasi-universal extraterritorial application.

A more sensitive, while at the same time protective approach, is to lessen the focus on the location of the individual (or the terminal), directing obligations instead to the entity engaged in the processing through an accountability-style program.

Accountable organizations, particularly those in the digital sector who benefit from the economies of scale enabled by the cloud, would be those with programs in place to protect the privacy of information regardless of the specific data flow. Such accountable organizations should stand ready to demonstrate and account to regulators not only what those protections are and how they are put into practice. This approach would lead to interoperability between regimes, as opposed to irresolvable conflicts of law.

The territorial applicability of the PDPB should be restricted to processing within the country. It must not be linked to non-territorial factors such as citizenship or origin of data – which would result in Thai law becoming applicable to virtually any processing which takes place outside the country. Such a model would lead to conflicting standards, and foreign controllers and processors having to comply with multiple standards. The pragmatic approach would be to have the PDPB apply only to controllers who are established within the territorial bounds of Thailand. Expanding the applicability of the PDPB beyond the borders of Thailand would result in unnecessary complexity.

Furthermore, it is unrealistic for any one regime to aspire to centralize the delivery of privacy protections for the entire world in just one regulator (and extremely costly). It would be unfeasible for one country's regulator to be charged with the task of overseeing the compliance of any organization around the world and to synthesize the various societal and cultural norms in enforcing a privacy law.. Modern and effective privacy regimes should instead seek to encourage the adoption and development of transnational best practices and standards through mechanisms of cooperation (such as co-regulatory frameworks or certifications or codes of conduct).

If the concern of the government relates to the safety of the personal data of Thai citizens when transferred abroad, the same may be ensured through a robust framework encouraging controller accountability.

To this end, we urge the Thai authorities to scope the PDPB so as to apply only to processing done by a data controller located within Thailand.

2. The PDPB is overly focused on consent. The PDPB should support other legal basis. (Sections 19 and 20)

Sections 19 and 20 of the PDPB:

Section 19, "*The Personal Data Controller shall not collect, use or disclose personal data if no consent of the personal data subject is, or has been, given in advance or at the time, unless permitted to do so by the provisions of this Act or any other law.*

Application for consent shall be made in writing, or via electronic means, unless it cannot be done by its nature.

In applying to obtain consent from the personal data subject, the Personal Data Controller must also indicate the purpose of collection, use or disclosure of Personal Data, and such application for consent must be clear and shall not be made to cause deception or misunderstanding to the personal data subject in respect to such purpose. The Committee may require the Personal Data Controller to apply for consent from the personal data subject in accordance with to the form and statements as prescribed by the Committee.

The personal data subject may withdraw his/her consent at any time, unless there is a limitation of right for the withdrawal of consent by law, or in the contract, which gives benefits to the personal data subject.

In the event that the withdrawal of consent will affect the personal data subject in any matter, the Personal Data Controller shall inform the personal data subject of such effects relating to the withdrawal of consent.

The application for the personal data subject's consent which is not in accordance with those prescribed in this Chapter shall have no binding effect to the personal data subject and shall not enable the Personal Data Controller to collect, use or disclose the Personal Data."

Section 20, "*In the event that the personal data subject is a minor who is not sui juris by marriage or has no capacity as a sui juris person under Section 27 of the Civil Commercial Code, the application for the consent from such person shall be made as follows:*

(1) In the event that the minor's giving of consent is not any act which the minor may be entitled to act alone as prescribed in Section 22, Section 23, or Section 24 of the Civil Commercial Code, such act must also be consented by the person exercising parental power, who has the power to act on behalf of the minor.

(2) In the event that the minor's age is not over ten years, the consent must be obtained from the person exercising parental power, who has the power to act on behalf of the minor.

In the event that the personal data subject is incompetent, the consent must be obtained from the custodian who has the power to act on behalf of the incompetent person.

In the event that the personal data subject is quasi-incompetent, the consent must be obtained from the curator who has the power to act on behalf of the quasi-incompetent person.

The provisions of paragraphs one, two and three shall apply mutatis mutandis to the withdrawal of consent of the personal data subject, the notice given to the personal data subject, the exercise of rights of the personal data subject, the complaint of the personal data subject and any other act under this Act in the event that the personal data subject is a minor, incompetent or quasi-incompetent."

The PDPB is overly focused on consent: requiring consent for use, collection, or disclosure of data; requiring that consent be "in writing" (which suggests that passive consent or consent by use of a service would not suffice); and the right to withdraw consent at any time (unless such right is restricted by law). We commend the fact that the PDPB provides multiple grounds for processing data, and that consent is just one of these grounds. However, it is worth emphasizing that repeated or multiple requests for consent through lengthy consent clauses, some of which may be unnecessary due to a lack of or reduced risk for harm, may lead to consent-fatigue and render consent meaningless. An approach that holds controllers accountable to act responsibly and adopt various privacy-preserving methods can help address consent fatigue.

The PDPB includes a specific consent requirement for minors, incompetent persons, and quasi-incompetent persons. This obligation could cause practical problems for online business as it is difficult to identify minors and obtain consent from their legal guardians. The parental consent requirement for minors would cause significant uncertainty and difficulty for businesses, especially as they roll out new products and technologies.

As such, it is important that the PDPB allow data controllers to obtain user consent in a flexible, context-specific manner - the nature, frequency, content, and form of consent required must vary depending on the type of information and context of processing. We discourage distinct consent requirements for different types of persons. This would result in significant uncertainty and difficulty for businesses.

Consent is not a one-size-fits-all solution to privacy concerns, and different types of data processing need to be governed by different standards. Implied consent is widely used across the world as a standard for lawful data processing when the actions of a person clearly indicate her consent to having her data processed regardless of whether she formally consented. As such, we urge the Thai authorities to also recognize implied consent as a valid ground for the lawful processing of data.

3. Transition Period should be not less than two years and the PDPB should not be applicable to data processed prior to the PDPB coming into force (Section 2 and Section 94)

Section 2 of the PDPB:

"*This Act shall come into effect after the lapse of a period of* ***one hundred and eighty days*** *from the date of its publication in the Government Gazette, except for the provisions of Chapter 1, Chapter 4 and Section 89, Section 90, Section 91, Section 92, and Section 93, which shall come into effect on the date following the date of the publication in the Government Gazette.*"

The transition period is too brief to allow industry, especially small and medium-sized businesses, to be fully compliant. The PDPB must provide a fair chance for enterprises and businesses to comply. It must only apply prospectively; in other words, the law should not be applicable for any data processed prior to the law coming into force.

In addition, it should not be overly burdensome by requiring companies to adhere to unworkable consent requirements in relation to data already collected. This would result in drastic compliance overhead for companies and hinder innovation. A workable alternative would be to provide companies the flexibility to transition to the new regime by giving them enough time to adapt to the new requirements, which should be no less than 2 years.

4. **Data sets which are anonymized, encrypted, pseudonymized, or already publicly available through lawful means should be exempt from the definition of personal data (Section 6)**

   Section 6 of the PDPB:

   "*In this Act,*

   "Personal Data" means any data pertaining to a person, which enables the identification of such person, whether directly or indirectly, but not including data of the deceased specifically."

   The definition of "Personal data" and "indirect data controller" needs to be clearly defined. The definition of personal data will define the scope of the PDPB. Emphasizing that privacy laws in general, and the definition of personal data specifically, must be scoped in a balanced manner to take into consideration the protection of the rights of data owners, the benefits that can be gained from responsible and innovative uses of data, and the benefits of freely sharing information publicly available through lawful means, it is important for the MDES to recognize that whether data is personal is a *contextual evaluation* – depending on whether data has the tendency to identify an individual or not. Data which does not have this capacity is not "personal data" and may be freely used.

   For instance, data sets which are anonymized, encrypted, or pseudonymized must be exempt from the definition of 'personal data' and therefore explicitly out of scope of the framework. This approach, which is recognized in data protection laws around the world, would also incentivize companies to adopt privacy-enhancing techniques in relation to the processing of data.

   Further, to encourage the free flow of information, the definition of "personal data" should exclude information that is already publicly through lawful means.

5. **The Personal Data Protection Committee ("PDPC") should include representatives from business sector (Section 8 (3))**

   Section 8(3) of the PDPB:

   "*There shall be a committee called the "Personal Data Protection Committee", consisting of:…*

(3) five ex-officio members consisting of the Secretary-General of the Council of State; the Attorney General, the Secretary-General of the Consumer Protection Board, the Director-General of the Rights and Liberties Protection Department, and the Executive Director of Electronic Transactions Development Agency; …"

To further ensure that the PDPC is able to take into consideration the various interests of all major stakeholders, including those of the business sector, it is suggested that an official from the Ministry of Commerce, Department of Business Development, or the Department of International Trade Promotion be included in the PDPC's membership.

As the PDPC will now consist only of government officials and those appointed by government, we suggest that the PDPC include members from several relevant business sectors as well.

We further recommend the formation of a consultative or advisory committee (such as that provided in the data protection laws of Singapore and Mexico, among others), comprised of academics, industry, and civil society, which would meet 3-4 times a year and advise the PDPC on important matters. Consultative and advisory committees have proved quite useful in providing additional expertise and timely feedback to PDPCs and other regulatory agencies.

6. The notification requirements should be flexible. The timeframe for notification requirements could be too tight. (Section 23)

Section 23 of the PDPB:

"... *In the case where there is a cause preventing the Personal Data Controller from notifying the personal data subject within the time period required stipulated under paragraph one, the Personal Data Controller shall inform the personal data subject of the details under paragraph one without delay but not later than* ***thirty days*** *from the date of collection and before the first disclosure of Personal Data.*"

The PDPA should encourage flexibility for controllers to provide dynamic notices in a format and with the content appropriate to the concerned data collection activity, and to the intended audience.

The 30-day period, which runs from the initial collection date, could be too tight a deadline. It is not practical and should be removed and replaced with more flexible terms that account for the differing natures of various businesses.

7. **The Personal Data Controller shall not collect Personal Data without the consent of the Personal Data Owner, unless..: (Section 24 (6))**

Section 24 of the PDPB:

"The Personal Data Controller shall not collect Personal Data without the consent of the Personal Data Owner, unless:

(6) it is necessary for lawful interests of the Personal Data Controller or other persons or legal entities, other than the Personal Data Controller, unless such interests are less important than the fundamental rights of the Personal Data Owner to their Personal Data;

The scope of legitimate collection of data is not clear. "Legitimate Interests" could be a useful balancing tool to consider the reasonable data processing basis when obtaining consent is unpractical. It is essential that data protection law stays future-proof and provides organisations with the ability to process data responsibly in the context of evolving technology and in a way that does not create risks to individuals. Implementing "legitimate interests" style provisions and showing examples through the guidelines could provide a predictability as well as flexibility in data processing.

8. **Personal data collected from other sources should only be subjected to a notification requirement (Section 25)**

Section 25 of the PDPB:

"*The Personal Data Controller shall not collect Personal Data from any other source apart from the personal data subject directly, except where:*

(1) the Personal Data Controller has informed the personal data subject of the collection of Personal Data from another source prior to, or during, such collection by obtaining the consent of the personal data subject; ..."

In the earlier draft, if the personal data is obtained from other source which is not from the data subject directly, only the notification of such other-source collection is required. We proposed removing the consent requirement. This is also beyond the requirements under the section 14 of the GDPR, which requires the controller to provide certain information to the data subject.

9. **The PDPB must not recognize a separate category of sensitive data. (Section 26)**

Section 26 of the PDPB:

"*Any collection of Personal Data pertaining to ethnicity, race, political opinions, doctrinal, religious or philosophical beliefs, sexual behaviour, criminal records, health records, labour union information, genetic data, biological data or of any data which may affect the subject in the same manner, as prescribed by the Committee, is prohibited, without the express consent of the data subject, except where: …*"

A separate category of sensitive data does not necessarily provide any tangible benefits to individual privacy, but it does add to the complexity and cost of compliance to businesses. In practice, the boundary between sensitive and non-sensitive personal data is porous and blurred. Instead, the law must encourage data controllers to adopt transparent collection, and risk-based security practices. Controllers should instead be required to determine the appropriate level of protection for particular types of data by use of a broader risk-based framework and security practices.

If Thailand strongly believes that a separate category for sensitive personal data is necessary, it should be a closed list. The PDPC or any other government agency should not have the authority to later create any new categories of sensitive data or any additional types of "*data which may affect the subject in the same manner, as prescribed by the Committee*" which shall not be collected without consent from a personal data subject. What constitutes sensitive data should not be open and subject to interpretation from a regulator, as the risk arises that an expansive interpretation will lead to treating an excessive amount of data types as sensitive, which will stall technological innovation and development.

The current definition list as drafted is also extremely broad and open-ended. By including a class of opinions and philosophical beliefs, it is out of step with international norms. A broad definition that encompasses political opinions and philosophical/religious beliefs could present significant obstacles for a platform like Facebook, through which users routinely engage with politicians and other users on legislation, events, and views of the day.

The law should also acknowledge that the processing of so-called sensitive data can have incredibly beneficial results for individuals and for society. These benefits include the ability to gain insights into disease control and other general health concerns. To ensure that there are opportunities for these beneficial uses of sensitive data to flourish, instead of a blanket prohibition on the processing of sensitive data without consent, there should be thoughtful mechanisms or legal bases to process sensitive data (beyond consent) and exceptions such as when the *"information has deliberately been made public by the data subject,"* such as that contemplated by South African laws.

10. The PDPB should not impose material restrictions on cross-border transfers of personal information (Sections 28 and 29)

Sections 28 and 29 of the PDPB:

Section 28, "*In the event that the Personal Data Controller sends or transmits the Personal Data overseas, the relevant destination country or international organization that receives such personal data shall have sufficient personal data protection standards, and such act shall be performed in accordance with the rules for the protection of Personal Data as prescribed by the Committee in Section 16(5), except in the following cases:....*"

Section 29, "*In the event that the Personal Data Controller or the Personal Data Processor who is in the Kingdom has prescribed the personal data protection policy in order to send or transfer the Personal Data to the Personal Data Controller or the Personal Data Processor who is in foreign country and in the same affiliated undertaking or affiliated business in order to jointly operate the undertaking or business, if such personal data protection policy has*

been reviewed and certified by the Office, such sending or transfer of Personal Data to foreign country, which is in accordance with such reviewed and certified personal data protection policy, can be done and shall be exempted from compliance with Section 28.

The personal data protection policy, the nature of the same affiliated undertaking or affiliated business in order to jointly operate the undertaking or business, and the rules and methods for the review and certification in paragraph one shall be as prescribed and announced by the Committee.

In the event that there is no decision of the Committee in Section 28 or no personal data protection policy in paragraph one, the Personal Data Controller or the Personal Data Processor may send or transfer the Personal Data to foreign country with the exemption from compliance with Section 28 if the Personal Data Controller or the Personal Data Processor provides the appropriate protection measures which can enforce the personal data subject's rights, including the effective legal remedy measures according to the rules and methods as prescribed and announced by the Committee."

Cross border data flow brings many benefits to an economy, necessitating that the regulation on transborder data flow should be flexible. Thailand is a member for APEC and ASEAN and that APEC CBPR has "sufficient protection" standards in section 28 which should be satisfied when the parties rely on APEC CBPR and other internationally recognized frameworks. The Commission's review on intra-group transfer in section 29 should also be satisfied when the corporate group participate in the CBPR System.

There is no clear exemption for intra-group transfers, which could be quite problematic. It may be that such requests would need to go through the PDPC, but there are no clear guidelines and procedures provided in the PDPB. This seems out of step with the best current international practices. If the controller of personal data continues to be responsible and accountable for that personal data, a blanket restriction on transfer based on the geographic borders of a country is unnecessary.

Major economies with privacy laws, such as the United States and Canada, do ***not*** impose material restrictions on cross-border transfers of personal information. These are ***viable, preferred models,*** particularly where organizations are required to remain "accountable" for the continued protection of transferred data at the level it is protected inside the jurisdiction.

We suggest that the law should not require that the PDPC be notified of a cross-border transfer, or that proposed categories of cross-border transfers be registered with or approved by the PDPC.

While, historically, some laws contain such requirements, the trend is moving away from this approach, as it is cumbersome and does not enhance privacy compliance. Many countries now realize that these requirements do not serve to increase the actual protection of individuals in practice.

Also, given the prevalence and volume of global data flows, technology, and processes, the enormous administrative burden and costs these cross-border obligations impose both on organizations (especially SMEs) and on data protection authorities are not justifiable.

Data transfers and meaningful protection from privacy harms are not mutually exclusive or antagonistic. Cross-border data flows are not only a factor of increasing connectivity and globalization, but an essential component of their emergence. Without cross-border flows, users would only be restricted to the few services provided by their local service providers, despite the fact that more affordable or better services may exist from providers abroad. As such, cross-border flows have not only enhanced consumer choice and interest, but cross-border investments and information flows as well.

Any interference with these flows is likely to result in economic isolation of a region or state, and harm local consumer and commercial interests. For these reasons, we would encourage the Thai authorities to safeguard and facilitate the free flow of data.

Measures that unduly restrict the free flow of data through onerous and complex data transfer requirements decrease consumer choice and raise compliance costs, as users and SMEs are forced to abandon cheaper cross-border alternatives in favor of local solutions.

Hence, any future rules regarding the protection of personal data sent or transferred abroad must provide a balanced approach which respects the role of cross-border data flows while ensuring personal data remains protected.

It is essential that countries legislating in this area take account of the existing transfer mechanisms, laws, and best practices that have evolved so that these mechanisms can provide for seamless but still accountable global data flows that work for all kinds of cross-border data transfers, including transfers to or between controllers or processors and between affiliated companies or with third parties.

Privacy laws that contain cross-border data transfer restrictions should also include a comprehensive set of available cross-border transfer mechanisms to enable accountable global data flows despite any transfer restrictions.

These mechanisms include:

a. **Cross-Border Rules**

   The law should allow for enforceable corporate cross-border privacy rules modeled on the APEC Cross-Border Privacy Rules (CBPR).

   An effort was started between APEC and the EU's WP29 in 2012 to streamline the CBPR/BCR certification and approval processes when companies seek "dual certification" under both systems. Now, with the enactment of the GDPR, this EU/APEC collaboration also includes the EU Commission and has broadened its exploration of interoperability with the CBPR to include not only EU BCR, but also, and possibly primarily, GDPR certifications and, down the road perhaps, GDPR codes of conduct. This effort to create interoperability could serve as a model for similar efforts between other regions and transfer mechanisms.

b. **Codes of Conduct, Certifications, Privacy Marks, and Seals and Standards**

The law should allow for the use of certified codes of conduct, certifications, privacy marks, and seals and standards as cross-border transfer mechanisms.

All of these mechanisms also impose substantive privacy requirements on organizations and are externally certified and enforceable. Any privacy law with data transfer restrictions should allow for the use of such mechanisms to enable accountable cross-border data transfers, in the same way BCR and CBPR currently enable them and as GDPR certifications and codes of conduct will in the future.

c. **Self-Certification Arrangements**

The law should allow the possibility of cross-border transfers based on negotiated arrangements, including arrangements that rely on "self-certification" to a given privacy standard, coupled with enforcement (such as the EU-US Privacy Shield).

i. Privacy laws that have cross-border transfer restrictions should also not preclude the option to develop bi- or multilateral frameworks and self-certification arrangements.
ii. The EU/US Privacy Shield Framework is one example. Under that framework, the US and EU negotiated a set of privacy principles for cross-border data transfers from the EU to the US to which US companies may "self-certify." Once a company self-certifies to the Privacy Shield, compliance with these privacy principles becomes binding and enforceable.
iii. Developing variations of this bilateral accountability model should be an option under any privacy law that contains data transfer restrictions. It would provide relevant authorities the flexibility to create data transfer frameworks that are particularly suited for SMEs and for contexts in which third-party certification may be impracticable and unnecessary.

Summary on thoughts on cross border data transfers

iv. To conclude, if a legislature or regulator is to establish cross-border data transfer restrictions, it should also establish appropriate and effective exemptions so that necessary cross-border data transfers can continue while protecting the data and privacy of individuals.
v. There are numerous available mechanisms and legal bases to facilitate such accountable transfers; which one of them is appropriate for a given transfer scenario will depend on the context.
vi. Industry should be given flexibility in choosing which mechanism or legal basis works best under the circumstances and within the confines of appropriate accountability mechanisms and enforceability by the responsible authorities.
vii. Unnecessary government involvement should be avoided, as this imposes administrative and cost burdens on government and industry alike.
viii. Finally, accountability-based mechanisms that ensure effective and real protection for individuals, such as BCR, CBPR and similar mechanisms,

should be encouraged and incentivized.

11. Additional data protection obligations on data controllers and/or data processors should be reconsidered.

The PDPB imposes additional obligations, including.

a. Right to data portability (section 31 (1))
b. Right to object (section 32)
c. Records of processing activities (section 38)
d. Data Protection Officer (section 40)

These obligations have been adopted by the GDPR. However, these obligations cause problems in practice and could lead to lessen incentive for business sectors to conduct business in Thailand. Thus, these obligations should be reconsidered and open for discretion by the data controller to deny exercising such rights in certain circumstances. For example, the Personal Data Owner should not be able to exercise rights under the PDPB if doing so would: (1) undermine privacy interests of other Personal Data Owners or data security interests of data controllers or processors; (2) enable fraud or other unlawful activity; (3) interfere with law enforcement or judicial proceedings; (4) be unduly burdensome or excessive; (5) reveal proprietary assets or business insights; or (6) require the collection or processing of additional personal data about the Personal Data Owner.

12. Data processor obligations (Section 39)

Section 39 of the PDPB:

"*… The Personal 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 such collection, use or disclosure of the Personal Data.*"

This is confusing and conflicts with the definition of data processor, which clearly states that the data processor shall not be the data controller. Furthermore, failure to comply with data processor obligations could trigger penalties under section 84 and, as the data processor would then be considered a data controller, the data processor could also be subject to liabilities as a data controller.

13. Appointment of a representative in Thailand is burdensome and beyond the jurisdiction of the Thai authorities (section 36 (5))

Section 36 of the PDPB:

"*The Personal Data Controller shall have the following duties:*

… (5) in the event of being the Personal Data Controller according to Section 5 paragraph two, to make an appointment in writing of the Personal Data Controller's representative who must be in the Kingdom and be authorized to act on behalf of the Personal Data Controller without any limitation of liability with respect to the collection, use or disclosure of the Personal Data according to the objective of the Personal Data Controller."

The liabilities of the "legal binding representative" should allow to be limited to reflect the activities and services of such entity (not unlimited as defined in the bill).

There is a conflict between this provision and other Thai law. It is unclear how an offshore entity would employ such a representative without breaching Thai foreign investment and licensing laws. Also, a requirement that an offshore entity must appoint a representative in Thailand with full authority to act on behalf of a personal data controller is beyond even the standards of the GDPR. The PDPB should be applicable only to data controllers and data processors located in Thailand.

14. Scope of authority's power against offshore entities should be removed (Sections 73 and 74)

Sections 73 and 74 of the PDPB:

Section 73, "*The Expert Committee shall have the power to order any person to submit documents or information in connection with the subject matter of a complaint or any other matter related to the protection of the Personal Data hereunder. The Expert Committee shall also have the power to request any person to make a statement of facts.*"

Section 74, "*In order to observe the provisions hereunder, the Competent Officer shall have the following authorities and functions:…*"

Requests for personal data should be accompanied by a court order.

As mentioned earlier, the PDPB should be applicable only to data controllers located in Thailand. The power of the authorities should be limited accordingly.

15. Additional punitive damages, criminal penalties, and increased fines and imprisonment could bar data analysis business in Thailand (Sections 76, 77 - 79, and 80 - 88)

The PDPB introduces additional punitive damages and criminal penalties, along with increased fines and imprisonment which, when considered in connection with class action laws, could entirely bar data analysis businesses in Thailand.

Criminal and Administrative penalties should only be ruled by court (like civil penalties). Imprisonment penalties should be removed. Such penalties could be abused to bar competition. They also go beyond the scope of the GDPR.

A regulatory environment whose primary tool for enforcement is the imposition of penalties, fines, and other sanctions is adversarial, lacks transparency, and hinders collaboration between regulators and controllers. Adopting such an approach would lead to controllers seeking to avoid proactive disclosures, and choosing to keep breaches and other incidents secret, for fear of punishment. Such an approach does not favor any of the various stakeholders under the PDPB.

An ideal regulatory model demonstrates the key principles of fairness, proportionality, accountability, constructive engagement, and mutual trust. Hence, the approach to enforcement under the PDPC must be characterized by a preference to incentivize maximum voluntary compliance, while reserving penalties and other punitive sanctions as a last resort.

The enforcement strategy of the PDPC must be guided by the objective of maximizing compliance through dialogue, collaboration, and transparency between the PDPC and data controllers. The focus must be on penalizing only those clear violations which result in tangible, measurable harm due to the misdeeds of malicious actors.

As such, penalties should be levied only in cases of deliberate, repeated, or egregious violations, after the PDPC has heard and warned the controller in question. The regulator must look to impose proportionate penalties only when necessary and after warnings and other cooperative measures have proved unsuccessful. In addition, any compensation shall be based on specific, quantifiable monetary losses.

Moreover, the drafters of the PDPB should provide incentives for controllers who develop and implement accountability programs, whether internal or industry-wide (such as self or co-regulation mechanisms, seals, and certifications). These incentives include allowing for a presumption of compliance, resulting in a statutory reduction of fines and possible exemptions from penalties.

Lastly, we once again convey our appreciation to the Thai Government for maintaining a requirement for the Royal Decree to undergo public consultation. We believe that close dialogue with the industry, allowing industry appropriate time to provide comments, and taking into consideration its views, will improve the legislative outcomes. As always, we are available to meet in person to discuss any of the above further.

Yours sincerely,

Mr Jeff Paine
Managing Director
Asia Internet Coalition
www.aicasia.org
jeff@aicasia.org