US-ASEAN Business Council
100 Beach Road, #22-04/05
Shaw Tower, Singapore 189702
Tel (65) 6339-8885
Fax (65) 6339-1982

July 16, 2019

Personal Data Protection Commission
10 Pasir Panjang Road
#03-01 Mapletree Business City
Singapore 117438

Re: Public Consultation on Proposed Data Portability and Data Innovation Provisions

On behalf of the US-ASEAN Business Council[1] ("**US-ABC**") and its members, thank you for this opportunity to comment on the Personal Data Protection Commission ("**PDPC**")'s public consultation on *Proposed Data Portability and Data Innovation Provisions*, as part of the Government of Singapore's ongoing review of the Personal Data Protection Act 2012 ("**PDPA**").

As outlined in the public consultation paper, data portability can provide various benefits to individuals, businesses, and to the digital economy overall. It can enable user control over their personal data and autonomy in their activities in digitally enhanced sectors, promote competition in digitally enabled services through reduced switching costs, and enhance innovation and support economic growth by improving access to data, within and across sectors.

In support of Singapore's continued development of its personal data protection regime, we would like to respectfully offer comments and seek further clarification on the *Proposed Data Portability and Data Innovation Provisions*, which are detailed below. **We respectfully request that PDPC and other relevant agencies consider these recommendations when reviewing the *Proposed Data Portability and Data Innovation Provisions*.**

Furthermore, we commend the Government for conducting a multi-stakeholder consultation process and would also like to express our appreciation to PDPC and the Infocomm Media Development Authority ("**IMDA**") for inviting us to a focus group discussion on Data Portability Codes of Practice ("**COP**") on June 17. Our members found the session extremely valuable and we look forward to furthering our discussions on the COP as PDPC and IMDA continue to develop them.

Thank you again for the opportunity to provide feedback on the proposed provisions, and to the Government of Singapore for its leadership in promoting data-driven innovation.

[1] For 35 years, the US-ASEAN Business Council has been the premier advocacy organization for US corporations operating within the dynamic Association of Southeast Asian Nations (ASEAN). Worldwide, the Council's membership, more than 160 companies, generate over $6 trillion in revenue and employ more than 13 million people globally. Members include the largest US companies conducting business in ASEAN, and range from newcomers to the region to companies that have been working in Southeast Asia for over 100 years. The Council has offices in: Washington, DC; New York, NY; Bangkok, Thailand; Hanoi, Vietnam; Jakarta, Indonesia; Kuala Lumpur, Malaysia; Manila, Philippines; and Singapore.

RESPONSES TO THE PROPOSED DATA PORTABILITY OBLIGATION

1. What are your views on the impact of data portability, specifically on consumers, market and economy?

US-ASEAN Business Council Response:

As acknowledged in the public consultation paper, we encourage PDPC to continue to review international data protection developments as it looks to create Singapore's own provisions. Interoperability and consistency are key to the facilitation of cross border data flows. Ensuring alignment with other existing data portability provisions, such as the European Union's General Data Protection Regulation ("**GDPR**") or Australia's Consumer Data Rights ("**CDR**") will further chart Singapore's progression as a robust digital economy and a hub for international businesses. The ISO Cloud Standard ISO/IEC 19941:2017 is also a global standard setting effort which addresses cloud computing interoperability and portability. In addition to other existing data portability provisions and standards, Singapore may also wish to monitor other data protection developments, such as the Brazilian Data Protection Law, Lei Geral de Proteção de Dados ("**LGDP**"). This law, which is already signed and comes into effect in 2020, is consistent with the GDPR and creates a standard that is effectively tri-continental in nature.

Standardized means of transferring data between services are essential for scalable, secure forms of data portability. Given that there are no internationally defined or developed standards to address data portability yet, we are supportive of the development of the industry-led initiatives. For example, the Data Transfer Project ("**DTP**") is a way of establishing best practices and industry standards around direct data portability solutions. While we recognize that the mechanism is still in active development, industry-developed standards can help ensure transfers are privacy-protective and secure, enable scalable implementation to cater to the varying size and expertise of organizations, and reduce compliance costs.

We further encourage PDPC to consider the principle of proportionality and overall cost of compliance. Depending on the mechanisms chosen, compliance with a Data Portability Obligation (or the "**Obligation**") may add a substantial cost on any business. Furthermore, many data portability requirements may be more burdensome for smaller providers than for larger providers. Smaller providers may have less capacity to efficiently process portability requests (both in porting and receiving data), and less ability to implement portability mechanisms more securely. Thus, any portability requirement should take into consideration the varying capacities among organizations.

Lastly, most jurisdictions that have adopted or are adopting data portability rights either require an organization to provide the data directly to the individual (e.g. California Consumer Privacy Act or "**CCPA**") or, if organizations are expected to exchange data without the data subject playing a direct role, to make sure not to put an additional burden on organizations to maintain processing systems which are technically compatible (e.g. GDPR Recital 68 and Article 20). We encourage PDPC to either consider making this clarification or adopting a "wait and see" approach to allow more time for better visibility from other international jurisdictions on the practical implications of introducing data portability rights.

2. What are your views on the proposed Data Portability Obligation, specifically –
   a. scope of organisations covered; and
   b. scope of data covered?

US-ASEAN Business Council Response:

Under the Discussion Paper on Data Portability issued on February 25, 2019, PDPC defines data portability as "allow[ing] individuals to obtain and re-use their personal data for their own purposes across different services. It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability."[2] Fundamental to this definition is the scope of data covered by a Data Portability Obligation. Clarity in determining what types of data are subject to the Data Portability Obligation will be essential to enable businesses – regardless of size and expertise – to appropriately develop portability mechanisms.

While PDPC's proposed Data Portability Obligation resembles the archetypal "right to data portability" in Art. 20 of the GDPR, it does not condition the fulfillment of an individual's request to have his or her data transmitted to another organization on *technical feasibility*. This is an important condition that we recommend PDPC include in a finalized Data Portability Obligation. If requests are permitted in circumstances where they are not yet technically feasible, individuals' expectations may not be met and organizations may attempt transfers that are neither technically sound nor secure, to the detriment of individuals' data protection interests and expectations.

a. Scope of Organizations Covered

We support the proposal to apply the Data Portability Obligation only to a data controller which "collects, uses or discloses personal data in Singapore."[3] However, we recommend a slight narrowing of the scope of organizations covered to include only those organizations which are collecting, using, or disclosing personal data based on consent or contract with the requesting individual, as in GDPR, and that the scope clearly excludes employee data. This ensures that only those organizations which have a direct relationship with the requesting individual and who are providing services directly to the requesting individual are included within scope. Whereas data intermediaries (data processors) would be excluded from the scope of this Obligation, they can still be engaged by the responsible organizations (data controllers) to provide services that support the data portability request.

Furthermore, we are supportive of the recipient organization having to inform the individual of the purposes for which it is collecting, using and disclosing ported data. However, there should be an explicit obligation on the receiving organization to protect the data appropriately to ensure the security of the personal data received. This is further discussed in our response to Question 4 below.

b. Scope of Data Covered

Section 2.22 states that the Data Portability Obligation would apply to only data held in electronic form. We would like to recommend that the Obligation apply only to data held in electronic form that is structured.

[2] United Kingdom ("UK") Information Commissioner's Office – Guide to General Data Protection Regulation (GDPR) / Individuals Rights / Right to Data Portability; Section 1.2 of the *Discussion Paper on Data Portability*

[3] Section 2.16 of the public consultation paper

Unstructured data, while electronic, is free-form and it may be very burdensome for organizations to identify and extract only the portions relevant to the data subject. Additionally, as unstructured data may include information that should not be disclosed to the individual, restricting the scope to only structured data would limit the risks of inappropriate disclosures by organizations.

As specified in Section 2.24, footnote 12, we note that the proposed provisions by Singapore are not limited to "personal data" as defined under the PDPA, particularly in cases where an individual may request for their data to be transmitted to another organization in another jurisdiction through a commonly used machine-readable format. If the data portability requirement is too broadly scoped, it could implicate the privacy interest of individuals other than the one making a request. In addition, we believe the extension of the scope of data covered under the data portability obligation does not fit within the purpose of the PDPA, which is meant to govern the "collection, use and disclosure of **personal** data"[4] (emphasis added). Furthermore, the proposed Obligation would apply only to an organization that "collects, uses or discloses **personal** data in Singapore."[5] Hence, non-personal data that does not fall under the "personal" data definition under the PDPA should not be part of this Obligation at all. Information that is generated for internal purposes, and which cannot be reasonably decoupled from personal data, should also not be subject to the Data Portability Obligation.

If the above recommendation is not adopted, then the scope of the "user activity data" should be clarified and narrowed down. First, it may be difficult to distinguish between "derived data" and "user activity data"; a consumer's use of an online service is the essential contributor to "derived data," which could lead to confusion from providers regarding the distinction, leading to either under or over reporting during porting exercises. Second, the broad definition of "user activity data" will make it exceptionally challenging for service providers, especially small ones, to determine what must be collected, saved, and ported. We therefore believe that the definition of "user activity data" should be more narrowly tailored and seek guidance from the PDPC to provide clear examples of what constitutes "user activity data" (vis-à-vis "derived data").

The inclusion of third party data is also problematic as it could adversely implicate the privacy interest of other individuals. Whereas Section 2.31 notes that consent must be obtained from third parties for the collection, use or disclosure of their personal data for other purposes, it creates an onerous burden on porting organizations, especially the social media industry, if they are expected to receive consent from all third parties involved. It would also be difficult for recipient organizations to ensure that such third party consents have been obtained, except to rely on the individual who has made the data portability request.

A broad scope may also cover information which implicates the intellectual property ("**IP**") of business interests of a compliant organization and stymies innovation. Based on "user activity data", inferred or observed data might include proprietary information that is used to provide or improve services. We appreciate that PDPC aims to strike a balance between implementing a Data Portability Obligation and protecting first movers from unfair competition by fast followers; however, requiring companies to make such information available for porting could compromise IP rights and their proprietary nature. In this age where a business' competitive edge is largely data-driven, including inferred data within the realm of data

[4] Article 3 Purpose of the Personal Data Protection Act 2012, (No. 26 of 2012)

[5] Section 2.16 of the public consultation paper

subject to the Data Portability Obligation ignores the investment and risk taken by the first mover to develop a viable business model. Inadvertent or intentional access to these insights could allow some companies to duplicate the unique features of others, reducing companies' incentives to innovate.

Section 2.29 further proposes that business contact information[6] (BCI) would be covered under the proposed Data Portability Obligation but not under the Data Protection Provisions of the PDPA. Many other data privacy laws, such as the EU GDPR, focus on the right of a natural person in their capacity as such, and not as an entity or an individual acting as an agent to an entity. While we appreciate that allowing BCI to be within scope would be helpful for facilitating business activities, we would caution against the cross-classification of BCI as the policies should remain focused on protecting the privacy of the individual.

The example in Section 2.35 states that personal data which are required to be collected by law for compliance purposes would not be subject to the proposed Data Portability Obligation. We agree with this scoping and would like to emphasize that the Obligation should expressly avoid situations where Anti-Money Laundering (AML), Know Your Customer (KYC) or data required to be collected to fulfill specific regulations or laws might inadvertently be caught in this scope.

We also hope to seek clarity on the porting of historical data. In particular, we would like to understand under what circumstances the proposed Data Portability Obligation would allow organizations to provide an individual's historical data to another organization, as this may impact compliance with existing data retention and data disposal rules for certain organizations. Organizations should not be required to retain data solely for the purpose of enabling portability, which may render some "user activity data" unavailable for porting depending on the time of the request. For business certainty, we suggest the Obligation clearly state a defined time period from which historical data must be available. For instance, a time period of six months could help ensure that companies are not unnecessarily storing excessive historical data.

The limitations and restrictions on the use of obtained data should be explicitly laid out. One point of reference is the GDPR's principle of purpose limitation and data minimization (see GDPR Art. 5(b) and (d)) which requires personal data to be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes and that the data processed is adequate, relevant and limited to what is necessary. This ensures that an organization's obligations are clear and that the responsible organizations do not incur excessive costs for porting data that would be effectively rendered useless to the consumer. For example, an organization could have data about individual's use of a service which may include every piece of content an individual has viewed within a certain period, every link the individual has clicked on, and every notification the individual has received. The challenge and operational burden of making such log data portable, especially for smaller and medium enterprises, may outweigh the benefits to the consumer.

[6] Business contact information is defined in the PDPA as "an individual's name, position name or title, business telephone number, business address, business electronic mail address or business fax number and any other similar information about the individual, not provided by the individual solely for his personal purposes".

3. What are your views on the proposed exceptions to the Data Portability Obligation, specifically –
   a. the proposed exception relating to commercial confidential information that could harm the competitive position of the organisation, to strike a balance between consumer interests and preserving the incentive for first movers' business innovation; and
   b. the proposed exception for "derived data"?

US-ASEAN Business Council Response:

We thank the PDPC for its thoughtfulness in supporting data-driven innovation and encouraging competition as it looks to introduce a Data Portability Obligation. We are generally supportive of the proposed exceptions to the Data Portability Obligation so as not to undermine business innovation and hope that PDPC preserves its pro-innovation intentions in the finalized Data Portability Obligation.

Confidential Commercial Information

While we understand that "commercial confidential information," or "confidential commercial information" as written in Section 2.27, may be hard to define, we hope that any future precedent recognizes that interpretations of "confidential commercial information" may vary depending on internal confidentiality policies.

"Derived Data"

We appreciate PDPC's recognition that data which has been used to derive new business insights with business-specific input can be proprietary information. However, we would appreciate further clarity on the proposed definition and scope of "derived data". Any definition should be inclusive of data analytics, enrichment services, and other data for which a company may have invested to derive greater insight into the data subject. Inadvertent or intentional access to these insights could allow businesses to duplicate the features of others, which would reduce businesses' incentives to innovate. Where such data has not been explicitly excluded, we encourage PDPC to offer further clarity on its definition and proposed scope.

In addition to the exceptions mentioned in Section 2.45 which are aligned with the exceptions to Access Obligation, the Data Portability Obligation may wish to consider providing exceptions to any data which may (i) compromise the privacy or security of personal information for other individuals, or (ii) violate laws or the rights and freedoms of other individuals.

4. What are your views on the proposed requirements for handling data portability requests?

US-ASEAN Business Council Response:

The overall proposed requirements for handling data portability requests are detailed and account for many different factors which can impact how personal data should be securely ported from one organization to another. However, under Section 2.37(d)(ii) of the *Proposed Data Portability and Data Innovation Provisions*, PDPC is proposing to prescribe that organizations have no more than seven calendar days for the porting of data upon confirmation of the data after a request. Seven calendar days may not allow feasible time for response, as time is needed for porting organizations to correspond with the individual, to verify the data

portability request and the data to be ported, to contact the receiving organization, to assess adherence to any COP, to ensure compatibility in data format, and more. Given that data portability will be new to many organizations in Singapore, we recommend that a timeline be provided only upon further clarity on the procedures and practical ability of companies to meet such Data Portability Obligation.

Moreover, this Obligation is much stricter than any other data subject rights under the PDPA. Under existing Access and Correction Obligation provisions, if an organization is unable to comply within 30 calendar days from the time it receives the request, it must inform the individual of when it will respond to the request within that time frame.[7] In line with this, ideally, we recommend a 30 calendar day period to respond to a request for the right of portability with a right to a further 60 calendar days extension where necessary. As an alternative model, the PDPC may also consider deriving guidance from the CCPA, which gives a timeline of 45 days to reply to the consumer upon receiving a verifiable consumer request with a permissible extension of 45 days (Art. 1798.130(a)(2) of the CCPA).

On the format for porting data, we thank PDPC for not prescribing a specific data format for the transmission of data and instead permitting flexibility in choosing machine-readable, accessible and open formats as noted in Section 2.37(e). To that end, we hope to understand if there would be any restrictions on the format of data that could potentially be proposed by PDPC in the COPs. As mentioned above, we encourage the PDPC to work with the industry in developing the best mechanisms for implementation of the Data Portability Obligation and implementing the processes that result in the least compliance cost and optimize operational efficiencies for the responsible organizations.

<u>Rejection of Data Porting Request</u>

We would appreciate additional clarification around the circumstances in which an organization might reject a data portability request, beyond instances where the "organization does not hold data of the individual that is covered by the requirement."[8] In instances where the receiving organization may be a bad actor, or where they may have suspect data protection practices, we would seek guidance on whether a porting organization can reject a request. We also would like to understand if an organization would be able to reject a data porting request so long as it makes a reasonable effort to explain the circumstances to the requesting individual.

<u>Data Security and Liability</u>

Data portability can pose many cybersecurity challenges, even when implemented correctly, as it may increase the likelihood of attack by enlarging the number of sources of vulnerabilities for attackers to siphon user data. Considering that the security of data is only briefly covered in the COP under Section 2.49(d), we encourage PDPC to further build upon this obligation. This would include specifying to what extent porting and receiving organizations would be responsible for ensuring security, particularly during data in transit.

One means of addressing concerns over data security and privacy in the context of a data portability request could be a system of accreditation or certification, based on existing global standards, under a COP developed in consultation with industry and relevant stakeholders. To avoid introducing burdensome additional reporting requirements or double certification with this system, there should be a carve-out for

[7] Section 15.18 of *Advisory Guidelines on Key Concepts In The Personal Data Protection Act*

[8] Section 2.37(f) of the public consultation paper

entities which adhere to certain global standards (e.g. ISO, NIST, etc.) or are already regulated within their respective regulatory authority (e.g. Monetary Authority of Singapore for financial services). Instead, these COP should encourage a joint government and industry mechanism to ensure individuals are informed about potential data recipients, and to guard against bad actors who might have subpar data protection practices or seek to obtain personal data under false pretenses.

Furthermore, PDPC should consider including limitations on liability. We are encouraged by Section 4.17 of PDPC's *Discussion Paper on Data Portability,* which states that "[t]he porting organization cannot be expected to vet all data recipients, so it should be exempted against any claims for damage from any misuse of data by data recipients." Portability requirements should limit the liability for organizations that port data pursuant to an individual request in a manner that is appropriately secure. Standards and protocols must be developed to verify the identity of the data recipient prior to the data portability request being fulfilled. For example, if there is a lack of proper verification of data recipient, this could create a mechanism for cyber criminals to siphon data and result in a data breach. To that extent, we encourage PDPC to issue further guidance on this point.

5. What are your views on the proposed powers for PDPC to review an organisation's refusal to port data, failure to port data within a reasonable time, and fees for porting data?

US-ASEAN Business Council Response:

PDPC proposes to have powers to review an organization's refusal to port data, failure to port data within a reasonable time, and fees for porting data in Section 2.47. We appreciate that these proposed powers are consistent with the powers to review for the PDPA's existing Access Obligation. However, for the reasons explained in our response to Question 4, it would be beneficial for organizations to have clear guidance around cases where it would be appropriate to reject a data porting request.

6. What are your views on the proposed binding codes of practices that set out specific requirements and standards for the porting of data in specific clusters or sectors?

US-ASEAN Business Council Response:

Given the complexity and challenge of trying to implement cross-sectoral data portability, we recommend limiting the *Proposed Data Portability and Data Innovation Provisions* to certain industries. There are many sector-specific considerations when introducing a Data Portability Obligation, and sectoral COPs that address consumer safeguards, counterparty assurance, interoperability and security of data could help add clarity to the appropriate levels of privacy and security required in each sector. For example, this is being done in Australia's CDR which will apply to open banking through a phased implementation approach starting from July 2019, with the energy and telecommunications sectors to follow. To this end, we also recommend that any dataset-specific COP should be developed in conjunction with various industry verticals to ensure applicability and appropriateness of the COP.

In addition, we would kindly ask PDPC to reconsider the "binding" nature of the COPs. As a usual practice, being voluntary in nature is the essence of any such "Codes of Practice" and they would best serve as voluntary guidelines, developed in coordination with the industry in a multi-stakeholder environment. With regards to the topics proposed to be covered by such COPs, we would advise PDPC against setting mandatory data formats, standards for transmission of data and for the integrity and security of participating systems that would apply and be specific only to Singapore. We believe these voluntary COPs should be developed together with the industry and their respective industry regulators in cases where the COPs will be dataset-specific (e.g. in financial services[9]) and should refer to international standards in support of regional and global interoperability. For the reasons outlined in our response to Question 1, the DTP could be a mechanism to support the establishment of voluntary COPs which are principles-based and rooted in best-in-class practices. We would also ask that PDPC actively participate in the establishment of voluntary COPs as there may be technical feasibility and operational hurdles to implementing data portability, and it would benefit the public if PDPC itself were also involved in this process of "learning by doing".

[9] For example, the Monetary Authority of Singapore has done significant amount of work supporting open APIs in the banking industry, which could be leveraged for the Data Portability Obligation.

RESPONSES TO THE PROPOSED DATA INNOVATION PROVISIONS

7. What are your views on the proposed approach for organisations to use personal data for the specified businesses innovation purposes, without the requirement to notify and seek consent to use the personal data for these purposes?

US-ASEAN Business Council Response:

With the rapid pace of change in technology, it is important that the regulatory environment maintains flexibility for continued innovation. We support the proposal to enable the innovative use of data without the need to notify and seek consent in every instance. The approach proposed by the PDPC achieves a good balance between the need to protect individuals' privacy while providing the space for innovation.

We commend PDPC for proposing data innovation guidelines that enable organizations to confidently use data to derive business insights and innovate in the development and delivery of products and services. All businesses should support and adopt privacy standards that promote innovation while ensuring appropriate protection of sensitive personal information.

For example, safeguarding consumer data and ensuring consumer trust are critical to the global payments ecosystem. Many data privacy proposals include provisions to enhance an individual's ability to access, rectify, limit and even delete data relating to them. While these "rights" are intended to give individuals greater control over their data, they can also become leverage points for fraudsters and other bad actors. If an appropriate identity verification process is not in place, there is potential for fraudsters and other bad actors to abuse access requests to obtain access to consumers' sensitive financial data. To safeguard against this, we support PDPC's statement that "[w]here individuals withdraw their consent for the use or disclosure of their personal data for the purposes for which the organization had collected the personal data, organizations may continue to use such personal data for business innovation purposes[10]." Specifically, it is crucial that these business innovation purposes include the use of data in connection with fraud monitoring and prevention.

8. What are your views on the proposed definition of "derived data"?

US-ASEAN Business Council Response:

As mentioned in our response to Question 3(b), we would appreciate further clarity on the definition and scope of "derived data," and recommend that PDPC clarify that it would be inclusive of data analytics, enrichment services, and other data for which a company may have invested into derive greater insight into the data subject. In Section 3.12, PDPC defines "derived data" as "new data that is created through the processing of other data by applying business-specific logic or rules." However, it may be helpful to clarify whether "business-specific logic or rules" refers specifically to the application of information or algorithms that are proprietary, confidential, or otherwise commercially important to an organization. We would

[10] Section 3.7 of the public consultation paper

encourage the PDPC to clarify and broaden the description of methods through which derived data may be developed.

In addition, we would like to understand if "derived data" includes inferred data. The reference to "new data" in the definition of "derived data" may inappropriately limit the scope of definition, as "derived data" may not always be new. It could, for instance, be a result of rearranging data or combining data to draw insights. Therefore, we would kindly suggest that PDPC remove the term "new" from the definition of "derived data".

9. What are your views on the proposal for the Access, Correction and proposed Data Portability Obligations not to apply to derived personal data?

US-ASEAN Business Council Response:

We would, in principle, be supportive of the proposed exclusions for the Access, Correction, and proposed Data Portability Obligations, although this would depend on the definition of "derived personal data" for the reasons noted in our response to Question 3(b). In particular, requiring that the Correction Obligation apply to derived data would be problematic as it would potentially apply to enriched information about an individual, which may include proprietary information, data analytics, and enrichment services.

CONCLUSION

Once again, the US-ASEAN Business Council and our members thank you for the opportunity to provide comments and seek greater clarification on the *Proposed Data Portability and Data Innovation Provisions*. We look forward to working with the PDPC on its ongoing review of the PDPA and its Data Portability COP and stand ready to support you in any way we can.