Singapore's Proposed Data Protection Regime Consultation
Comments due Oct 25th

General:

- The US-ASEAN Business Council appreciates the opportunity to comment on Singapore's Data Protection Regime. Data protection and privacy matters are important to the US-ASEAN Business Council and its member companies because the movement of electronic information, digital goods and services within and across borders is critical to businesses around the world. Such issues are also of interest to the Council as it is essential to ensure consumers trust that their personal data is protected in order to for them to engage further with information communication technologies and services, services which hold great potential to stimulate economic development and job growth. Information services are important to electronic retailers, search engines, social networks, web hosting providers, registrars and the range of technology infrastructure and service providers who rely directly on the Internet to create economic value. They are also critical to the much larger universe of manufacturers, retailers, wholesalers, financial services and logistics firms, universities, labs, hospitals and other organizations which rely on hardware, software and reliable access to the Internet to improve their productivity, extend their reach across the globe, and manage international networks of customers, suppliers, and researchers
- Singapore is of great importance as a trusted hub for international businesses
- We offer strong support for Singapore's approach and the proposed Data Protection law. Singapore should be applauded for striking a good balance between data protection, consistency with international best practices while also providing for a light regulatory touch to enable flexibility for businesses and organizations which is essential given the rapid changing pace of technology. The Data Protection regime as proposed is likely to protect the interests of consumers and deliver economic benefits for Singapore including ensuring that Singapore remains a trusted hub and conducive environment for global data management and processing industries.

Questions in relation to objectives and principles of proposed DP framework:

Question 1: Do you have any views / comments on the impact of the proposed DP law on specific sectors? Do you have any suggestions on measures to mitigate this or any other anticipated impact? Share your views.

Singapore should be commended for its efforts to achieve a balance between privacy and business by having a baseline Data Protection Act.

Also, it is important to ensure that the DP regime to be adopted recognizes limitations to internet intermediary liabilities from third-party actions, similar safe harbors in e-commerce legislation for 3rd-party copyright infringement. The critical role of internet intermediaries, such as online platforms, search engines and access providers, in enabling economic growth and innovation has been well documented.

Additionally, we are concerned about the viability of the DP regime working simultaneously with the Banking Secrecy regime.

Question 2: With reference to paragraph 3.8, do you have any views / comments on the concurrent application of the DP law with existing sectoral regulations? Share your views.

MICA's approach to have a baseline law apply across the board with existing sectoral regulations which may impose more stringent data protection regulations (i.e. banking) seems reasonable. Given that there may be potential conflicts between sectoral regulation and the proposed baseline Data Protection Act, guidance should be provided as to which law would apply.

Additionally, sectoral regulations and the Data Protection Act should be technology neutral; that is they should not require, or accord greater legal status to, the implementation of a specific technology or technological specifications for meeting requirements of data protection regulations.

Questions in relation to the definition of "personal data":

Question 3: Do you have any views / comments on the proposed definition of personal data outlined at paragraphs 3.9 to 3.11? Share your views.

As outlined in Section 3.12 the Council generally supports that the proposed law wouldn't prescribe a fixed/hardcoded list of personal data that should be protected given it can be context specific and in view of technology developments are ever changing. In order to provide greater clarity for businesses, we also strongly support the DPC publishing guidelines giving examples of information that may constitute personal data following the enactment of the Data Protection Act. Absent the clarity provided by regulations/guidelines, and using only a reasonableness standard for what constitutes personal data, there would be a much higher risk for litigation to determine whether an organization's actions were reasonable.

Additionally with respect to Section 3.12, there is a need to proceed with caution in particular with considering unique identifiers such as IP addresses and unique numbers associated with cookies and devices as personal data because such identifiers are often not used to actually identify a person and may be associated with more than one person.

MICA should consider applying a different set of regulations for "identifiable" data from "identifying data". In many, if not most, cases, businesses do not attempt to identify individuals from the potentially identifiable data they collect. If a collector of potentially identifiable data commits to not attempt to identify individuals (and to restrict others with whom they share such data to not attempt to identify individuals), or is otherwise not in a position to legally and certainly identify an individual using reasonable means, then such data should be subject to less restrictive regulations.

We applaud Section 3.14 wherein Singapore suggests the application of less restrictive regulations for business contact information and work product information.

Question 4: With reference to paragraphs 3.15 to 3.16, do you have any views / comments as to whether the proposed DP law should cover the personal data of the deceased? If it should, do you have any views / comments on the proposed approach to the protection of personal data of the deceased? Share your views.

NO COMMENT

Questions in relation to the organisations and activities covered by the DP law:

Question 5: Do you have any views / comments on the proposed organisations covered by the DP law? Share your views.

The definition for organizations is acceptable, however the blanket applicability of the Data Protection law such that it applies to all organizations, including small ones, could pose some challenge in setting a baseline regulation that will be protective enough of individuals' data. Despite the added complexity, the "light touch" set forth in 3.19 may be too light if it applies too broadly.

Question 6: With reference to paragraphs 3.20 to 3.22, do you have any views / comments as to whether the DP law should extend to organisations located outside Singapore, so long as they engage in personal data collection or processing activities in Singapore? Do you have any suggestions as to how the DP law could be implemented if it should apply to such organisations? Share your views.

We agree with MICA that while there are valid reasons for extending the coverage of Singapore's Data Protection law to all data collection and processing activities in Singapore, regardless of whether the organization responsible is in Singapore, there are practical difficulties to implementing such a regime including carrying out investigations and enforcement. We support applying Singapore's Data Protection law to cover only organizations in Singapore. Nevertheless, Singapore ought to be able to participate in international or regional initiatives (such as the APEC CBPR) that will facilitate cross-border privacy protection.

That said, MICA should be cognizant of the possibility that not pursuing extraterritorial applicability could work against international acceptance of Singapore as a hub for data processing in that it may be seen as a safe haven for bad actors if they can escape liability by processing data there.

Questions in relation to the general exclusions from the DP law:

Question 7: Do you have any views / comments on the proposed general exclusions from the DP law? Share your views.

The Council supports the exclusion for business contact information.

Question 8: With reference to paragraph 3.26, do you have any views / comments as to whether there should be exclusions for artistic and literary purposes under the DP Act? How should these exclusions be defined if exclusions for artistic and literary purposes should be provided for? Share your views.

NO COMMENT

Question 9: Are there any other exclusions that should be catered for under the DP Act? Share your views.

There should also be exclusions for information an employer collects and maintains about employees as outlined in Section 3.14 and 3.44.

Questions in relation to the proposed general rules:

Question 10: Do you have any views / comments on the proposed general rules under the DP law? Share your views.

As recognized, it is a common practice for organizations to outsource certain processing activities with personal data and we concur that the organization that engages in such outsourcing should remain ultimately responsible. The organization that receives such outsourced data, however, should not be expected to comply with the complete set of regulations. For example, the company receiving the outsourced data typically has no means of providing (or even verifying) if appropriate notice and consent has been provided or obtained. It may be reasonable, however, to impose upon the processing organization obligations of security and restrictions of use of such outsourced personal data.

Section 3.31 provides that "an organization may not, as a condition of supplying a product or service, require an individual to consent to the collection, use or disclosure of personal data beyond what is necessary to provide the product or service." Such restriction is overly prescriptive and an unwarranted restriction on the freedom of contract. For example, it is common for organizations to want to use collected

information to assist in the creation of new products or services, or to offer their customers new products or services. Another common example is the use of collected personal information to present targeted advertising to data subjects which supports the organization's ability to provide the product or service free of charge or at a reduced charge.

Question 11: With reference to paragraph 3.35, do you have any views / comments as to whether individuals should be deemed to have given consent for organisations to collect, use or disclose their personal data if they are notified and given reasonable time to opt out but do not? Share your views.

With reference to paragraph 3.35, we generally agree with this statement as always requiring explicit/implicit opt-in may be too onerous in certain circumstances and as long as there is reasonable time to opt out, this should be sufficient.

Also, we agree that MICA should not prescribe the detailed manner in which consent may be given as it may depend upon the situation. However, as with the definition of personal data, it may be beneficial for the DPC to issue guidance in some situations to provide greater clarity for organizations to ensure they are compliant with the Data Protection regime.

Questions in relation to the proposed rules on collection, use and disclosure of personal data:

Question 12: Do you have any views / comments on the proposed rules on collection, use and disclosure of personal data? Share your views.

Section 3.40 sets the bounds of what can be collected as what a "reasonable person" would deem appropriate. Organizations would flourish with a more defined requirement. We suggest that the bounds of what be could be collected would be that which the organization clearly notifies and, where appropriate, obtains the consent from individuals.

Section 3.41 requires the disclosure of the contact information of the officer or employee who is able to answer questions about the organization's collection of personal data. Employees, and their roles within an organization, change over time. Suggest that the identification of such person (or people) be to the role in the organization rather than a person.

Question 13: Do you have any views / comments on the proposed exceptions to the rules on collection, use and disclosure? Should an exception be provided for organisations to collect, use and disclose an individual's personal data for the purposes of identifying him or her as a member, or for circulation within the organisation? Are there any other exceptions that should be provided? Share your views.

In general, we do not disagree with any of the exclusions outlined by MICA.

In particular, with respect to Section 3.45, we support exception for organizations to collect, use and disclose an individual's personal data for the purposes of identifying him or her as a member, or for circulation within the organization. It is often important and necessary for this information to be used for the internal functioning of the organization including for security and protection of confidential business information purposes.

We strongly support the exclusion for consent for when an organization outsources collection/processing of personal data to another organization as long as individual previously consented to the collection of his personal data by the organization and sharing is solely for purposes for which info was collected as outlined in Section 3.48.

We support the exception outlined in Section 3.56 for organizations to disclose personal data for research purposes without consent provided that personal data isn't linked to other information that could be harmful to the individuals identified by the personal data and the benefits are clearly in public interest.

We support the specific exclusion in Section 3.57-3.59 for sharing and transfer of personal data in order to facilitate due diligence in the case of mergers and acquisitions.

In addition to the exclusion of consent outlined in Section 3.53, which we support, as it relates to a public agency or law enforcement agency in Singapore for the purpose of an investigation or to comply with a subpoena, warrant or order issued by made by a court, we suggest that this exclusion apply regardless of whether such request or demand is made within Singapore or by the legal process of another jurisdiction.

Additionally, we suggest that the exclusion of consent apply where the use of personal data is pursuant to an organization's investigation of potential violations of law or the organization's policy.

Question 14: Do you agree with the proposed approach to the transfer of personal data outside Singapore outlined at paragraphs 3.60 to 3.61? Share your views.

We agree with MICA's proposed approach regarding the transfer of personal data outside Singapore, in particular not implementing prescriptive rules and instead placing the onus on organization to ensure appropriated measures are taken to protect personal data where such data is transferred outside Singapore.

Questions in relation to the proposed rules on accuracy, protection and retention of personal data:

Question 15: Do you have any views / comments on the proposed requirements for the accuracy, protection and retention of personal data outlined at paragraphs 3.62 to 3.67? Share your views.

We support Section 3.63 as it recognizes accuracy requirements can be unnecessarily onerous and that the efforts by organizations should be reasonable. The degree of

accuracy and completeness of the data should be judged in light of the use of the data for example, if personal data is likely to be used to make a decision that affects the individual to whom the PD relates than a higher standard of reasonableness should apply as suggested by MICA.

With respect to Sections 3.64-3.65, we support that the proposed regulations regarding security are technology neutral, that is, they not require, or accord greater legal status to, the implementation of a specific technology or technological specifications for meeting requirements of data security regulations. Additionally, the reasonableness of the security measures should be judged in light of the sensitivity of the data.

Question 16: With reference to paragraph 3.67, do you have any views / comments as to whether organisations should be required to specify the retention period when collecting personal data? Share your views.

Organizations should not be required to specify the retention period at the point of collection of the personal data.

Questions in relation to the proposed rules on access to and correction of personal data:

Question 17: Do you have any views / comments on the proposed rules on access to and correction of personal data? Share your views.

We support, as outlined in Sections 3.68-3.73, organizations' ability to charge a reasonable fee for access to personal data and not being required to provide access to personal data if it is subject to legal privilege or if the disclosure of information would reveal confidential commercial information that if disclosed, could, harm the competitive position of the organization. We also support the organizations ability to refuse individuals' access to personal data where they face frivolous requests or when it would be unreasonable.

Furthermore, in cases where the personal data is merely "identifiable" (but does not positively identify individuals), organizations should not be required to provide individuals with access, deletion and correction capabilities. To do so may have the perverse effect of requiring organizations to collect identifying data in order to authenticate the individual to effectuate their request.

Questions in relation to the proposed penalty and enforcement regime:

Question 18: Do you have any views / comments on the proposed enforcement powers of the DPC or the proposed appeals mechanism? Share your views.

Question 19: Do you have any views / comments on the proposed penalties for contravention of the DP law outlined at paragraphs 4.4 to 4.5? Do you have any views / comments on the criteria for breaches that would warrant financial penalties? Share your views.

Although desirable for purposes of deterrence, penalties should always take into account the purpose of the law which is to prevent harm to individuals from wrongful collection or misuse of personal information.

We are deeply concerned about making this law subject to criminal penalties, especially the addition of a private right of action as it may result in numerous frivolous lawsuits. If criminal penalties are enforced, they should be for substantial breaches where the potential for harm is very large and where the defendant has been proven to act with malicious intent.

We request clarification from MICA that the potential penalty is on a per incident basis rather than on a per individual basis.

Question in relation to guidelines for organisations:

Question 20: Do you have any suggestions on specific guidelines that the DPC should provide to help organisations achieve compliance with the DP law? Share your views.

Questions in relation to transitional arrangements:

Question 21: With reference to paragraphs 4.11 to 4.14, do you have any views / comments as to whether a one to two year "sunrise" period would be appropriate? Share your views.

We commend MICA for recognizing the need for a sunrise period for organizations to prepare to comply. The training and education piece in particular is very important. Agree that two years would be an appropriate sunrise period.

Question 22: With reference to paragraphs 4.15 to 4.19, do you have any views / comments on the proposed treatment of existing personal data? Share your views.

We support MICA's proposal to deem that consent has already been given by an individual for the organization to use and/or process existing personal data in cases of where the existing uses are reasonable taking into account the nature of the organization's business.

Question 23: Are there certain organisations that may require different transitional arrangements? Share your views.

Questions in relation to proposed National Do-Not-Call registry:

Question 24: Do you have any views / comments as to whether a National Do-Not-Call registry should be set up in Singapore? Share your views.

The Council has no specific position on the development of a National Do-Not-Call registry but support Section 5.5. Which states that if an individual has specifically consented for the organization to call/send them telemarketing messages than this would still be permissible even if the individual has registered with the national DNC registry.