Personal Data Protection Commission
460 Alexandra Road
#10-02 PSA Building
Singapore 119963

PDPC's Public Consultation on Approaches to Managing Personal Data in the Digital Economy

Google would like to thank the Singapore Personal Data Protection Commission ("PDPC") for the opportunity to provide comments on its review of the Singapore Personal Data Protection Act ("PDPA") in respect of the collection, use and disclosure of personal data, and the considerations on the need to introduce mandatory data breach notification requirements.

2 Google supports a flexible regulatory framework that can respond to a rapidly evolving technology landscape, while providing guidance to the industry on how to ensure that users have standard levels of privacy and security throughout the technology ecosystem. In this regard, we are encouraged by the PDPC's recognition of the value that data driven innovation can bring to society and the participatory, proactive role organisations can play in safeguarding individuals' personal data.

Enhanced Framework for Collection, Use and Disclosure of Personal Data

3 The PDPC has rightly observed that the current consent-based approach to data protection faces challenges in the changing digital economy. The public consultation document noted, for instance the dangers of "consent fatigue" and the difficulties for individuals to exercise "meaningful" consent.

4 It may be useful to note the ability for individuals to exercise "informed" choice is also dependent on the whether they have access to sufficient information, presented in a user-friendly way, to make decisions about their relationship with organisations. The best indication of an "informed" choice might be expressed when individuals interact with mechanisms such as account settings, regardless of whether they make adjustments or accept the default settings.

5 Google's transparency and control tools are a good example of how to offer meaningful choices that users can modify over time. Google has long been committed to being transparent with our users about what data we store, and we offer settings that empower our users to control how this data is collected and used. We continue to improve the tools we offer to our users. One example is Google's Dashboard (available at https://myaccount.google.com/dashboard), which allows users to review the data collected by our products and make changes to their privacy settings, all in one place. From the Dashboard page, a user could review her Google activity in the last month, see how many emails, documents and photos she has, and get answers to questions by discovering links to relevant help centre articles. Launched in 2009, we have updated the Dashboard through the years to keep current with Google's products and user expectations. We have also added tools over time to help users make meaningful choices about their privacy, and these have proven very popular. For example, since we launched Privacy Checkup[1] in 2015 (a simple tool for controlling your data across Google

[1] https://myaccount.google.com/privacycheckup?pli=1

and updating the personal information you share and make public), tens of millions of Google users around the world have used it to adjust their privacy settings.

6 Additionally, it could be helpful to consider the inevitable evolution in consumers' interaction with devices, and how that would impact the consent- or notification-based approach to personal data protection. For instance, users in Singapore are tech-savvy and often the first adopters of new technologies. As voice-enabled devices become increasingly available and popular, we can expect the volume of human-to-device vocal interactions to rise in Singapore. In this new landscape where "audio" replaces "text" as the default mode of communication, a consent-based (or even an overly-prescriptive notification-based) approach to every collection, use or disclosure of personal data would potentially be difficult to implement while maintaining a positive user experience. It is hard to imagine that users would find it helpful to listen to the device recite how their voices would be collected, used or disclosed each time they use their device for a specific function or purpose. Instead, this technology may require innovative methods of providing transparency and choice for users. Overly prescriptive rules may reduce the opportunities to develop new solutions in this context.

Question 1: Should the PDPA provide for Notification of Purpose as a basis for collecting, using and disclosing personal data without consent?

7 While advance notice and consent is often the best method of providing users with the control and safeguards necessary to process personal data, we agree with the proposal to provide "Notification of Purpose" as an alternative to consent. Such an approach would be a practical way to balance data use and data protection in situations where consent would be impractical or counterproductive, while still providing information to the public about their intentions and activities. A strict consent requirement would likely result in a bad user experience, and may even lead to more confusion for individuals trying to understand how their personal data is used. The purposes for the use of personal information can be fluid and change over time as organisations innovate and develop new services. To provide clarity for the user, it would be useful to suggest that the additional/new purposes would have to be compatible or related to the purpose of the collection and use of the personal information. This is a principle that has been documented and described in the APEC Privacy Framework. For example, collecting users' location data to provide a better navigation service might one day also be used to estimate traffic delays or provide information about the best restaurants nearby (in response to the user's query).

8 We also agree with the PDPC's view that the organisation should be left to "*assess and determine the most appropriate form of notification*". Detailed and prescriptive conditions for the notification could increase compliance cost, without necessarily bringing additional benefits to end users. Nonetheless, organisations should, as a best practice, provide users with sufficiently clear and easy to read information about the purpose for the collection, use or disclosure of personal information. Doing so provides more context to users, helping them understand how the information would improve the experience of the service(s), evaluate the options available to them and ultimately make a choice about the relationship they would like to have with the service provider(s). Flexible standards can help ensure that users receive the best information from each service they use, and that companies are incentivized to be innovative in how they present information to their users.

Question 2: Should the proposed Notification of Purpose approach be subject to conditions? If so, what are your views on the proposed conditions (i.e., impractical to obtain consent and not expected to have any adverse impact on the

individual)?

9 We have no comment on the proposal that the Notification of Purpose be subject to conditions, save to note that any such condition should be sufficiently general so as not to defeat the very purpose of having notification as an alternative to consent. The consultation paper itself provides some examples of when Notification of Purpose could be appropriate.

10 While not among the proposed conditions, we do wish to comment on the requirement that organisations conduct a risk and impact assessment, such as a data protection impact assessment ("DPIA"). While undoubtedly well-intentioned, this could present itself as a significant challenge for businesses, given that the scope of a DPIA can potentially be diverse and broad. Additionally, this type of assessment is the most valuable when it is designed to identify the risk of harm. Taking a harm-based approach gives the assessment meaning beyond rote evaluation and process. Singapore has a long tradition of encouraging innovation, and data will continue to play a critical role in advancing economies. Adding process without purpose risks impeding the degree of innovation Singapore has built. In particular, this kind of requirement is particularly burdensome on businesses without a strong background in risk assessment, such as SMEs. Small organisations will struggle to develop an effective or well-scoped DPIA, thus failing to accurately assess the risks of using data (the goal of having a DPIA to begin with).

11 Instead, the PDPC should consider working with the industry to establish best practices that organisations should adopt when relying on the Notification of Purpose approach. Such best practices should outline principles and identify situations where DPIAs would be beneficial and reasonable, and the scope of risk assessments to be undertaken. In this regard, a voluntary mechanism (instead of a requirement) for DPIAs would be appropriate.

12 Further, it might be more reasonable for the requirement for assessment to be tied to the conditions for Notification of Purpose, specifically whether or not the collection, use or disclosure of personal data is expected to have an adverse impact on individuals. This would help limit the scope of the assessment, and help avoid a situation where a burdensome process (obtaining consent) is replaced with an equally burdensome but less transparent requirement (DPIA).

Question 3: Should the PDPA provide for Legal or Business Purpose as a basis for collecting, using and disclosing personal data without consent and notification?

13 We support the proposal to provide for Legal or Business Purpose as a legitimate basis for collecting, using and disclosing personal data without consent and notification. This is aligned with privacy regimes around the world, which generally permit such exceptions to notice/consent requirements. As the public consultation document points out, there are certain circumstances under which the collection, use or disclosure of personal information needs to be conducted without consent and notification. Examples of such circumstances include (but are not limited to) instances where there is the potential of death or serious physical harm to an individual, or where consent or notification would result in a violation of a legal process, or could obstruct a governmental investigation.

Question 4: Should the proposed Legal or Business Purpose approach be subject to conditions? If so, what are your views on the proposed conditions (i.e., not desirable or appropriate to

obtain consent and benefits to the public clearly outweigh any adverse impact or risks to the individual)?

14 We have no specific comments to provide in response to this question, save to reiterate our comments on the mandatory risk and impact assessment requirement.

Mandatory Data Breach Notification

15 We believe that the introduction of a data breach notification framework would help to build and reinforce trust between users and organisations. Users should be assured that their personal information is protected; implicitly, they expect organisations to notify them in instances where a data breach has occurred, including an advisory on the steps users can take to safeguard their data. For instance, users should be notified where appropriate of unauthorised access on their email accounts and be advised on the action they can take (e.g. changing their passwords and enabling 2-Factor authentication) to prevent further unauthorised access.

Question 5: What are your views on the proposed criteria for data breach notification to affected individuals and to PDPC? Specifically, what are your views on the proposed number of affected individuals (i.e., 500 or more) for a data breach to be considered of a significant scale to be notified to PDPC?

16 We understand that, for determining risk of impact of harm to affected individuals, the PDPC intends to issue guidelines on assessing such impact or risk. We suggest those guidelines be subject of a separate consultation process and that the PDPC considers setting out clear guidelines on how they will manage the notifications.

Question 6: What are your views on the proposed concurrent application of PDPA's data breach notification requirements with that of other laws and sectoral regulations?

17 We have no specific comments to provide in response to this question.

Question 7: What are your views on the proposed exceptions and exemptions from the data breach notification requirements?

18 We are supportive of the proposed exceptions and exemptions from the data breach notification requirements. It may be worth pointing out that for data intermediaries such as cloud service providers, the data being held and processed would already be encrypted per industry best practices. In some cases, the encryption keys would be held by the organisation that the data intermediary is processing the personal data on behalf of instead of the data intermediary. This means that the data intermediary would have no insight into the nature, content and sensitivity of the data. In this regard, it is appropriate for that organisation (not the intermediary) to be responsible for complying with the breach notification requirements under the PDPA, as they would have the knowledge to assess harm or scale of impact of the data breach.

Question 8: What are your views on the proposed time frames for data breach notifications to affected individuals and to PDPC?

19 In the event of a data breach, it is crucial for the organisation (be it the data intermediary or the organisation the data intermediary is processing personal data on behalf of) to first identify the cause of the data breach, understand what has taken place, what data are impacted, and start appropriate remedial actions to prevent the breach from escalating. Many would argue that this is as important as the reporting or notification requirement.

20 In the case of the data intermediaries, we note the proposal to require data intermediaries to immediately inform the organisation it is processing the data on behalf of. Given the importance of starting remedial actions and the prevention of further breaches, it may be more appropriate to include a "reasonableness" factor (e.g. notification to be done as soon as reasonably possible) in the requirement. This provides room for data intermediaries to focus on taking remedial action without unnecessarily delaying the notification process. In any case, existing contractual agreements are in place to dictate how expedient the notification process would be.

20 In addition, it may be useful to clarify that a data breach does not include:

- Unsuccessful access attempts or similar events that do not compromise the security or protection of the data (including pings, port scans, denial of service attacks, and other network attacks on firewalls or networked systems); or
- Accidental loss or disclosure of data caused by the organisation's use of the data intermediary's services or the organisation's loss of account authentication credentials.