Public Consultation on Review of the Personal Data Protection Act 2012 – Proposed Data Portability and Data Innovation Provisions (Issued 22 May 2019)

Comments from Facebook

3 July 2019

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.

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 now.

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?

Still 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 angle, 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 –

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"?

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.

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.

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

PDPC's proposal for handling data portability requests (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.

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?

As PDPC proposes 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) (2.47-2.48), 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.

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?

The proposed powers (2.47) 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, and how PDPC would undertake such a review.

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?

Here, PDPC's proposal (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. <u>How should organisations protect privacy while enabling portability?</u> Does the transferring party bear any responsibility if an individual ports his or her 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 practice 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 practice 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 practice could also provide users with at-a-glance information about the practices 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?

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"?

PDPC proposes (3.12) 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 (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.

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.