Joint industry submission on the Philippines Data Privacy Act

4 September 2020

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

Hon. John Reynald M. Tiangco,
Chair, Technical Working Group (TWG)
Committee on Information and Communications Technology
Republic of the Philippines

Hon. Gregorio Honasan II
Secretary, Department of Information and Communications Technology (DICT)
Republic of the Philippines

Ms. Ivy Grace T. Villasoto,
Director, Privacy Policy Office, National Privacy Commission
Republic of the Philippines

Subject: Industry Submission on the Proposed Amendments in the Substitute Bill (of the Philippines Data Privacy Act)

The Asia Internet Coalition (AIC), US-ASEAN Business Council and Information Technology Industry Council (ITI) and our members ("We") wishes to express our sincere gratitude to the **Committee on Information and Communications Technology**, for the opportunity accorded in August to submit comments on the amendments to the **Philippines Republic Act No. 10173 (the Substitute Bill on Data Privacy Act) under House Bill Nos. 01188 and 05612**.

As responsible stakeholders in this policy formulation process, we appreciate the ability to engage with the Technical Working Group (TWG) on key elements of the data protection framework in the Philippines. Collectively, we represent the internet industry and have partnered with the Government of Philippines to promote stakeholder dialogue and best practices on ICT and the digital economy.

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 context, the Data Privacy Act ("DPA") is a much-needed effort and parallels the global movement towards data protection legislation.

Although we appreciate the Philippines government efforts towards developing the DPA, we believe that there are concerns regarding its provisions, aspects of which contradict widely implemented regulations such as the EU GDPR. Furthermore, existing provisions would significantly alter the landscape for digital companies and make it difficult for them to provide their services to citizens and businesses in the country. We strongly recommend that the DPA should have more parity with the best practices, on the grounds that standardization of national data protection regime to help improve compliance and improve business environment. It is useful and important to recognise that many of the ambitious conversations in this area are the subject of in-depth, evidence-based, and lengthy policy research and exchanges, where a panoply of policy solutions are being explored rather than a single legislative route or limited set of questions.

We would like to highlight the following issues and provide recommendations:

1. Firstly, the Substitute Bill further seeks to amend the existing definition of 'Sensitive Personal Information' in Section 3 of the DPA 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 do not support the expansion of this definition to other categories of personal information such as gender identity, financial data, and government ID numbers. The inclusion of "financial data" in particular is broader than other laws (including the GDPR). References to financial data should be removed from the definition of sensitive personal information. Including the category of "privileged information" is first-of-its-kind to the world and is confusing with the sensitive information. We are of the view that privileged information is unprecedented and should be removed. The proposed amendment under the Substitute Bill should not unduly expand the definition of sensitive personal information. It should at least be aligned with definitions found under other data privacy laws, such as the GDPR, Malaysia's Personal Data Protection Act, Australia's Privacy Act, Korea's Personal Information Protection Act and Japan's Protection of Personal Information Act.

2. Secondly, the Extraterritorial Application in Section 3 of the Substitute Bill, amending Section 6 of RA 10173, are broad and practically onerous. We suggest that language in this Section of the Substitute Bill be amended to specify that the provisions apply only to the personal data of data subjects who are in the Philippines, which will help position the country's privacy regime within the international system. A core component of other comprehensive privacy laws, such as GDPR, is to ensure that any user within the territorial scope of the law is afforded the full protections of its provisions and that there is a level playing field for all businesses operating in that jurisdiction. Maintaining the provisions of the 2012 Act which seek to bring all Philippines citizens within scope

irrespective of where they are located and is out of alignment with today's international standards.

3. Thirdly, the DPA currently requires consent even if a data transfer agreement is in place. However, we would recommend considering conforming cross-border transfer requirements to other regimes globally, such as APEC Cross-Border Privacy Rules ("CBPR") and the EU GDPR. The free movement of data underpins the digital economy and plays a fundamental role in ensuring data-driven growth and innovation, and data transfers will allow the use of existing and internationally recognized data transfer mechanisms, such as CBPR. We are encouraged that the Philippines submitted its intent to join CBPR in September 2019 and we look forward to its formal participation. We further suggest that the Philippines consider approaches taken by other data hubs such as Singapore, Hong Kong, or the EU GDPR's Article 46, which provide for a range of independent mechanisms upon which organizations may rely to facilitate cross-border data transfers. These may include Binding Corporate Rules, performance of contract, consent, appropriate safeguards, certification mechanisms (e.g. ISO, APEC CBPR), fraud or crime prevention, the establishment of defense of legal claims, and the broader public interest, etc. To that end, the focus should be on adopting an accountability-based model for data transfers, where the data users are required to be responsible for ensuring security of the personal data transferred in compliance with the Act. There should also be a flexible set of transfer mechanisms to choose from that maintain accountability of the organization undertaking the transfer, while allowing for the most appropriate mechanism to be selected. The ability to transfer data across borders is of significant importance for the Philippines given the role and contribution of the Business Process Outsourcing sector to the economy.

4. Fourthly, we note that the Commission can impose administrative sanctions up to P5,000,000 (app. SGD140,000) per violation. When imposing such sanction, we would suggest that the Commission must take into account the factors such as nature, gravity and duration of the infringement, the intentional or negligent character of the infringement, any action taken to mitigate damage, the degree of responsibility of the controller or processor, any relevant previous infringements, the degree of cooperation with the regulator and other aggravating or mitigating factors. This aims to ensure that fines are properly tailored to the circumstances of the case at hand.

5. Fifthly, we note that the data subject has the right to reasonable access. We would suggest limiting this data access to personal data that were collected or used in the past year. Further, organisations should not comply with the request if it would mean disclosing information about another individual who can be identified from that information, except if the other individual has consented to the disclosure or it is reasonable to comply with the request without that individual's consent.

6. Finally, we note that the controller shall notify the Commission and affected data subjects within 72 hours upon being aware or upon reasonable belief that a personal breach occurred. The threshold to notify authorities and data subjects should be distinguished. It should be made clear that notification to authorities is necessary only where the personal data breach is likely to result in a risk to the rights and freedoms of natural persons and the organisation has not been able to prevent the likely risk of serious harm with remedial action.

In this regard, we are grateful to be able to present our concerns on the same, and would also like to restate our continuous support and assistance to the Philippine government in its efforts to bring about this transformational change in the privacy landscape. We look forward to our continued engagement with the government and in building a credible and globally consistent data privacy framework in the Philippines. Our Secretariat, Mr. Sarthak Luthra, would be happy to answer any questions or concerns that your office may have. He can be reached at mobile +65 8739 1490 or via email at Secretariat@aicasia.org.

Respectfully,

Jeff Paine
Managing Director
Asia Internet Coalition (AIC)

Naomi Wilson
Senior Director of Policy
Information Technology Industry Council (ITI)

Alexander C. Feldman
Chairman, President & CEO
US-ASEAN Business Council