Response to PDPC Public Consultation on Data Portability and Data Innovation Provisions (DBS – 12 July 2019)

Key Feedback

1. The financial sector is very complex and there is potential for many unintended consequences if we adopt broad portability. There is a need to be led by sector specific policy to complement overarching policy. Standards and requirements should also apply to activities instead of just entities. For instance, if a parallel (to banking) industry player decides to offer payments as a service, their activity should be subjected to the same data standards and requirements in the code of practice for financial sector.

2. The considerations proposed in the paper are tilted heavily towards the rights of individuals. There should be a better balance of interests between the rights of individuals and companies, and consequences to society. While conferring rights to individuals on data portability, the policy should also seek to educate individuals and safeguard their interests with respect to potential abuse of their data that could arise under the framework. It is inadequate and perhaps inappropriate to rely on sending organisations to serve as the policing mechanism. Many may lack the sophistication, resources and desire to do so. Steps should also be taken to prevent the misuse of data by receiving organisations who may incentivise individuals to port data from other organisations.

3. The broad scope of in-scope data and onerous requirement on the operational due diligence (required of sending organisation) not only creates an unlevel playing field between incumbent organisations and 'new-to-market' organisations, but also significantly increases the cost of compliance and at the same time widening the surface area of cybersecurity attacks.

4. There should be a recognition that many user activities data are co-owned with the organisations who set up the entire infrastructure to capture, store and manage the data (e.g. banking and credit card transactions) which otherwise may not exist. An individual may not have the sole ownership right to request such data to be ported.

5. DBS also proposed for certain categories of Personal Data (e.g those relating to a corporate relationship) and user activity data (e.g information used for authentication purposes, information containing Personal Data of another individual) to be excluded, and for the historical time period for data portability to be limited to 1 year for relevancy of information.

6. DBS supports the proposed provision on Data Innovation.

DBS

Q1. What are your views on the impact of data portability, specifically on consumers, market and economy?

PDPC Requirements	Key Points
• (1.4) provides consumers more choice and control over their data held by organisations. When consumers are able to move their data easily from one service provider to another, consumers are better empowered to try out or move to new or competing service offerings that may better suit their needs. • (1.4) positive impact on the growth of the Digital Economy by enabling greater data flows which support data innovation.	We propose that impact be holistically assessed from four angles, namely perceived benefits (vs reality); risks; costs; and future investment appetite- 1. **Perceived benefits vs reality** – There is a lack of empirical support that (i) competition is being held back due to lack of data portability nor (ii) of significant potential benefits on to consumers, market and economy: • Singapore, similar to other countries, already have in place the PDPA to enable requests for personal data (Access Obligation). However, the number of people who actually access their own information is very small. There is evidence in place that this is a pre-existing right that virtually nobody uses; • Competition, particularly in the Singapore financial services industry (e.g., deposits, credit cards, mortgages, investment products), is not held back by lack of data portability; no studies support otherwise; • There is little incremental benefit to establish an additional data portability regime for financial institutions – there are already well-established, structured mechanisms to enable such financial data flows / transfers such as MyInfo, Credit Bureaus and FPDS (upcoming); 2. **Risk** - data flows between organizations widen the attack surface on cyber security. Uneven levels of maturity & scrutiny between sending organisations and receiving organisations pose new challenges to privacy and information security: • Enabling transfers of highly sensitive financial services data – even within the heavily regulated financial services industry – increases data leakage exposure, potentially leading to identity theft or fraud risk; • Enabling transfers of financial data outside the industry increases data exposure risks significantly due to differing data security standards and level of scrutiny / enforcement among different industries; • Increased risk of misuse of data by receiving organisations who may incentivise individuals to port data from other organisations. 3. **Costs** – Requirements add significant costs to comply and administer, particularly for the financial services industry that has rich and varied datasets which ultimately will be borne by a large proportion of customers who will not benefit materially from these portability requirements; 4. **Future Investment appetite** – Investment in business transformation, innovation and competitiveness may be negatively impacted over the longer run as effort to innovate, build and serve at scale will be undercut by players which would not undertake nor cannot recoup the necessary investment (compliance cost). In summary – a legislation mandating data portability, if not well thought through across the dimensions, may be of limited benefit to consumers, the market or the economy in return for increased risks and costs.

Q2. What are your views on the proposed Data Portability Obligation, specifically – a) scope of organisations covered; and b) scope of data covered?

PDPC Requirements	Key Points
• (2.16) proposed Data Portability Obligation will apply to any organisation that collects, uses or discloses personal data in Singapore, • (2.16) Organisations will not be required as a matter of compliance with the proposed obligation, to transmit data to overseas receiving organisation • (2.24) apply to data that is provided by the individual to the organisation ("user provided data"); and generated by the individual's activities in using the organisation's product or service ("user activity data")	Scope of Organisations covered: 1. The proposed legislation understandably encompasses a wide span of industries (both highly regulated and less regulated) which differ significantly in terms of the types of data assets, sensitivity and implications, and data protection standards, this results in a unlevel playing field amongst the different sectors. Propose to limit data portability requests to within the same industry sector. Scope of Data covered: 1. Proposed scope of data covering –"user provided data" and "user activity data" is overly broad. a. Propose these "user provided data" to be excluded: i. Data that had been collected for identity authentication purposes (e.g. signature, voice biometric) so as to minimise the risk of identity theft. ii. Data that does not originate from the sending organisation even though it is user provided data e.g. Marriage certification, educational certificates, so as to minimise reliance on the sending organisation as a record/ data repository b. Propose recognition that many user activities data are co-owned with the organisations who set up the entire infrastructure to capture, store and manage the data (e.g. banking and credit card transactions) which otherwise may not exist. An individual may not have the sole ownership right to request such data to be ported. c. Propose these "user activity data" to be excluded: i. Observed data obtained from recordings and images potentially contain personal data of third parties and often not practical to segregate the individual ii. Data involving an organization's employees. E.g., call logs that record conversation between the customers and staff can contain personal information about both the customer and the staff. And it is often not practical to segregate the two. Similarly, user activity data generated during an employee's course of work (e.g emails, system usage logs) should be excluded since this information belongs to the bank and not the individual employee. 2. More definition is required for "personal data of third parties" in data portability request from individuals in scenarios of a. Joint relationship i. Joint account relationship (single to sign and two to sign) ii. Portability request is made by supplementary cardholder on main account transactions b. Estate management, whereby DOA execute portability request for the deceased 3. Proposed for scope of data to exclude employee records as there are established market practice for employment / reference checks. There is minimum incremental benefits to establish a legal framework for porting employee records. 4. The proposal also does not specify any limit on time period of "user activity data". Scope should take into account that certain historical data are kept according to regulations – e.g., Companies Act, Banking Act, Income Tax Act, Corruption, Drug Trafficking. However, for historical data that we store, we will provide only those that are 'online' and easily accessible instead of those that are kept on tape backup, because it is too costly and time-consuming to retrieve the latter. The data retrieval cost even if picked up by receiving organisations (as fees that we charge) will eventually be priced by them into the products/services for the customers. To prevent cost escalation, we propose 1 year of data history to be made available to customers. 1 year is sufficient to form behavioural trends and anything beyond might have limited benefits of recency. 5. We also propose for data portability requests to be limited to situations whereby an individual had established a business relationship with the sending organisation, and as such, requests for information relating to 'unsuccessful/ rejected' or "pending" applications for products and services should be excluded.

Q3. 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 Requirements	Key Points
• (2.27) PDPC is proposing to provide for a similar exception for data which, if disclosed, would reveal confidential commercial information that could harm the competitive position of the organisation. • (2.27) This is not intended to affect general competition in the market, but to protect first movers who bring to market an innovative product or service from unfair competition by fast followers. • (2.28) PDPC refers to new data that is created through the processing of other data by applying business-specific logic or rules as "derived data". • (2.29) Data Protection Provisions of the PDPA do not apply to BCI, it is proposed for such information to be covered under the proposed Data Portability Obligation as BCI is provided by the individual to facilitate business activities, allowing individuals to port his or her data supports this objective of promoting business activities. • (3.13) Derived personal data enriches the information that an organisation has about an individual. Where personal data is used for the creation of derived personal data for business innovation purposes (i.e. for operational efficiency and service improvements; product and service development; or knowing customers better),	Agree that "commercial confidential information" and "derived data" should be excluded from the scope. However, given the wide range of data, it is essential to consider other exceptions as well. Propose below exceptions to be included in Annex B- 1. Data sourced from third parties pursuant to commercial arrangements entered into by the bank, or data acquired in mergers and acquisitions. 2. Information about an organization's product / services at a granular level in "user activity data". E.g., type of card in credit card spend history. Such information reveals performance of organization's products/services which can be used by competitors to emulate our strategy. They should be considered as "commercial confidential information". 3. Information about third parties in "user activity data". Although it is discussed in the paper, the quoted example does not sufficiently represent most scenarios. Other examples are, payee information in fund transfers; merchant information in card transactions. Such information can either be personal data or "commercial confidential information". 4. Information of transaction activities contributed by an individual for business purposes (e.g. corporate internet banking transactions executed by individual) should be excluded as such "user activity data" relates to the corporate relationship with the organisation and does not belong to the individual. Such information should be considered as "commercial confidential information". Similarly, any Business Contact Information (BCI) provided by an individual in a corporate relationship capacity should be excluded. 5. Any forms of system log / clickstream data. Even though these are generated by user activities, such data is captured in relation to an organization's systems/processes which are proprietary to the organization. It is often operational in nature and used for internal monitoring, process improvement and audit trail purposes. In this regard, such data should be considered as "commercial confidential information". Moreover, such data will not be relevant to the receiving organisation as it relates to customer journeys/processes specific to the sending organisation.

Q4. What are your views on the proposed requirements for handling data portability requests?

PDPC Requirements	Key Points
• (2.37a) Receiving the request – The organisation must provide an avenue for individuals to submit requests for data porting, • (2.37b) Verifying the request – Upon receiving a data portability request by an individual, the porting organisation must ensure the veracity of the request • (2.37c) Verifying the data to be ported – Before the organisation ports the data, the porting organisation should allow the requesting individual to view the data before transmitting it to the receiving organisation. The requesting individual may remove data that he or she does not wish to port • (2.37d) Porting the data – Following verification of request and individual's confirmation of the data to be ported, the porting organisation must provide the following information to the individual: fees payable by the requesting individual, if any, for the porting; when the data will be ported to the receiving organisation. • (2.37e) Format for porting data – Given the wide range of types of data that could be processed by organisations, PDPC will not prescribe the data formats that an organisation should adopt for transmitting data • (2.37f) Informing the individual of a rejection – Where the organisation rejects a data porting request (e.g. it does not hold data of the individual that is covered by the requirement, or an exception applies), it must inform the individual as soon as practicable of the rejection and the reason for the rejection. • (2.39) Where the data is irrelevant or excessive in relation to the product or service that it provides to the individual, it may choose not to accept the data or to retain only a portion of the data.	1. As part of administration, data portability requests require building a workflow from the initial request to transmitting of data to the receiving organisation. Other than the cost to comply and administer, the workflow is required to incorporate feasible lead time for individual to review, access and correct and having a "cooling off" period. The proposed 7 calendar days in which sending organisation should port the data as prescribed in Annex A is not a feasible lead time taking into considerations the activities from request to porting and long weekends. Note that the 7 days as described in 2.37(d)(ii) is from confirmation of data which differs from Annex A, from receipt of request. 2. There should be a clear liability framework in place in the relationship between "individual", "sending organisation" and "receiving organisation" e.g., receiving organisation must ensure the veracity of data requested to be ported commensurate to the purpose of service / product that is offered to the individual. To this end, use cases will help in better understanding these considerations. These can be first developed within vertical industry segments before extending them to cross-industry sectors applications. 3. Stepping back, there are already SG Govt initiatives e.g. MyInfo, MyInfo Business; where information of individuals and corporations are available to organizations through SingPass or CorpPass. Entrenching these as central repositories of information to be drawn upon (including enabling their corrections/updates) instead of porting the same via different organizations, will be a better approach to preserve the integrity of the underlying data and minimize the proliferation of silo data sources as well as data quality issues permeating through the system. 4. Data to be ported should be in a structured format as prescribed by sending organisation especially in user activity data e.g. transactional activities. From a cost, operational and data authenticity perspective, it is not feasible to a. allow individual to request for/ customize the data to be ported e.g. remove specific transaction data b. allow receiving organisations to customise the format for the data to be ported. i.e indicate the specifics type and structure of data to be received 5. When sending organisation received a request to correct personal data (under PDPA's Correction Obligation), section (22.2.b) of the Correction Obligation should not apply for sending organisation to inform receiving organisation that there is correction on the data that was previously ported, as receiving organisation in itself is a data controller. Individual should contact receiving organisation for any correction of personal data. 6. Ported data that is deemed irrelevant or excessive data received by the receiving organisation may not (or cannot be) purged. As such, such 'unused' ported data should be subjected to the PDPA's Protection Obligation and Retention Limitation Obligation as it is in possession of the receiving organisation.

Q5. 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?

PDPC Requirements	Key Points
• (2.47) PDPA will provide for PDPC's powers to review an organisation's: (i) refusal to port data; (ii) failure to port data within a reasonable time; and, (iii) fees for porting data • Would provide the necessary regulatory safeguards and recourse to protect consumers in the exercise of their right to data portability	1. The basis in which 'reasonable' fees is determined is not clear and risks creating an inherent bias between larger incumbents vs newer, smaller competitors – influencing the flow of data and ultimately competitiveness. We request PDPC to provide more guidance on fees, perhaps leveraging the information from other jurisdictions where data portability is already in place. Reasonable fees has to be assessed in relation to the complexity and legacy of platforms and systems, and efforts required to generate the requested data to be ported, and will vary between organisations. 2. The net flow of data will decidedly be biased against incumbents. With the ability to source data cheaply by leveraging on incumbent players, newer entrants may focus through a narrower set of activities, leading incumbents to eventually withdraw essential but less-profitable services (or increase prices for these services), impacting financial inclusion.

Q6. 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?

PDPC Requirements	Key Points
• (2.49) proposing to introduce the power for PDPC to prescribe binding codes of practices for data portability that may apply to organisations in specific clusters or sectors. • (2.49) codes of practices will be issued as subsidiary legislation under the PDPA and will be legally binding. • (2.49) PDPC intends to develop these codes of practice in consultation with the relevant sector regulators and industry stakeholders. • (2.49) Matters to be prescribed include the following: Consumer safeguards; Counterparty assurance; Interoperability; Security of data.	1. Confidence in the reliability and security of the underpinning technical infrastructure will be critical for success. This is in particular given the extent of identifiable information shared coupled with recent incidents of data breaches. We propose instead for PDPC to set out or consult on proposed technical specifications, including security management requirements, cryptography standards, sessions logging etc. This will ensure consistency across organizations and sectors and in turn, promote the confidence of requesting individuals, sending organisations and receiving organizations. The aspirations of data portability can only be as strong as its weakest link. 2. We also propose for PDPC to ensure alignment of codes of practices across clusters or sectors for cross cluster/sector data porting to eliminate variances in practice between clusters or sectors e.g. those that are highly regulated versus those that are not/ less regulated. Independent audits/checks should also be mandated on both sending organisations and receiving organizations, including the ramifications when not meeting these requirements e.g. barred from participating in data porting. These will help reassure the robustness of any established data porting infrastructure. 3. Additionally, the financial sector is very complex and there is potential for many unintended consequences if broad data portability is adopted. We agree that there is a need to be led by sector specific policy to complement overarching policy. However, standards and requirements should also apply to activities instead of just entities. For instance, if a parallel (to banking) industry player decides to offer payments as a service, their activity should be subjected to the same data standards and requirements in the code of practice for financial sector. In this regard, an industry work group set up by MAS and ABS is in place for Financial Planning Digital Services ("FPDS"). We propose that the principles and considerations for FPDS be the basis for data portability code of practice in the financial sector. 4. If employment records remains in scope, there should be a corresponding code of practice for employment records that applies across all clusters or sectors.

Q7. 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?

PDPC Requirements	Key Points

• (3.3) For the purposes of:
  • Operational efficiency and service improvements
  • Product and service development or
  • Knowing customers better
	Agreed, and we would like to further propose for "Risk Management" to be included as one of the purposes for data innovation.

Q8. What are your views on the proposed definition of "derived data"?

PDPC Requirements	Key Points
• (3.12) Data that is created through processing of other data by applying business-specific logic or rules as "derived data"	The given definition of derived data rests on the assumption that business-specific rules must be applied in order to derive data. Many AI based solutions derive data and insights without business-specific rules being applied. In fact this is one of the key factors in differentiating between AI and non-AI solutions as inferred in the PCPC 'Proposed Model Artificial Intelligence Governance Framework'.

Q9. What are your views on the proposal for the Access, Correction and proposed Data Portability Obligations not to apply to derived personal data?

PDPC Requirements	Key Points
• (3.16) Organisations need not, upon the individual's request, provide the individual with derived personal data, nor correct derived personal data about the individual that is in the possession or under the control of the organisation • (3.17) Required to provide the individual information about the ways in which the derived personal data has been or may have been used or disclosed by the organisation within a year before the date of the request. • (3.18) Develop a standard list of all possible third parties to whom the derived personal data may be disclosed and provide information on the purposes rather than the specific activities for which the derived personal data had been or may have been used or disclosed.	Derived data should be excluded from Access Obligation (PDPA Section 21) of PDPA in totality and not in parts because notification of its usage or disclosure (in the past year to other organisation) may compromise an organisation commercial position or such data are proprietary in nature e.g. customer internal (credit) risk scores based on bank's assessment.