# Response to Public Consultation on the Review of Personal Data Protection Act 2012 - Proposed Data Portability and Data Innovation Provisions

While we agree that data portability can provide some benefits to consumers and businesses, we believe that a broad legal obligation to ensure data portability can also be abused and hamper market development.

In this regard, we recommend for the PDPC to further clarify the objectives it is trying to achieve with this requirement, and also consider if it can (a) achieve these objectives outside of legislation, for example, through working with industry to develop sector-specific voluntary standards and partnerships; and (b) share if there are specific sectors and types of data in which there are concerns (for example, from a market failure or competition perspective), to which further consultations and work can be targeted at.

Our detailed concerns with the proposed provisions are outlined in the confidential Annex. We request to be consulted if the PDPC would like to share this information with third parties.

ANNEX

| Area | Paras | Comments |
|---|---|---|
| Scope of Data Covered | 2.24 to 2.26 | We have concerns that the requirement to convey "user activity data" will erode the investments made by existing market players.<br><br>Investments have been made to instrument for, digitise, collect and store user activity data. Transferring such data resources to other commercial entities can allow other entities to improve their competitive advantage despite not putting in the investments. This reduces existing players' incentive to innovate.<br><br>In addition, some forms of user activity data can be used to obtain insight into companies' operations, algorithms, business partners, and pricing strategies. We suggest that these be considered commercial confidential information that are excluded from the data portability obligations. We would suggest for further discussions on the types of user activity data that should be shared. |
| Scope of data covered - Business Contact Information | 2.31, 2.35 | Given the limited definition of BCI, the cost of setting up portability for BCI exceed the potential benefits to individuals. BCI should be excluded from portability requirements. |
| Scope of data covered - personal data of third parties | 2.32 to 2.33 | We seek clarification if there are additional obligations for porting organisations to obtain consent from third parties.<br><br>We also seek confirmation that the receiving organisation should be able to ingest the data without any further need to seek consent from the third party. |
| Handling data portability requests & receiving ported data | 2.39 to 2.43 | As the porting of the data is triggered by a user request, one option is for the porting agency to provide the data to an individual directly, instead of to the receiving agency.<br><br>This provides a clear milestone where the obligations of the porting organisation agency ends, and allows for the porting agency to better estimate the associated compliance costs and cost of providing the service. The current proposal places a disproportionate burden on the porting organisation (viz. the receiving organisation) for compliance. |

| | | |
|---|---|---|
| | | In addition, current business processes are built around access and correction requests. As such, we suggest that the 7 day period should be aligned with the current 30-day period for access/correction requests. |
| Handling data portability requests & receiving ported data | 2.39 to 2.43 | If we must ensure the transmission of the data to the receiving organisation, we suggest for greater clarity and a set of guidelines on the obligations of porting and receiving organisations with regards to data protection and data security.<br><br>For example, we suggest to make clear that the porting organisation should not be under any due diligence obligation in regard to the ability of the receiving organisation to provide adequate protection of data. The porting organisation should also not be under any obligation to assess if consent had been obtained by the receiving organisation so long as the individual's instructions are clear. The porting organisation should also not be penalised if the individual uses the data outside of personal and domestic purposes.<br><br>It is unclear which party is responsible for data security when it moves between services. Furthermore, the receiving organisation may "choose not to accept the data or retain only a portion of the data", though a fuller set of data would have already been transmitted.<br><br>While Grab is confident in our data security capabilities, we are concerned that receiving organisations may not be able to protect our customer's information as securely. Any data leakage in the data porting process would compromise user privacy and pose a reputational risk to Grab. |
| PDPC power to review | 2.49 | PDPC should also review failure of an organisation to provide data in accordance with a Code of Practice, or in a commonly-used machine readable format. |
| Codes of Practice | 2.51 | We welcome PDPC's proposal to introduce sectoral codes of practice. This could include a "whitelist" of data for which portability should be enabled, that is determined via consultation with industry players. The codes can also outline that would be considered a machine readable format. We also seek confirmation that the intention is for the Codes of Practice to clarify and prescribe the specific data that will be subject to portability requirements.<br><br>In addition, we suggest for specific mechanisms to identify organisations covered by particular Codes of Practice. This will allow data transferors to identify other organisations operating with similar |

| | | |
|---|---|---|
| | | practices and thereby ease data flows. |