21st February 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

Dear Ms Ajarin Pattanapanchai

The Asia Internet Coalition ("AIC") is an industry association made up of 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 Apple, Expedia, Facebook, Google, Line, LinkedIN, PayPal, Rakuten, Twitter and Yahoo (Oath).

The Asia Internet Coalition (AIC) welcomes the opportunity to respond to the draft Personal Data Protection Act. We recognize that the deadline to submit comments has passed, however we do hope that even at this stage our comments are useful to you.

Comments on the Thai Consultations on a draft Personal Data Protection Act

The Personal Data Protection Act must be created in a balanced manner which accounts for diverse social, economic, and innovation-oriented objectives. It should protect the rights of data owners, but also not be drafted in an overbroad manner that could result in roadblocks to innovation and technological advancement. In the same way we place utmost importance on the fact that rights of data owners must be respected and their data treated with care, various stakeholders must similarly acknowledge that there is much to be gained from nurturing the growth of data-driven services and technologies.

I Definition of Personal Data

Section 5 of the draft Personal Data Protection Act (PDPA):

"Personal data" means data regarding a person who can be identified, whether directly or indirectly from that data, excluding the identification of only their name, position, workplace or business address, and data of a deceased person in particular;

The definition of personal data will define the scope of the PDPA. Emphasizing that privacy laws in general, and the definition of personal data specifically, must be scoped in a balanced manner to take into consideration both the protection of the rights of data owners and the benefits that can be gained from responsible and innovative uses of data, 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 must 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. Such an approach would also incentivize companies to adopt privacy-enhancing techniques in relation to the processing of data.

It is noteworthy to mention that Recital 26 of the GDPR states that:

" ... The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable.

This Regulation does not therefore concern the processing of such anonymous information, including for statistical or research purposes."

Further, as an oft-quoted Report mentions:

> "*…personal information can be contextual—the same piece of information can be personal in the hands of a certain data controller and functionally anonymous in the hands of another data controller—e.g., possession of a license plate number in the hands of an insurance company can be considered as personal information but the same plate number in the tape of a security camera in a petrol station will not be personal information, as the station has to take considerable efforts for determining the identity of the person. The definition of personal information therefore should be at high level (not prescriptive) giving space for various contexts*."[1]

[1] Report of the Group of Experts on Privacy, headed by Fmr. Chief Justice Ajit Prakash Shah, High Court of Delhi, 16 October 2012

II The Personal Data Protection Committee (PDPC)

Section 7 of the draft PDPA:

There shall be a Personal Data Protection Committee consisting of:

(1) the chairperson appointed by the Cabinet, who shall possess evident knowledge, expertise, and experience in personal data protection, consumer protection, , information and communication technology, social sciences, law, health, or in other fields relevant and beneficial to personal data protection;

(2) the Permanent Secretary of Ministry of Digital Economy and Society as the vice chairperson;

(3) three ex officio members, namely the Permanent Secretary of the Prime Minister's Office, the Secretary General of the Consumer Protection Board, the Director General of the Rights and Liberties Protection Department;

(4) five qualified members appointed by the Cabinet, who shall possess evident knowledge, expertise, and experience in the fields of personal data protection, consumer protection, , information and communication technology, social sciences, law, health, or other fields relevant and beneficial to personal data protection.

The Secretary General shall be the member and secretary and shall appoint no more than two officers of the Office of Personal Data Protection Committee as assistant secretaries.

The rules and procedures for the selection of person to be appointed as the chairperson and qualified members, including the selection of qualified members to replace those who retire before the expiration of their term, pursuant to Section 10, shall be in accordance with the regulations prescribed by the Minister.

We note that this section strives to have diversity within the PDPC, and assigns the Permanent Secretary of the MDES as vice-chairperson. However, 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 PDPC's membership.

We further recommend the formation of a consultative or advisory committee (such as that provided in the data protection law of Singapore and Mexico, among others) that is composed of academics, industry, and civil society, that 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 DPAs and other regulatory agencies.

III Cross-border Flows of Data

Section 13 (5) of the draft PDPA:

> *The Committee shall have the following powers and duties: … (5) to prescribe the rules regarding the protection of personal data sent or transferred abroad;*

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 though more affordable or better services may exist from providers abroad. As such, cross-border flows have not only enhanced consumer choice and interest, but also cross-border investments and information flows.

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 MDES and the Thai authorities to safeguard and facilitate the free flow of data if and when they decide to prescribe rules regarding the protection of personal data transferred abroad.

Measures that unduly restrict free flows 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.

Controllers in Thailand may be made responsible for ensuring that foreign recipients of personal data from Thailand adopt adequate protections in relation to the data received. Specifically, controllers must ensure that foreign recipients of data maintain at least as strong data protection measures as required under Thai law - measures that shall not overly rely on adequacy determinations, but rather look to other more modern and efficient mechanisms such as model contractual clauses or binding corporate rules and recognition of modern accountability

frameworks such as the APEC CBPRs, or other mechanisms such as certifications or codes of conduct.

The adequacy-based model of regulating data transfers implemented in Europe is highly complex, extremely political, and of questionable efficacy. There is no evidence that it is superior in protecting data transfers than other models (e.g. controller accountability), nor has it resulted in an advantage to home-grown businesses (after 25 years of data transfer regulations, EU cloud and digital services sectors significantly lag the US). What's more, the legal framework for data transfers is now beginning to unravel, with a series of legal challenges to the whole model, threatening its viability (i.e. Schrems I and II before the CJEU). It is also worth highlighting that after said challenges, no country has been granted with EU adequacy status.

Rather, a first-generation data protection law, to be effective and successful, needs to be simple, easy to understand and to implement.

IV The Powers and Duties of the PDPC

Section 13 of the draft Act:

The Committee shall have the following powers and duties:

(1) to prepare strategic plans for the promotion and protection of personal data, which are consistent with the relevant national policies and plans, and to propose strategic plans and measures to resolve problems and obstacles regarding compliance with such national policies and plans;
(2) to stipulate measures or guidelines for personal data protection, in order to ensure that it is executed in accordance with this Act;
(3) to issue notifications or rules to ensure that actions will be carried out in compliance with this Act;
… … …
(12) to perform any other acts prescribed by this Act or other laws as power and duties of the Committee.

The PDPC must work in tandem with sectoral regulators, and industry participants (such as controllers and processors) to formulate plans, guidelines, and rules. In addition, the PDPC should also recognize the role of self and co-regulation by encouraging industry bodies to develop regulatory models and certifications which may then be certified or approved by the government. In addition, all rule and policy formulation must be carried out on the basis of public consultations with all stakeholders including the business sector, civil society, and the public.

In order to broaden the scope of powers of the PDPC, and to encourage it to adopt the key principles of constructive engagement and mutual trust, we suggest that a duty to educate, advise, collaborate with, and guide its regulated sectors be added to Section 13 of the Act.

It is also recommended that the powers to represent the Thai government internationally on matters relating to data protection, and to manage technical cooperation and exchange in the area of data protection with other organizations, including foreign data protection authorities and international or inter-governmental organizations, be added to this Section, to clarify that the PDPC shall have the primary authority to liaise with foreign entities on data protection matters.

Another duty worth adding is the duty to help advance the digital development agenda of Thailand, in line with the mission and vision of government agencies such as the MDES. It would benefit all stakeholders if the duties of the PDPC are aligned with the Thailand government's goal to promote and support business, industry development, digital technology and innovation, and to boost economic and social development. This is comparable with the Singapore government's approach of integrating its Personal Data Protection Commission (PDPC) with its Infocomm Media Development Authority (IMDA), which has the following as its Missions: *Develop competitive Infocomm and Media sector and talent; Power innovation and foster a spirit of enterprise; Build trusted environment for businesses and consumers; and Connect people and bond communities.*

V Consent

Section 16 of the draft PDPA:

> *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;*
>
> *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;*

A personal data owner may at any time revoke their consent, unless there is any restriction on revoking consent under the law or agreement for the interest of personal data owner.

If revocation of consent affects a personal data owner in any way, a personal data controller shall inform the personal data owner of such effects from revoking consent.

We commend the fact that the draft Act provides for multiple grounds for processing, 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 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.

As such, it is important for the PDPA to 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.

VI Notice

Section 19 of the draft PDPA:

In collecting personal data, a personal data controller shall notify a personal data owner before or at the time of collecting personal data of the following details:

(1) the objective of collection;
(2) personal data to be collected;
(3) categories of persons or agencies to which the collected personal data may be disclosed;
(4) the information regarding a personal data controller, place of contact, and contact method; and
(5) rights of a personal data owner under sections 25, 26, and 27.

In the event that the details under the first paragraph cannot be notified to a personal data owner within the period specified in the first paragraph, a personal data controller shall notify the personal data owner of the details under the first paragraph without delay.

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. This audience may be the individual whose data is being processed, but it may equally be for a regulator such as the PDPC. The manner, type, and content of notice will therefore need to vary - individuals will require concise and simple information to make quick, non-expert assessments about data collection and processing. Whereas, the information that may be appropriate for purposes of ensuring company accountability, and aiding data protection authority evaluations and assessments, would be considerably more complex.

Also, the requirement to provide notice must be qualified to read: *"In the event that the details under the first paragraph cannot be notified to a personal data owner within the period specified in the first paragraph, a personal data controller shall use reasonable efforts to notify the personal data owner of the details under the first paragraph without delay."* This qualification is necessary to protect against circumstances where contacting data owners requires disproportionate effort on the part of the controller.

VII Grounds for the Collection of Personal Data

Section 20 of the draft PDPA:

> *A personal data controller shall not collect personal data without the consent of personal data owner, except in the following cases:*
>
> *(1) for the benefit of study or statistics for the public interest, and the personal data is kept confidential;*
> *(2) for the purpose of preventing or abating harm to life, the body, or health of a person;*
> *(3) if the data is available in the public domain with the direct or implied consent of personal data owner;*
> *(4) it is necessary for a personal data controller to perform duties for the public interest or a personal data controller to exercise the power given by the government, except where such interests are overridden by the interests or fundamental rights and freedoms of personal data owner;*
> *(5) it is necessary for the legitimate interests of personal data controller or third party, except where such interests are overridden by the interests or fundamental rights and freedoms of personal data owner, especially in case the personal data owner is a child; but this shall not be enforceable in case where government agencies process personal data in their duty;*
> *(6) for compliance with the laws*
> *(7) for other circumstances as prescribed in ministerial regulations.*

The emergence of the data-driven economy means that there are several new and innovative forms of data processing activities that have become commonplace. Therefore, it is important to recognize additional grounds on the basis of which processing of personal data may take place. These include:

- contractual necessity, such as when the processing of personal data is related to the fulfillment of a contract with the data owner, or is necessary in order to take steps at his or her request prior to the entry into a contract;
- processing that is necessary to provide a service, that is, in situations such as where the data owner is a client or uses a service of the controller;
- situations wherein the data owner is deemed to have given consent, such as a scenario where the data owner, without actually giving consent, voluntarily provides his or her personal data to the controller;
- notification of purpose, which allows controllers to collect, use, and disclose data when it is impractical for the controller to obtain consent (and deemed consent does not apply), and the collection, use, and disclosure of data is not expected to have any adverse effect on the data owner.

The addition of these grounds for processing personal data gives the PDPA the flexibility to address the evolving challenges brought by ubiquitous computing, the swift growth of Internet of Things ("IoT") devices, artificial intelligence, and machine learning. These trends have resulted in the ability to process large amounts of data, thus leading to possibilities to gain insights that can yield enormous benefits for individuals and society.

Moreover, the "legitimate interests" ground for processing personal data needs to be clarified by the specification of examples, such as for purposes of: *fraud and crime detection and prevention; information, system, network, and cybersecurity; employment data processing; general corporate obligations and due diligence; product development and enhancement; and communication, advertisement, marketing, and intelligence.*[2]

VIII Sensitive Personal Data

Section 22 of the draft PDPA:

[2] (CIPL Examples of Legitimate Interest Grounds for Processing of Personal Data, 16 March 2017, https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/final_cipl_examples_of_legitimate_interest_grounds_for_processing_of_personal_data_16_march_2017.pdf)

No personal data related to race, ethnicity, political opinion, religious or philosophical beliefs, sexual behavior, criminal records, health data, or any other data that affects the feelings of the public, as prescribed by the Committee, shall be collected without consent from a personal data owner, unless:

(1) it is granted an exemption under section 20 (2), or (6);

(2) in any other cases as prescribed in ministerial regulations.

The PDPA must not recognize a separate category of sensitive data as it would lead to additional confusion and difficulties in business – without providing any tangible benefits to individual privacy. In fact, some countries that are recognized as having robust data protection frameworks, such as Canada, Hong Kong, and Singapore, do not have a separate category of sensitive personal data.

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. In addition, having this separate, additional category commonly defined as sensitive personal data would be too rigid, and lack essential context, causing additional complexity and delivering little practical benefit. 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.

However, in case Thailand strongly believes that such a category is necessary, it should be a closed list. The PDPC or any other government agency should not have the authority to later on create any new categories of sensitive data or any additional types of "data that affects the feelings of the public", which shall not be collected without consent from a personal data owner. What constitutes sensitive data should not be open and subject to interpretation from a regulator, because the risk that arises is that an expansive interpretation will lead to treating an excessive amount of data types as sensitive, which will stall technological innovation and development.

The law should also acknowledge that the processing of so-called sensitive data can have incredibly beneficial results for the individual 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.

Further, we strongly urge that the phrase *"or any other data that affects the feelings of the public"* be deleted from this section, due to it being vague and over-broad.

IX Access Rights

Section 25 of the PDPA:

> *A personal data owner has the right to request access to their personal data under the responsibility of personal data controller, or request that personal data controller disclose how personal data is obtained without the consent of personal data owner.*
>
> *A personal data controller shall comply with the request under the foregoing paragraph, and may only reject the request in the following cases:*
> *(1) if the request is in conflict with, or contrary to, the provisions of other laws, or for compliance with the court orders;*
> *(2) if the request affects the investigation or interrogation by a competent officer under the law;*
> *(3) if the disclosure of how personal data is obtained may have an adverse effect on the rights and liberties of other person;*
> *(4) in other case as prescribed the ministerial regulations.*
>
> *If a personal data controller rejects the request under the first paragraph, the personal data controller shall enter the rejection along with the reasons therefor in the record under section 30.*
>
> *Upon a request by a personal data owner under the first paragraph that cannot be rejected in accordance with the second paragraph, a personal data controller shall grant the request within 30 days from the date on which the request is received. The Committee may prescribe a shorter period for granting a request, or may extend the existing period, or prescribe other rules as deemed appropriate.*

The PDPA must strike a balance between the rights of users, and the processors and controllers. Recognizing only data owners' rights would unduly burden businesses and thwart the emergence of innovative business models, ultimately harming consumer choice. It is suggested that access rights be recognized, *but only to the extent that they may be accommodated in a commercially feasible manner that is not unreasonably burdensome.* Another ground to reject a request that should be added is *where the provision of the information requires disproportionate effort,* which is currently one of the grounds for rejecting requests under Irish law.

We likewise recommend the addition of another ground for rejecting a request to access data: *when the data is in an anonymized or pseudonymized format, and it would require a*

disproportionate effort on the part of the controller to honor such a request. Article 11 of the GDPR contemplates this case:

> *Article 11*
>
> *Processing which does not require identification*
>
> *1. If the purposes for which a controller processes personal data do not or do no longer require the identification of a data subject by the controller, the controller shall not be obliged to maintain, acquire or process additional information in order to identify the data subject for the sole purpose of complying with this Regulation.*
>
> *2. Where, in cases referred to in paragraph 1 of this Article, the controller is able to demonstrate that it is not in a position to identify the data subject, the controller shall inform the data subject accordingly, if possible. In such cases, Articles 15 to 20 shall not apply except where the data subject, for the purpose of exercising his or her rights under those articles, provides additional information enabling his or her identification.*

An additional ground to reject a request for access that should be added to this section is where the request is frivolous or vexatious.

X Duties of Controllers

Section 28 of the draft PDPA:

> *A personal data controller shall have the following duties:*
>
> *(1) to evaluate the implication on the privacy of personal data on a regular basis;*
> *(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;*
> *(3) if personal data must be provided to other person or juristic person who is not a personal data controller, there must be an action to prevent such other person from using or disclosing personal data without authorization or in a wrongful manner;*
> *(4) to destroy personal data after the expiration of the retention period, or personal data that is not relevant, or in excess of necessity pursuant to the objectives of the collection of such*

personal data, or when a personal data owner revokes consent, except the collection for the purpose of verification and examination, whereby the provisions in the third paragraph of section 26 shall apply to the destruction of personal data, mutatis mutandis;

(5) to notify a personal data owner of a breach of personal data without delay. In the case of a breach of personal data owner 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 delay. Notification shall be conducted as prescribed in rules and procedures by the Committee.

Given the various methods available to ensure that controllers are able to secure their users' data, and that conducting Privacy Impact Assessments is just one among a host of suitable methods, we recommend that Sec. 28 (1) instead read: *"to take the appropriate measures to ensure compliance with the law;"* Approaches that reflect the fact that there are various ways to demonstrate care and respect for data owners' personal data help avoid mere checklist compliance and encourage controllers to find the best, most appropriate privacy-enhancing techniques and technologies, which improve and evolve over time.

For simplicity and clarity, Section 28 (3) should be revised to instead say *"to ensure that data sharing between controllers is supported by legal basis."* However, we stress that the law must focus on ensuring controller accountability for the actions of processors under them (instead of the idea that all parties in the chain of data transfers shall be held liable or responsible). Such an approach would reflect contractual arrangements and principles such as privity.

We likewise strongly suggest that once the data storage period expires, data controllers should be allowed to anonymize the data and use it for other legitimate purposes. This would allow for various beneficial uses of data, such as for research that would improve a wide range of products and services, while similarly protecting data owners, through the anonymization of their data.

Furthermore, we highly recommend that only breaches affecting certain specific forms of personal data must be mandatory to report – and within a reasonable time frame which permits sufficient fact-gathering, investigation, and mitigation. In addition, no notification should be mandated where there is no foreseeable risk of serious harm to users, such as where breached data is pseudonymized, anonymized, or encrypted.

XI Civil Liability and Penalties (Sections 67 – 75)

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 PDPC's various stakeholders.

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

The enforcement strategy of the PDPA must be guided by the objective of maximizing compliance through dialogue, collaboration, and transparency between the PDPA and 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 PDPC 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 which result in a statutory reduction of fines and possible exemptions from penalties.

XII Transitory Provisions

Section 81 of the draft PDPA:

> *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 shall request new consent from the personal data owner to collect, use or disclose such personal data in accordance with this Act in a manner and within a period of not more than three years from the implementation of this Act as described in the ministerial regulation.*

The PDPA must provide a fair chance for enterprises and businesses of all nature and sizes 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 harm 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 not be less than 2 years.

XIII Territoriality

The territorial applicability of the PDPA 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 PDPA apply only to controllers who are established within the territorial bounds of Thailand. Expanding the applicability of the PDPA beyond the borders of Thailand would result in unnecessary complexity.

Furthermore, it is unrealistic for any regime to aspire to centralize the delivery of privacy protections in just one regulator, one that would be charged with the task of overseeing the compliance of any organization around the world, with their norms. Modern and effective privacy regimes should instead seek to encourage the adoption and the 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 MDES is in relation to the safety of the personal data of Thai citizens when transferred abroad, the same may be ensured through a robust statutory framework for data transfers and controller accountability.

Conclusion

Thank you once again for the opportunity to submit comments, which we do hope will be useful to you. Should you have any queries regarding the content of our submission, we would of course be happy to meet with you.

Yours sincerely

Mr Jeff Paine
Managing Director
Asia Internet Coalition