9 March 2020

Hon. Yap, Victor A.
Chairman, Technical Working Group (TWG) of the Committee on Information and Communications Technology
Republic of the Philippines

Subject: Submission on the proposed amendments to the Philippines Republic Act No. 10173 (the Data Privacy Act) under House Bill Nos. 01188 and 05612

On behalf of the Asia Internet Coalition (AIC) and its members, I am writing to express our sincere gratitude to the **Committee on Information and Communications Technology**, for the opportunity to submit comments on the amendments to the **Philippines Republic Act No. 10173 (the Data Privacy Act) under House Bill Nos. 01188 and 05612**. AIC is an industry association comprised of leading internet and technology companies in the Asia Pacific region with a mission to promote the understanding and resolution of Internet and ICT policy issues in the Asia region. Our current members are Airbnb, Amazon, Apple, Expedia Group, Facebook, Google, LinkedIn, LINE, Rakuten, Twitter and Yahoo (Verizon Media).

We acknowledge the importance of this consultation that outlines the key elements of the data protection framework, with an objective of having a safe and secure online environment, and align with global best practices. In the past, AIC has been very active in submitting industry recommendations on some of the key policy issues in Asia, details of which can be accessed here.

In the backdrop of digitalization and growth of digital services across the world, the role of data has become more and more significant. This has given rise to concerns of informational privacy and the exercise of rights over personal data. Without a framework to govern these two subjects, no digital industry can be sustainable.

In this regard, we are grateful to be able to present our concerns and recommendations and would also like to re-state our continuous support and assistance to the Philippines government in its efforts to bring about this transformational change in the privacy landscape. As such, please find appended to this letter detailed comments and recommendations, which we would like to respectfully request **Committee on Information and Communications Technology** and the **Philippines Government** to consider.

Should you have any questions or need clarification on any of the recommendations, please do not hesitate to contact me directly at Secretariat@aicasia.org or +65 8739 1490. Thank you for your time and consideration. Importantly, we would also be happy to offer our inputs and insights on industry best practices directly through meetings and discussions to help shape the dialogue for an effective privacy regime in the Philippines.

Sincerely,

Jeff Paine
Managing Director
Asia Internet Coalition (AIC)

A. PROPOSED AMENDMENTS UNDER HOUSE BILL NO. 05612

1. Definition of Personal Data Breach (Section 3)

We welcome the stated objective of House Bill No. 05612 to align the 2012 Data Privacy Act (*DPA*) with international standards. In this regard, the proposed amendment to the definition of Personal Data Breach would align with one such international standard as provided for in the EU's General Data Protection Regulation (Regulation 2016/679) (*GDPR*). We are fully supportive of aligning the 2012 Data Privacy Act with the General Data Protection Regulation.

2. Definition of Sensitive Personal Information (Section 3)

House Bill No. 05612 further seeks to amend the existing definition of 'Sensitive Personal Information' in Section 3 of the 2012 Data Privacy Act and to align with the definition of 'Sensitive Personal Information' as provided for under Art. 9 of the GDPR.

While we are supportive of this alignment, we would also urge for the deletion of individual's financial data in the definition of Sensitive Personal Information which is in line with international standards, including GDPR. Further, we would recommend the inclusion of a definition of 'biometric data' in this Bill. For example, GDPR defines 'biometric data' as meaning "personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data". Furthermore, we would welcome clarification in the Bill that the processing of photographs should not be covered by the definition of biometric data. At a minimum, Section 3 (2), should include the proviso, "for the purpose of uniquely identifying a natural person" after 'biometric' to provide clarity to controllers as to the scope of this provision.

3. Scope of the DPA (Section 4) and Extraterritorial Application (Section 6)

Section 4 states that to administer and implement that provision of the Act, and to monitor and ensure compliance of the country with international standards set for data protection, an independent body, i.e., National Privacy Commission will be created.

We are supportive of the proposed amendments to Section 4 encompassed within this Bill, which would empower the National Privacy Commission to regulate the processing of information within the jurisdiction of the Philippines irrespective of the location of the data controller.

With regard to the extraterritorial application in Section 6, the Act applies to an act done or practice engaged in and outside of the Philippines by an entity if:

(A) The natural or judicial person involved in the processing of personal information is found or established in the Philippines;
(B) The processing of personal information is being done in the Philippines;
(C) The processing of personal information relates to a Philippine citizen or resident who are in the Philippines, where the processing activities of a natural or judicial person outside the Philippines involves offering of goods or services, or monitoring of behavior within the Philippines; or
(D) The processing relates to personal information of a Philippines citizen or a resident and the entity has a link with the Philippines

Following on from Section 4, we would welcome further clarification in the language of Section 6. In particular, we would suggest the deletion of "found" from Section 6 (A), because "established" has clear legal meaning and covers the objective of this provision.

In the interest of further clarity, we suggest that language in Section 6 (B) and (C) would be amended to specify that they apply only to citizens in, or residents of, the Philippines.

As Section 6 (A) - (C) as amended provides for greater clarity on scope and alignment with international law, Section 6 (D) does not necessarily add further to this and might risk unnecessary confusion. We would suggest the deletion of Section 6 (D) from the Bill.

4. Functions of the National Privacy Commission (Section 7)

We support a strong, independent National Privacy Commission. However, we suggest that the current provisions of the DPA regarding the requirement for the NPC to file proceedings for contempt with the Courts be retained to ensure due process and an opportunity for data controllers to contest such proceedings in accordance with the law. The proposed amendments in this Bill would remove that opportunity for due process and afford the NPC significant powers to hold and punish for contempt in the context of investigations/proceedings without such due process.

5. Criteria for Lawful Processing of Personal Information of Children (Section 12)

While GDPR provides for a digital age of consent between 13-16, there is a considerable body of evidence internationally that points to thirteen as the appropriate age at which parental consent should not be required to access the services of information society providers.

Children do not represent a homogeneous demographic group. Different age categories might have different levels of understanding complex information. Even within similar age categories, children may have differing capacities to understand information depending on their literacy level, cultural background, and education.

Consequently, the Bill does not recognise the varying maturity levels of children at different age groups. While parental/guardian approval makes sense for certain types of collection and use of personal data from children below the age of 13 years, young adults between the ages of 13 and 18 years should be permitted and empowered to make decisions about their data.

A lower age of consent would afford the youth (especially teenagers) better access to: (a) health information, which are vital at their stage of development; (b) educational resources and tools, which they may use in and out of school; (c) resources that would inform them of relevant and current issues, raising their civic and political understanding and consciousness; and (d) ready support resources and platforms, that are already available online.

A recent example of another jurisdiction which followed this international evidence is Ireland. The Irish Ombudsman for Children and the Internet Safety Advisory Committee recommended a digital age of consent of 13 years, which was supported by the Irish Special Rapporteur on Child Protection, the Irish Society for the Prevention of Cruelty to Children and the Irish Children's Rights Alliance, which represents more than 100 organisations involved in child welfare, also supported setting that age of digital consent at 13.

We, thus, propose that the provision be revised to reflect the following: (a) parental consent would only be necessary when consent is the legal basis for the processing (i.e., child-directed services that process data based on legitimate interest, for example, shouldn't necessitate parental consent); and (b) for instances where there is legal basis for consent, to change the digital age of consent to "more than 12 years old", and accordingly reword Section 12, par. (a) as follows:

"PROVIDED, THAT IN THE SPECIFIC CASE OF INFORMATION SOCIETY PROVIDERS OFFERING SERVICES DIRECTED TO CHILDREN , THE PROCESSING OF THE PERSONAL INFORMATION OF A CHILD BASED ON CONSENT SHALL BE LAWFUL WHERE THE CHILD IS MORE THAN 12 YEARS OLD. WHERE THE CHILD IS 12 YEARS OLD OR BELOW, SUCH PROCESSING SHALL BE LAWFUL ONLY IF AND TO THE EXTENT THAT CONSENT IS GIVEN OR AUTHORIZED BY PERSONS EXERCISING PARENTAL AUTHORITY OVER THE CHILD;"

6. Sensitive Personal Information and Privileged Information (Section 13)

We welcome this Bill's introduction of additional legal bases for processing sensitive personal information, which aligns with international law and best practice.

However, the proposed amendment to paragraph (A) removes a data subject's right to make decisions about the processing of his or her own personal information; we therefore recommend that the cross-reference to other laws be removed. Such cross-reference could also lead to confusion and overlap.

The 2012 Data Privacy Act and the amendments proposed in this Bill necessarily provide a high standard for the obligations of data controllers regarding the processing of personal data. In this context, we suggest that the reference paragraph (F), "provided that further processing shall not be contrary to law, morals, good customs, public order or public policy", be removed. This would bring this provision more fully into line with GDPR in the context of the objective of this provision.

As Sections 4 and 6 of the 2012 Act, as amended by this Bill, cover the application of the Data Privacy Act to personal information collected from foreign residents, we would suggest that paragraph (K) is not required within Section 13.

7. Rights of the Data Subject (Section 16)

We welcome the greater alignment of Section 16 with GDPR, but would suggest some clarity in the language.

For Section 16 (B)(2), we suggest a deletion of "as well as the significance and the envisaged consequences of such processing for the data subject". This aligns it with the GDPR which does not contain a similar requirement. It would suffice for subjects to be informed of the purpose of the processing, which is already covered in Section 16(B)(3).

We would recommend that Section 16 (E) provide for the right to restriction or erasure, rather than include a range of actions ("suspension, blocking and destruction") which are not necessary in order to provide the data subject rights envisioned in this provision. Including this range will place an undue

burden on small businesses and entrepreneurs which would have to facilitate a range of overlapping and complex actions in order to comply.

Section 16 (E) (e) and (g), expands on the circumstances in which the right to erasure might apply, which includes situations in which the data controller has "violated" the rights of the data subject or the personal information is "prejudicial" to the data subject. In order to provide clarity for data controllers and data subjects, we would recommend aligning with best practice in international law and removing these paragraphs. It should be noted that having a general "prejudicial" clause lacks the necessary clarity, certainty, and specificity for it to be actionable, as controllers would have no way of knowing what is, in fact, prejudicial, unless it has been held as such by the courts.

As for the reference to "violated the rights of the data subject", if this remains, it should be qualified by "violated the rights of the data subject *under this Act*" and not a general "violated the rights" as that is so general as to also not be actionable, because data controllers would not have sufficient certainty to know which rights are being referred to in this provision.

While we respect the right of an individual to control personal information available about him/her on the internet, this has to be balanced with other rights and concerns of others, such as: (a) the right to freedom of expression, the right to free access to information, etc.; (b) any overarching matter of public interest or concern; and (c) the right to exercise a legal claim against another. We would also propose that this right contemplates a flexible balancing mechanism or exceptions to enable businesses to consider deletion requests against legitimate business purposes for retaining data to the extent technically feasible and commercially reasonable.

Most of these exceptions are incorporated into the text and are made to apply to specific instances or grounds to request for erasure, blocking, or removal. We, however, suggest that these exceptions be made applicable to all grounds.

In line with the general right of persons to access information as well, we recommend that any blocking, removal or erasure also be made to apply locally only. Data protection law should hew to established principles of territoriality, regulating businesses to the extent they are actively doing business within the jurisdiction. Extra-territorial application unnecessarily hampers the growth of new businesses and creates conflicts of law between jurisdictions.

We thus recommend re-wording the right to erasure as follows:

"(E) RIGHT TO ERASURE. "THE DATA SUBJECT SHALL HAVE THE RIGHT TO DELETION OF PERSONAL INFORMATION PERTAINING TO HIM OR HER FROM THE PERSONAL INFORMATION CONTROLLER'S FILING SYSTEM, WHERE:

A) THE PERSONAL INFORMATION IS BEING USED FOR A PURPOSE NOT COVERED BY THE CONSENT PROVIDED BY THE DATA SUBJECT, OR WHERE CONSENT IS INITIALLY GIVEN, DATA SUBJECT WITHDRAWS CONSENT OR OBJECTS TO THE PROCESSING, AND THERE IS NO OTHER LEGAL GROUND OR OVERRIDING LEGITIMATE INTEREST FOR THE PROCESSING ;
B) THE PERSONAL INFORMATION IS NO LONGER NECESSARY FOR THE PURPOSES FOR WHICH THEY WERE COLLECTED;

C) THE PERSONAL INFORMATION WAS UNLAWFULLY OBTAINED OR THE PROCESSING IS OTHERWISE UNLAWFUL ; OR

THE PERSONAL INFORMATION CONTROLLER MAY NOTIFY THIRD PARTIES WHO HAVE PREVIOUSLY RECEIVED SUCH PROCESSED PERSONAL INFORMATION.

THE RIGHT TO ERASE DOES NOT APPLY, OR IS LIMITED TO THE EXTENT THAT DATA PROCESSING IS NECESSARY:

A) IN THE EXERCISE OF THE RIGHT TO FREE EXPRESSION AND OF THE PRESS;
B) IN THE EXERCISE OF THE RIGHT TO FREE ACCESS TO INFORMATION;
C) TO COMPLY WITH A LEGAL OBLIGATION, OR WITH AN ORDER OF A DULY CONSTITUTED GOVERNMENTAL AUTHORITY;
D) FOR REASONS OF PUBLIC INTEREST OR PUBLIC HEALTH, AS DIRECTED AND DETERMINED BY THE GOVERNMENT; AND
E) TO ESTABLISH OR IN THE EXERCISE OF A LEGAL CLAIM OR DEFENSE.
F) PROVIDE PRODUCT OR SERVICE REQUESTED BY THE CONSUMER;
G) TO DETECT OR RESPOND TO SECURITY INCIDENTS, PROTECT AGAINST MALICIOUS, DECEPTIVE, FRAUDULENT, OR ILLEGAL ACTIVITY, OR IDENTIFY, INVESTIGATE, OR PROSECUTE THOSE RESPONSIBLE FOR THAT ACTIVITY;
H) FOR THE PURPOSES OF LEGITIMATE INTERESTS PURSUED BY THE PERSONAL INFORMATION CONTROLLER OR BY A THIRD PARTY, EXCEPT WHERE SUCH INTERESTS ARE OVERRIDDEN BY THE INTERESTS OR FUNDAMENTAL RIGHTS AND FREEDOMS OF THE DATA SUBJECT.

We would also recommend that the right to be informed should not apply if the data subject already has the information or the provision of such information is impossible or would involve a disproportionate effort, as is the case under GDPR.

Also, the right to object to automated decision making should not apply if the decision is necessary for the performance of a contract between the data subject and a data controller or is based on the data subject's explicit consent, as is also the case under GDPR. This provision should also clarify that this objection only applies to decisions made by automated processing which produce a legal, or similar significant, effect concerning the data subject.

We would also suggest that under the right to rectification, third parties who have received processed personal information, shall be informed of its inaccuracy upon reasonable request of the data subject unless complying with this request proves impossible or involves disproportionate effort.

In Section 16 (F), the Bill provides for a private right of action for data subjects. Internationally, it is not clear whether this right actually protects data subjects or resolves underlying privacy matters and, instead, private rights of action result in vexatious litigation for deep-pocketed defendants, leading to a significant burden on small businesses without creating additional privacy protections for people. Another risk is that private rights of action could lead to inconsistent interpretation of rights and obligations in the courts, which would lead to confusion for companies seeking to comply with the law.

A better way to provide meaningful recourse for people is to require companies to respond to complaints people may bring to them and empower the DPA to adjudicate complaints and bring enforcement actions.

8. Security of Personal Information (Section 20)

We submit that the instances of a Data Breach Notification should be properly scoped and defined. We, thus, propose the following amendments to the definition of Personal Data Breach:

a) Limit the application of the reporting requirement to breach of "Sensitive Personal Information" only: We note that the law already expands the definition of "Sensitive Personal Information" in the proposed legislation (i.e., to include other items such as financial data, genetic and biometric data, identification numbers, etc.). The expanded coverage is wide and we submit that: (i) the duty to report breaches should, thus, be limited to breaches of such Sensitive Personal Information only; and (ii) the portion of the provision making it mandatory to report breaches of information which may be used for "identity theft," as well as breaches of "other information" should be deleted.

   Indubitably, the wider definition of Sensitive Personal Information should already cover information sufficient for identity theft. The inclusion of "other information" is too generic, and might only serve to confuse Personal Information Controllers in determining whether an incident is reportable or not.

b) The impact of the Data Breach should also be considered: The previous text includes a materiality threshold, which was unfortunately deleted in the amendatory bill. We submit that the trigger for a legal requirement to notify the National Privacy Commission or users in the event of a Data Breach, based also on the materiality and the possible impact of the breach to the Data Subjects, should be reinstated, i.e., re-include the requirement of significant or serious harm to warrant reporting.

   Applying a "significant harm" or "serious harm" threshold to breach notifications helps to ensure regulators have visibility into the incidents that pose actual risk to users and ensures regulators will be able to focus guidance and oversight activities where they are most needed. Removing the standard could result in over-notification to the Privacy Commissioner and to individuals. (N.B. Within the first nine months after the GDPR took effect, 64,684 data breach notifications were made to EU DPAs).

c) The timeline for notification should be amended to "without undue delay" after becoming aware of the breach instead of within a 72-hour timeframe. Requiring notifications on short timelines can delay a company's efforts to investigate and stop the data breach, as well as interfere with ongoing law enforcement investigations.

d) The requirement for personal information processors to "submit the breach notification to the Commission", where the personal information controllers are not located in the Philippines, is impracticable, globally unprecedented and have counter-productive outcomes for privacy protection. This is because personal information controllers manage the collection of, and access to, personal data. It would not be appropriate, however, for processors to be responsible for reporting data breaches. Personal information processors often do not have visibility over the content of personal information controllers, meaning that they would not be able to distinguish between a mere security incident that does not impact personal data and a personal data breach. Given so, any notification to the NPC , must be made by the controller, and not the processor.

Even if a personal information controller is located outside of the Philippines, the personal information processor is still not in a position to meaningfully assess an incident and report it if necessary, and including such an obligation in the DP Act would (a) not achieve any of the data breach principles specified above, and (b) would incentivize data controllers to move offshore in order to reduce their obligations. Furthermore, such a framework would have counter-productive outcomes for privacy protection and a data breach notification framework, as it will dis-incentivize personal information controllers outside the Philippines from taking *any* responsibility over the reporting of a data breach to the NPC. Given that processors may not be able to tell if personal data was involved in a given breach, this would have substantial implications for a workable data breach notification regime, and potentially result in a lacuna in the law and the regulatory framework.

Based on the point made above, we would likewise want to propose deletion of the amendments to Section 20, Paragraph (e)(4) (Section 11 of House Bill No. 5612), insofar as it also requires Personal Information Processors to file notifications of Personal Data Breaches, within the contemplation of the same section. We propose that the portion thereof reflecting this requirement be deleted in its entirety, for the following reasons:

a) The determination of whether there is a Data Breach belongs to the Personal Information Controller, consistent with existing international laws and rules. Pertinently, the GDPR and other foreign regulations, such as the U.S. Health Insurance Portability and Accountability Act (HIPAA) both place the responsibility to determine and report a Data Breach on a Personal Information Controller.

b) The extent of the Personal Information Processor's participation in the handling of the data is limited to what is stated in the appropriate contract and/or document between it and the Personal Information Controller. Ultimately, the Personal Information Processor merely acts upon the instructions of the Personal Information Controller, the latter of which is ultimately accountable to the Data Subjects. The Personal Information Controller, being essentially the one having ultimate responsibility over the data and its use, is in a better position to determine whether the Data Breach has in fact, occurred, and whether it materially and seriously affects the Data Subjects. In many cases, due to contractual and/or technical limitations, the Processor will not or cannot have access to data necessary to determine if an eligible data breach has occurred.

c) With the substantial administrative penalty and criminal liability attached to non-reporting, Personal Information Processors, if only to avoid being penalized and/or criminally charged, might default to filing notifications for all instances of breach, as a matter of prudence and self-preservation, especially as the 72-hour deadline approaches, on the pretext that the Personal Information Controller is "unable" to file the report. This will be detrimental, not only to the Personal Information Controller, but might also create undue panic on the part of Data Subjects. The regulator might also indubitably meet a deluge of notifications, which may not be productive use of its time and resources.

For these reasons, we propose deletion of this paragraph in its entirety. We would like to reiterate that the notification regime should be easy enough for offshore data controllers to be able to file their own notification. If they are unable to do it, then they can appoint another party to do it on their behalf, but it should not fall on the Data Processor. It creates a moral hazard if the Data Processor has to be involved in notification, because the Data Controller is not going to be motivated to take the right steps to assess data

breaches or minimize their impact and to communicate effectively. We would like stress that a data processor should not be considered a proxy for a data controller.

9. Restitution (Section 37)

The same conduct should not give rise to both administrative and criminal sanctions. This could lead to disproportionate and excessive punishments for privacy violations. We recommend that the last paragraph in Section 37 be removed.

Furthermore, through the private right of action under Section 16, the DPA now envisages that penalties might be levied on data controllers for violation of specified provisions of the Act and for the same contraventions, the PDP data subjects would have the right to claim damages. This combination of penalty coupled with compensation imposes an onerous burden on controllers, and amounts to "double punishment" for the same contravention.

B. PROPOSED AMENDMENTS TO PENALTIES FOR VIOLATIONS OF THE 2012 DATA PRIVACY ACT UNDER HOUSE BILL NO. 01188

We do not support criminal penalties, such as imprisonment, for privacy violations. Criminal penalties are not relevant to the data protection ecosystem as they are inappropriate remedies for non-compliance, which may be corrected through civil fines and penalties.

For this reason, we do not support the proposed increases to the imprisonment timeframes under the DPA.

Imposing criminal liability on data controllers is out of step with international data protection regulations. Imprisoning individuals for violating data protection regulations is excessive in light of alternative punishment approaches that are available. The potential for actual imprisonment for data protection violations will result in many companies avoiding the Philippines as a potential market, a result that would be detrimental to foreign investments.

By placing over-reliance on criminal punitive measures, the Bill ignores opportunities to strengthen enforcement and adopt other means to prevent harm. The Bill should implement an enforcement strategy that focuses on better data breach detection by fostering trust between the regulator and the regulated, promoting accountability mechanisms through codes of practice, and cautiously using punitive sanctions as a last resort. The NPC should also operate as a mediator to enable more efficient data protection mechanisms to fiduciaries and processors. An enduring participatory enforcement strategy is not possible when the law leans more to deterrence and punitive measures.

For this reason, we do not support the proposed increases to the imprisonment timeframes under the DPA.