15 July 2019

To
Mr. Tan Kiat How
Commissioner, Personal Data Protection Commission (PDPC)
10 Pasir Panjang Road,
#03-01 Mapletree Business City, Singapore 117438

Subject: Industry Submission on the Public Consultation on Review of the Personal Data Protection Act 2012 – Proposed Data Portability and Data Innovation Provisions

On behalf of the **Asia Internet Coalition ("AIC")** and its members, I am writing to express our sincere gratitude to the Personal Data Protection Commission (PDPC) and the Government of Singapore, for the opportunity to submit comments on the **Public Consultation on Proposed Data Portability and Data Innovation Provisions**. AIC is an industry association comprised of leading Internet and technology companies in the Asia Pacific region with an objective to promote the understanding and resolution of Internet and ICT policy issues. Our current members are Airbnb, Amazon, Apple, Expedia Group, Grab, Facebook, Google, LinkedIn, LINE, Rakuten, Twitter and Yahoo (Oath), and Booking.com.

We commend the government's efforts on leading this public consultation on the proposed data portability and data innovation provisions. We are of the view that the proposed data portability provision will provide individuals with greater control over their personal data and enable greater access to more data by organisations to facilitate data flows and increase innovation. The issue of data portability and data flows is at a unique crossroads between data protection and competition regulations and should not be considered in isolation.

Such efforts and dialogue are critical, particularly at a time when cross-border data flows and data security has taken a center stage in a digital economy development. As responsible stakeholders, we appreciate the ability to participate in this consultation and the opportunity to provide input into the policy-making process. As such, please find appended to this letter detailed comments and recommendations, which we would like to respectfully request PDPC to consider, particularly to reap maximum benefits from data portability.

Should you have any questions or need clarification on any of the recommendations, please do not hesitate to contact our Secretariat Mr. Sarthak Luthra at Secretariat@aicasia.org or at +65 8739 1490. Importantly, we would also be happy to offer our inputs and insights on industry best practices, directly through meetings and discussions and help shape the dialogue around effective data portability framework in Singapore.

Sincerely,

Jeff Paine
Managing Director | Asia Internet Coalition (AIC) | https://aicasia.org

Detailed Comments and Recommendations
to the Questions Provided in the Consultation Paper

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

We recognize that data portability can provide people with control over their information. Making it easier for individuals to choose among services, facilitates competition and innovation, empowers individuals to try new services, and enables them to choose the offering that best suits their needs. Data portability can benefit consumers by lowering barriers to entry in the market for digital services for competitors who provide comparable services and can enable new business models and innovative services through easier access to data. Competition and innovation are important for the Internet economy—and for creating services people want.

We encourage PDPC to continue to review international data protection regimes and developments as it looks to create Singapore's own framework. Interoperability and consistency are the key to facilitate cross-border data flows, and therefore it is important to ensure alignment with other existing data portability provisions, such as the European Union's General Data Protection Regulation ("GDPR"), Australia's Consumer Data Rights ("CDR"), and the Brazil's data protection law, Lei Geral de Proteção de Dados (LGPD) (unofficial English translation available **here**), which will further chart Singapore's progression as a robust digital economy and a hub for international businesses. The LGPD 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. Like the **EU General Data Protection Regulation (GDPR)**, the LGPD has extraterritorial scope and will apply to global businesses that meet these criteria, regardless of where the company is headquartered. However, the LGPD does not apply to data processing carried out:

- by a person for strictly personal purposes;
- exclusively for journalistic, artistic, literary or academic purposes; or
- exclusively for national security, national defense, public safety or criminal investigation or punishment activities.

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 consider making this clarification.

We also suggest referring to the global standard ISO Cloud Standard ISO/IEC 19941:2017, which addresses cloud computing interoperability and portability requirements. 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 development stages, 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 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.

2. What are your views on the proposed Data Portability Obligation, specifically –

a. scope of organisations covered; and

b. scope of data covered?

We commend PDPC on the proposed data portability obligation **(2.14)**. The obligation as proposed resembles the archetypal data portability regulation, Article 20 of the European Union's General Data Protection Regulation (GDPR), which organisations have been working to implement for many months.

However, unlike GDPR, PDPC's proposed obligation does not condition the fulfillment of an individual's request to have his or her data transmitted to another organisation on technical feasibility. This is an important condition that we recommend PDPC include in a finalised data portability obligation. If requests are permitted in circumstances where they are not yet technically feasible, individuals' expectations may not be met and organisations may attempt transfers that are neither technically sound nor secure, to the detriment of individuals' data protection interests and expectations.

With respect to the **scope of organisations covered (2.16)**, we again commend PDPC's proposal, which generally applies to all organisations that collect, use, or disclose personal data in Singapore. However, we recommend a slight narrowing to the scope of organisations covered, to only those who are collecting, using, or disclosing personal data on the basis of consent or contract with the requesting individual, as in GDPR. This ensures that only those organisations which have a direct relationship with the requesting individual and who are providing services directly to the requesting individual are included within scope.

With respect to the **scope of data covered (2.21-2.36)**, PDPC's proposal is generally appropriately scoped, but could use one improvement. As it stands, the proposed obligation covers "user provided data" and "user activity data," but not "derived data." We agree with the

inclusion of "user provided data" and the exclusion of "derived data" (discussed further below) but recommend that additional limitations be placed on the inclusion of "user activity data."

In paragraph **2.24**, **"user activity data"** is defined as data that is "generated by the individual's activities in using the organisation's product or service." Examples given in **paragraph 2.26** include "the individual's transactions and purchases, search history, location data, outgoing and incoming call logs, steps count, and pulse rate collected through the use of an activity tracker." However, organisations often maintain data generated by the individual's activity in using its product or service that goes beyond the types listed above—data that may prove difficult to make portable.

For example, how organisations retain data might affect the data that should be portable. It seems uncontroversial that organisations should not be required to retain data solely for the purpose of enabling portability, so at least some "user activity data" won't be portable simply because it won't be available at the time of the request. But what about the data that is technically available, but will soon be deleted? Should organisations build tools to export this data too?

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 laid out explicitly. One point of reference is the GDPR's principle of purpose limitation and data minimisation **(see Articles 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 that 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.

Another question is whether there are cases where the burden of making data portable outweighs the individual's interest in exporting it. For example, an organisation's data about an individual's use of a service could include a list of every page or piece of content the individual has viewed within a certain period, every link he or she has clicked on, and every notification he or she has received. Organisations often keep logs of this information for periods of time, but the process of making this log data portable could be challenging, and the benefits to the individual might not

always be obvious. Would it be useful, for example, to be able to export a list of all the link clicks an individual makes on a service within a certain period? Or an archive of every advertisement an individual sees while scrolling through News Feed?

Given that portability is partly intended to encourage competition and the emergence of new services, we should consider these questions in light of the operational burden they would impose on small and medium organisations. Viewed from that perspective, it seems clear that some limitations should be imposed around an organisation's obligation to make user activity data portable. Considering data retention periods and weighing the burden on organisations against the benefit to individuals could be helpful in determining what those limitations should be.

3. What are your views on the proposed exceptions to the Data Portability Obligation, specifically –

1. 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
2. the proposed exception for "derived data"?

PDPC's proposal reflects a thoughtful approach to addressing confidential and proprietary information. As data portability is intended to support the growth of the digital economy and encourage competition and innovation, the scope of data covered should not undermine those goals. PDPC's proposed exception relating to commercial confidential information that could harm the competitive position of the responsive organisation and the proposed exception for "derived data" both work to accomplish the same goal.

Derived data could include or be based on proprietary information (including algorithms) used to provide or improve services. Including derived data or other proprietary information could also expose analytic information containing valuable business insights generated by an organisation through its own efforts—insights that could eventually lead to innovative new features or more efficient operation. Inadvertent or intentional access to these insights could allow some companies to duplicate the features of others, reducing the incentive of companies to innovate. 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 the incentive for businesses to innovate. Where such data has not been explicitly excluded, we encourage PDPC to offer further clarity on its definition and proposed scope.

PDPC's proposed exceptions for commercial confidential information and derived data appropriately aim to preserve the pro-innovation intentions behind data portability and should remain in the finalized text.

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?

PDPC's proposal for handling data portability requests **(Section 2.37-2.38)** is detailed and accounts for many of the different factors that can impact how personal data should be securely ported from one organisation to another. For example, the proposal is flexible as to how requests should be received and requesting individuals should be verified, while also ensuring that requests are submitted in a manner that ensures their authenticity. Similarly, PDPC wisely chooses not to prescribe formats for transmitting data, which would likely chill innovation, and instead permits flexibility in choosing common, machine-readable, accessible, and open formats as appropriate. 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 7 calendar days for the porting of data upon confirmation of the data after a request. 7 days may not allow feasible time for response, as time is needed for porting organizations to correspond with the individual, verify the data portability request and the data to be ported, contact the receiving organization, ensure compatibility in data format, and so forth. 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.

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. 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. To avoid introducing burdensome additional reporting requirements or double certification with this system, there should be a carve-out for 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).

Furthermore, PDPC should consider including limitations on liability. We are encouraged by the proposal in **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.

We recommend additional clarification around the circumstances in which an organisation might reject a data portability request or choose not to perform a transfer to a particular recipient organisation. If an organisation receives a request to port personal data to a destination whose data protection practices are suspect or who may be a bad actor, should the organisation be required to transmit personal data to that recipient? Or should the organisation be able to reject the request so long as it makes a reasonable effort to explain the circumstances to the requesting user?

Upon assessing PDPC proposal in **Section 2.47-2.48,** that it should have the authority to review an organisation's refusal to port data or even to direct an organisation to suspend transmission of data in certain circumstances (e.g. where there are counterparty risks), it would be beneficial for organisations to have clear rules around when refusals to port are appropriate, and how PDPC would undertake such a review, without being overly invasive.

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?

In **Section 2.47,** 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 seem generally appropriate for ensuring that organisations handle data portability requests in good faith. As noted above, given the proposed PDPC power to review refusals to port, it would be beneficial for organisations to have clear rules around when refusals to port are appropriate.

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?

We recommend limiting Proposed Data Portability and Data Innovation Provisions to certain industries. There are many sector-specific considerations when introducing a Data Portability Obligation, and sectoral code of practises 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.

While, PDPC's proposal in **Section 2.49** improves upon other similar data portability requirements, there remain a number of unresolved policy and technical questions with respect to data protection and security in the context of data portability, many of which are sector-specific. Key questions include:

1. <u>What data should be freely portable?</u>
    - Individuals should have the ability to transmit their data to different organisations. But what exactly is their data? What happens when one person wants to transfer data that is associated with another person? Who "owns" that data? How should

commercially confidential or proprietary information or derived data be identified in particular sectors?

2. How should organisations protect privacy while enabling portability?
    - Does the transferring party bear any responsibility if an individual ports their data to a third party that misuses their data? Can a transferring organisation impose some baseline data protection restrictions even when carrying out a transfer to comply with a portability request. If so, which conditions or limitations of liability are appropriate?

3. When individuals' data is transferred, who is accountable if the data is misused or otherwise improperly protected?

Sectoral codes of practise based on an existing global standard and that address consumer safeguards, counterparty assurance, interoperability, and security of data could help shed light on specific answers to the above challenges to implementing data portability mechanisms and provide information to individuals about the obligations on transferring and recipient organisations. The codes of practise could require entities to implement privacy and security safeguards appropriate to particular sectors before receiving user-requested data. Compliant organisations could then be identified with a seal or other certification and would be eligible to receive data from transferring organisations pursuant to portability requests.

A seal or certification associated with a code of practise could also provide users with at-a-glance information about the practises of a third party organisation, and service providers that port data to compliant recipients could be exempted from liability in the event data is misused or improperly processed following a user's data portability request.

We would also like to clarify whether signing up for binding codes will be voluntary in nature, and the codes will only be binding if an organisation chooses to participate, or if the intention is to impose these binding codes of practice on organisations belonging to certain sectors, even without the organization having signed up for the relevant code of practice.

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?

Enabling organisations to use personal data for specified business innovation purposes without the requirement to notify and seek consent to use the personal data for these purposes is a positive development.

However, we would like to seek clarification on whether the scenario below would fall under this approach / exception:

- Assuming that an organisation collected data from individuals without having notified them that the data may be used for any of these business innovation purposes, and that

data was shared with a third party, for business innovation purposes, would the sharing be considered as a business innovation purpose, thus not necessitating notification and consent?

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

In **Section 3.12,** PDPC proposes to define "derived data" as "new data that is created through the processing of other data by applying business-specific logic or rules. Though this definition is useful, additional clarity would be helpful. For example, what is meant by "business-specific logic or rules"? Does this mean that the application of information or algorithms that are proprietary, confidential, or otherwise commercially important to an organisation to other types of personal data would create derived data? There are many ways of creating derived data that may not be due to the application of "business-specific logic or rules"; for instance, through the rearranging of data, or combination of data to draw insights. Hence, clarification and broadening of the description of the methods through which derived data may be developed is necessary.

We would also like to clarify that derived data includes inferred data. In addition, the use of the term "new" in the definition of "derived data" may inappropriately limit the scope of "derived data", since derived data may not always be new - it may simply be, for instance, arranged in a different form. It is thus suggested that the term "new" be removed 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?

As discussed above, PDPC's proposal in the **Section 3.16-3.19,** that the Access, Correction, and proposed Data Portability Obligations not apply to derived personal data appropriately accounts for the risk to the competitive positions of organisations that might receive requests for Access, Correction, or Portability.

As data portability is intended to support the growth of the digital economy and encourage competition and innovation, the scope of data covered should not undermine those goals. Exclusion of derived data from the obligation is consistent with those aims for data portability. Further, it is important that the definition of "derived personal data" is clearly provided (see response to question 3).

Enabling individuals or organisations to access or modify that same derived data through the Access or Correction obligations would simply undercut the purpose of excluding derived data from the portability obligation, so it is appropriate to extend the exclusion to those obligations as well.