RESPONSE TO PUBLIC CONSULTATION ON THE DRAFT PERSONAL DATA PROTECTION (AMENDMENT) BILL 2020 ("BILL")

Submitted on: 28 May 2020

We thank PDPC for the opportunity to provide feedback on the planned amendments to the Personal Data Protection Act.

We understand and agree with the need to strengthen the accountability of organisations, enable meaningful consent where necessary and provide greater consumer autonomy. Nonetheless, we strongly believe that these have to be implemented in a manner that is (a) not overly onerous or costly to comply with while also (b) balancing organisations' need to protect their own proprietary information and the privacy concerns of third parties.

Additionally, where legislation requires organisations to make some form of subjective judgment (e.g. in determining 'significant harm', and 'legitimate interest') or rely on exceptions to protect specific interests, more clarity through subsidiary legislation, detailed guidelines, or parliamentary readings which provide more information on the anchor purpose of the legislation, how various interests should be weighed, key factors to consider and examples of scenarios which are permissible or not, would be critical to ensure consistency across the board.

We also request that the industry should be further consulted in the drafting of subsidiary legislation pertaining to Data Portability, given the persisting strong concerns by players from across industries. We had previously highlighted some of these to PDPC in its consultation for Proposed Data Portability and Data Innovation Provisions and further provided more feedback in this submission.

Finally, given the current COVID-19 situation and recession, we would suggest an extended period of 2 years after subsidiary legislation is passed for companies to comply with the regulations pertaining to Data Portability, given that it will be operationally onerous and would require extensive investment and resources to do so.

Our detailed comments are in the appended table.

One part of our submission under the Data Portability section that should be treated confidentially has been redacted should PDPC decide to publicly disclose this document. This part of the submission provides insight into our commercial and product strategy, and is thus commercially sensitive information.

Area of Consultation	Reference	Grab's Comments/Suggestions
Mandatory Data Breach Notification	Paragraphs 13 to 26 of the Consultation Paper; clause 12 of the Bill	**1. Notifiable Data Breaches** Sections 26B(1)(a), and 26D(2), (4) and (5) under clause 12 of the Bill make references to "significant harm" being caused to the affected individual. As this concept involves some form of subjective judgment being passed, to ensure a minimum level of consistency across the board, we request that MCI/PDPC provide more clarity through the parliamentary readings, subsidiary legislation or even a set of guidelines outlining some key factors and examples of scenarios where data breaches not involving the section 26B(2) list of data nevertheless meet the threshold for "significant harm". Examples should ideally illustrate cases closer to the threshold of what would cross the line from a lower level of harm to "significant" (e.g. would the leak of a person's mobile number, personal email address or even email password constitute "significant harm"?). **2. Duty to notify occurrence of notifiable data breach** Section 26D(3) refers to the data breach notification containing certain mandatory information that is to be prescribed. In the absence of the substantive list of such information at this stage, we suggest that this list should not require organisations to provide in-depth information relating to the data breach. This is because internal investigations may still be ongoing (at this relatively early stage) and organisations may not be in a position to provide clear and accurate information to the Commission. There is a tradeoff between timeliness of notifying and having all the details in place. One option, therefore, on the prescribed list of information is to mirror the approach taken by the Philippines' National Privacy Commission ("**NPC**"), which has mandated for their domestic data breach notifications to contain the following list of information: 1. ***Nature of the Breach.*** *– There must be, at the very least, a description of: (a) the nature of the breach; (b) a chronology of events, and (c) an estimate of the number of data subjects affected;* 2. ***Personal data involved.*** *– stating the description of sensitive personal information or other information involved.* 3. ***Remedial Measures****. – there must be: (a) Description of the measures taken or proposed to be taken to address the breach; (b) Actions being taken to secure or recover the personal data that were compromised; (c) Actions performed or proposed to mitigate possible harm or negative consequences, and limit the damage or distress to those affected by the incident; (d) Action being taken to inform the*

		data subjects affected by the incident, or reasons for any delay in the notification; and (e) the measures being taken to prevent a recurrence of the incident. 4. ***Name and contact details.*** *– of the Data Protection Officer or contact person designated by the Personal Information Controller to provide additional information.* Grab submits that the NPC's approach strikes a good balance between timely notification for the regulator to understand basic details regarding the incident, and the lack of confirmed facts from companies at the initial mandatory breach reporting stage. Having a common breach reporting template also assists organisations which operate across multiple jurisdictions to align notification requirements amidst such time-sensitive and resource-intensive circumstances. In addition to the above, the existing practice of allowing organisations to provide a data breach notification with basic information to the PDPC, before following up with more details based on their ongoing internal investigations should continue. Section 26D(7) provides for a situation where the Commission may waive the organisation's notification requirement to affected individuals. We understand that this is meant to cater to exceptional circumstances such as where circumstances involve overriding national security or national interests. We request MCI/PDPC to provide more details through the parliamentary readings, subsidiary legislation or even in a set of guidelines on factors that the Commission may take into account in determining whether organisations may qualify for such waivers. Clarity on this point would assist organisations in assessing the viability and necessity of making such requests, and reduce the volume of unmeritorious requests for waivers. Section 26D(9) states that the organisation's obligation not to notify affected individuals if directed or instructed by either the Commission or another prescribed law enforcement agency does not affect the organisation's obligation under other laws to notify any other person of the data breach or provide information on the data breach. Related to this, we submit that there could be a scenario where a data breach incident falls within the jurisdiction of another regulator in Singapore (e.g. Monetary Authority of Singapore) and requires notification to affected users. If so, our interpretation of this clause is that organisations should go ahead to notify users, even if it complicates PDPC's intent or investigations. We seek confirmation from PDPC that this is the right interpretation and how organisations should resolve any inconsistencies between two regimes. To our minds, organisations should only be required to follow the data breach handling and notification protocols mandated by one regulator, and not be required to comply with two sets of potentially

		inconsistent or duplicative reporting regimes. This would allow organisations to focus their limited resources on investigating and remediating the breach. In the event that MCI/PDPC requires organisations to simultaneously comply with two regimes, legislative amendments should be introduced to clarify how organisations should deal with the inconsistencies (e.g. should organisations notify PDPC of the parallel notifications taking place such that PDPC may provide more clarity in that situation on how the organisation should conduct itself and comply with its notification obligations?). There seems to be a typographical error in Section 26D(2). "Subject to subsections (4), (6) and (7)," should instead be replaced with "Subject to subsections (4), (5), (6) and (7)", as subsection (5) sets out the technological protection exemption to the requirement to notify affected individuals.
Offences relating to egregious mishandling of personal data	Paragraph 30 of the Consultation Paper; clause 20 of the Bill	Part VIIIA makes multiple references to the thresholds of "knowingly" and "recklessly" in determining the culpability of an individual for offences under this Part.[1] We would request for MCI/PDPC to define what these two concepts entail under the PDPA and illustrate these with a couple of examples (e.g. does wilful blindness or "ought to have known" constitute sufficient knowledge such as to make out the *mens rea* requirement under these offences?). As these terms are either defined in other statutes (e.g. "knowingly" under the Penal Code) or used elsewhere (e.g. "reckless" under the Securities and Futures Act), we also request for MCI/PDPC to confirm if we are expected to cross reference to these other statutes and authorities related to them in interpreting these *mens rea* requirements. It would be useful for more clarity on these during the Second Reading of the Bill as a reference point for future cases.
Enhanced framework for collection, use and disclosure of personal data	Paragraphs 38 and 40 to 42 of the Consultation Paper; clauses 7 and 32 of the Bill	**1. Deemed consent by notification** We would request for MCI/PDPC to provide more guidance through the parliamentary readings or a set of guidelines on what it considers a "reasonable period" for an individual to opt out and what it considers a "reasonable manner". We understand that the PDPC has suggested elsewhere that "just in time" notifications can be used when obtaining consent. However, there may be legitimate cases where it may not be feasible to provide "just in time" notifications, or to set out a relatively lengthy description containing the information specified in section 15A(3)(b). In such cases, we would appreciate some guidance on what PDPC would consider to be reasonable, having regard to the constraints that organisations may face in implementing "just in time"

[1] For a discussion on the potential differences between the various criminal *mens rea* thresholds, please refer to https://www.academypublishing.org.sg/Journals/Singapore-Academy-of-Law-Journal/e-Archive/ctl/eFirstSALPDFJournalView/mid/495/ArticleId/632/Citation/JournalsOnlinePDF.

		notifications and the need for apps to be consumer-friendly, and therefore not a suitable medium to contain lengthy disclosures or multiple interruptions in the user journey, which has a negative impact on the customer experience (especially for users who are using the app on-the-go). **2. Legitimate interests** We note that Part 3 of the proposed First Schedule refers to the need to balance the benefit to the public (or a section of it) against the "adverse effect" on the individual. As what is considered an "adverse effect" may be context specific, we request for MCI/PDPC to provide us with some guidance through the parliamentary readings, subsidiary legislation or even a set of guidelines on what would constitute a public benefit that could trump the "adverse effect" on an individual, especially in edge cases. In this regard, we would be happy to collaborate with the PDPC to explore some use cases on how this exception to consent may apply. **3. Business improvement exception and research exception** We note that the proposed exception allows organisations to perform their own data analytics to learn about and understand the behaviour and preferences of their own customers, as well as to develop and enhance their products and services (amongst others). This is an exception to *use* personal data without consent and, presumably, does not extend to the disclosing or sharing of datasets with external organisations. We understand this to extend to the use of data to improve/enhance our services by allowing greater personalisation of content on our platform and services for our users. We seek MCI/PDPC's clarification if this understanding is correct. We further note that the research exception is proposed to be widened and would like to seek clarity on whether organisations may rely on this exception to collaborate with other (commercial) organisations to conduct market research into their common customer base (i.e. the pool of customers that use both organisations' services) to gain more insights about their existing customers. Such research is valuable in allowing organisations to provide more personalised content that better addresses the needs of their users. Currently, a key barrier to this relates to the uncertainty surrounding whether circumstances are such that it is "impracticable for the organisation to seek the consent of the individual for the disclosure". In commercial contexts, while it may be theoretically possible to seek consent, the implementation of such consent seeking may very well be commercially unfeasible (e.g. it may not make commercial sense to start a mass exercise to seek a one-off consent to allow two organisations to share their datasets containing non-directly

		identifying personal data in order to gain some insights into the preferences of their common customer base). We would respectfully submit that "impracticality" also includes the lack of commercial feasibility. This will encourage more data-driven research that will ultimately benefit consumers.
Data Portability	Paragraphs 43 to 52 of the Consultation Paper; clause 13 of the Bill	It is crucial that MCI/PDPC clearly defines the anchor purpose for data portability within the PDPA, which we strongly believe should be focused on providing convenience for users. This is, for example, the benefit of number porting between telcos that PDPC had previously shared as an example of data portability. Clarity in the purpose will facilitate subsequent decisions over the whitelist of data categories that would be included. A broad definition of "user activity data" incorporating the secondary purpose of spurring innovation gives rise to serious concerns given the potential to cause leakage of proprietary information. We would also like to stress the significant efforts, time and costs required to meet the requirements of the data portability regulations, for example, to build new systems and processes. We are concerned that the cost imposed on organisations may outweigh the potential gains for users, especially given that Singapore is in an unprecedented pandemic and only at the start of the worst recession in Singapore's history. These resources could otherwise be used to support other activities critical during this crisis, such as spending to support drivers and merchants, investing in new capabilities to adjust to the new normal. The tradeoffs become more stark when resources are limited. We thus request for at least a two-year sunrise period to afford organisations the time and resources to implement the necessary requirements, as well as prepare for economic recovery. Our further detailed concerns and comments are stated below: 1. <u>Leakage of proprietary and confidential commercial information</u>: We strongly urge MCI/PDPC to scope the 'whitelist' of "user activity data" to focus only on enabling the data subject to obtain an adequate experience in "switching" service providers. If MCI/PDPC nonetheless proceeds, we seek confirmation that we may rely on the exception for confidential commercial information to avoid disclosure and porting of data which may reveal proprietary information. Without adequate safeguards and clarity on what needs to be ported, the definition of "user activity data" can potentially lead to the unintended effect of disincentivising innovation; later players to the market may simply free-ride on the investments of the first mover by reverse engineering the ported datasets that have been obtained through years of investments.

		Transaction metadata which may fall within the definition of "user activity data" can include proprietary attributes that we consider to be our trade secrets. [redacted] 2. Privacy concerns**:** We note that the proposal is for user activity data to be made portable, and that the consent of a third party is not required to be obtained when fulfilling this data porting request. Grab is a multi-sided platform used by passengers, users, drivers and delivery riders alike. By allowing the personal data of a third party to be ported without his/her consent, potential privacy/harassment issues may arise. To cite an example, in the case of a GrabHitch driver (i.e. a social service) trying to port his activities over to a competing platform, he may opt to port the details of the person hitching a ride from him (as this is considered user activity data) which may include the name (as registered with Grab) and addresses (via pick-up and drop-off points) associated with people hitching a ride with this individual. The requirement for the porting to be done in a personal and domestic capacity will not exclude such porting. While Grab conducts due diligence over the individuals providing the GrabHitch service to ensure the safety of the community, it is not unfathomable that the ability to associate an address with an individual and being able to port this over to another service may increase the risks of harassment or breaches of privacy and safety. Outside of the Grab framework (e.g. Code of Conduct, contractual restraints, suspensions), there is no way of sanctioning any anti-social behaviour arising from such porting. Similar concerns may arise in respect of users who request to port their user activity data to alternative service providers. Indeed, it is precisely due to this concern that our systems currently limit what our users, riders and driver can view in respect of past services rendered (e.g. for GrabFood, users are no longer able to see their delivery riders' details beyond 72 hours). We understand that there is currently no need to provide access or porting of data if the data "can *reasonably be expected to threaten* the safety, or physical or mental health,

		of an individual other than the individual to whom the applicable data relates" ("**Safety Exception**"). This is a non-negligible general risk for firms but it may not be "reasonably expected" in a specific case (i.e. organisations are often not in a position to know or judge whether a particular person requesting for the porting of his data is planning to harass the third party individual whose personal data is being ported along with his, but the danger of harassment can be borne out of their analysis of general trends on their services). Given that organisations are subject to high levels of risk, our preference is therefore to be more conservative about who we disclose the data to. To this end, we submit that organisations should be allowed to reject porting certain types of data if there are such non-negligible risks. It would also be useful to have clear guidelines containing examples to illustrate the execution of when organisations may rely on the Safety Exception. Should organisations be required to port data that they consider to potentially give rise to safety risks, we seek MCI/PDPC's express confirmation within the PDPA that organisations will have immunity against follow up legal actions arising from their compliance with the data portability obligation. 3. <u>Inability to assess capacity from which porting requests emanate</u>: We note that data portability is meant to cover only requests made in the requester's personal or domestic capacity. While this may typically be straightforward in the case of our passengers or consumers, this is not so for our other user bases; in the case of Grab's drivers and delivery riders, it may not always be the case that these individuals are performing services with the main aim of earning a living. Some may be doing these activities casually, with the side benefit of earning some money. For such individuals, Grab has no way of determining if their data porting requests arise from a personal or domestic capacity and it would not be scaleable for us to assess this aspect on a case by case basis. As such, it would be helpful to understand how far organisations are expected to go to discharge the obligation and satisfy themselves that the request is made in "P's personal or domestic capacity" as proposed in Section 26H(2)(a). For instance, would an express declaration or ticked check-box by the data subject to this effect in his porting request suffice, or even a blanket rejection of such requests arising from B2B products or features? Are organisations expected to fact check the capacity that P is

		acting in with the receiving organisation to confirm he is indeed only acting in a personal or domestic capacity on both ends? This would, however, be onerous to implement on a large scale, and also counterintuitive since it involves the collection of additional information and data about P just to give effect to his data portability request. Given the above, we would propose that only "first level" user activity data be made portable, namely: 1. Transaction date (in UTC format) 2. Transaction time (in UTC format) 3. Transaction currency (currency code) 4. Transaction value This will help receiving organizations calculate aggregates (such as transaction frequency, cumulative spend, purchase behaviour, etc.) to support the porting users with a relevant experience. 4. Complex and onerous to extract unstructured data: We strongly suggest that unstructured data (e.g. text, click logs) should be excluded from the scope of "user activity data" as the effort to comply through structuring and processing this data would be incredibly onerous.
Increased Financial Penalty Cap	Paragraphs 58 to 60 of the Consultation Paper; clause 17 of the Bill	Some clarity on the definition of "annual turnover exceeding $10 million" within the Act would be appreciated. Would this turnover be limited to turnover in Singapore only, or the organization's global annual turnover?
Referrals to Mediation	Paragraph 68 of the Consultation Paper	We suggest that guidelines should be shared on when parties will be referred for mediation, taking into account the need to deter frivolous claims brought forth by individuals given the time and resource to engage in these could become excessively onerous.

Prohibitions to Providing Access	Paragraph 74 of the Consultation Paper	We understand that the PDPA seeks to strike a balance between data protection and commercial realities; and the current set of proposed amendments are aimed at resolving existing issues faced by organisations in implementing the access obligation where they are required to give access to personal data containing the personal data of third parties as well. We are concerned that the proposal to give individuals access to (or allowing them to port) their user activity data, despite such data containing personal data of individuals who did not consent to such disclosure, may be tipping the balance overly in favour of giving access at the risk of third parties' privacy. Based on the proposed definition of "user activity data", this could be wide enough to include in-vehicle camera footage and CCTV footage which may contain sensitive information. As an organisation, we wish to be able to mask or withdraw the personal data of our employees, users and independent contractors to protect them from abuse and unnecessary exposure. Given the prevalence of video clips and audio clips going viral over social media platforms, the removal of the need to redact personal data or obtain the consent of third parties featured in such clips, raises potential privacy and doxxing concerns. Similar to what we have raised under our comments on data portability above, we would be grateful for clarifications from MCI/PDPC in the course of parliamentary readings, subsidiary legislation or even a set of guidelines outlining whether organisations can rely on the Safety Exception to reject porting/access requests if there are non-negligible privacy and doxxing-related risks. Finally, we wish to confirm that organisations would be allowed to recover any incremental costs in order to respond to such access requests per the status quo.
Other miscellaneous issues	Clause 2 of the Bill	**1. Derived personal data** We note that the definition of "derived personal data" is wide enough to cover insights that an organisation has gained over this individual, including those that the organisation has independently enriched using its own proprietary logic and systems (which are potentially capable of disclosing our confidential and proprietary logic and strategic focus). While we do not disagree with the need to give access to individuals to some level of derived personal data about themselves (e.g. our high level understanding of their preferences, such as "Person X likes bubble tea"), we are concerned about the extent of derived personal data that is required to be disclosed especially if such data is in an unstructured form, has been enriched by our own proprietary

		systems, or if the derived personal data may contain commercially sensitive and confidential information (e.g. one may be able to reliably estimate what the strategic focus of the business is by looking at its approach when profiling an individual for marketing purposes). It may also be commercially impractical (having regard to the costs involved and the extent of the undertaking) to gather and provide access to unstructured data. We therefore request that MCI/PDPC clarify the extent of "derived personal data" that is subjected to the Access Obligation through subsidiary legislation or even in a set of guidelines, in particular the level of granularity that is expected. We submit that derived personal data should only consist of structured data that will not reveal any commercially sensitive and confidential information (such as information that reveals the strategic focus on the organisation in conducting its marketing/profiling activities.)
	-	**2. Personal and domestic capacity** As mentioned above, practical issues surround the implementation of data portability and how organisations can determine if the data subject's request arises in their personal or domestic capacity. More generally, what constitutes "personal" and "domestic" such that a particular collection, use or disclosure of personal data is outside the scope of the PDPA remains uncertain. We request that MCI/PDPC take this chance to clearly define these terms so that organisations and individuals can be guided by it.