RESPONSE TO CONSULTATION PAPER

Respondents should organise their submissions as follows:

a) Cover page (including their personal/company particulars and contact information);
b) Summary of major points;
c) Statement of interest;
d) Comments; and
e) Conclusion.

Supporting materials may be enclosed as an annex to the submission.

7 All submissions should be clearly and concisely written, and should provide a reasoned explanation for any feedback. Where feasible, please identify the specific provision of the draft PDP (Amendment) Bill which you are commenting on.

8 All submissions should reach MCI/PDPC no later than **5pm on 28 May 2020**. Late submissions will not be considered. Submissions are to be in softcopy only (in Microsoft Word or PDF format). Please send your submissions to DataRegulation@mci.gov.sg, with the subject "**Public Consultation for the PDP (Amendment) Bill**".

a) Cover page (including their personal/company particulars and contact information);

Consultation topic:	Public Consultation on PDP Amendment Bill
Name[1]/Organisation: [1]if responding in a personal capacity	Deutsche Bank A.G., Singapore Branch
Contacts for any clarification:	Yan Peng Ong (yan-peng.ong@db.com) +65 64234074 Richard Lee (richard-a.lee@db.com) +65 64237016 Sumitraa Srinivasan (sumitraa.srinivasan@db.com) Jiali Liu (Jiali.liu@db.com) +65 64235979

b) Summary of major points

Deutsche Bank is supportive of the proposals by the Personal Data Protection Commission (PDPC) and the Ministry of Communications and Information (MCI) to update the Personal Data Protection Act 2012 (PDPA) to reflect increasing and new uses of data driven by developments in technology. The revisions to the consent framework and introduction of data portability will spur innovative applications of data to develop new and improved products and services, to the benefit of organisations and consumers.

The PDPC's move towards a more risked-based accountability approach also enables organisations to adopt common frameworks and international standards to demonstrate accountability in protecting the personal data of consumers, in an increasingly sophisticated landscape of cyber threats.

We would like to take this opportunity to clarify requirements in the proposed amendments and set out our position so that PDPC can take these into account in prescribing further regulations. Deutsche Bank also welcomes the PDPC's intention to further consult with the industry and relevant sector regulators to develop these requirements.

c) Statement of interest

As a financial services provider with a global network, Deutsche Bank recognises the value of data as an intrinsic part of business activity and data-driven innovation will be a critical lever for economic competitiveness. The role of regulatory data frameworks to enable cross-border data flows and cross-sectoral data sharing cannot be overstated, and this is supported by measures taken by PDPC and the Monetary Authority of Singapore (MAS) with respect to opening up data regimes. The PDPC's proposals to facilitate data-sharing across relevant sectors are key to unlocking wide economic benefits for both businesses and consumers while ensuring a level playing field.

The development of data sharing mechanisms to provide appropriate security and standardisation will address key challenges to safe and effective operationalization of the data portability obligations. We welcome the PDPC's approach to work with the industry and sector regulators to set out the scope, processes and standards to guide implementation.

The regulations and technical requirements, once in place, should provide ample time for organisations to implement requirements. We also urge the PDPC to give due consideration to competition rules as business models evolve in the data economy to identify and address any hurdles to data sharing.

d) Comments:

Enabling Meaningful Consent

Specific provision of the draft PDP (Amendment) Bill

Section 15A: Deemed Consent by Notification:

An individual is deemed to consent to their collection, use and disclosure of their personal data if (3) the organization determines that the collection, use and disclosure of the personal data is not likely to have an adverse effect on the individual, the purpose for which the personal data is collected and a reasonable period within which the individual may notify the organization that they do not provide their consent.

Section 17: An organization can treat as deemed consent any personal data collected for research purposes or legitimate business interest

We are supportive of the proposed amendments to expand the definition of deemed consent. We seek clarifications on the application of deemed consent by notification:

i) Presently, organisations provide information to customers of their rights over their personal data in existing forms of notices and disclosures. We would like to seek clarification that organisations would continue to be given flexibility to manage this communication to clients as appropriate, such that the absence of a request from client to 'opt-out' would be treated as 'deemed consent' by notification.

ii) We seek clarity that organisations would be allowed flexibility to specify the applicable time period an individual has to inform its decision to opt-out. Organisations require certainty in clients' consent to further processing of personal data at any point of time to be able to proceed further in client relationships. Alternatively, an opt-out period may not be necessary as individuals may at any time withdraw their consent given, or deemed to have been given.

iii) We would also like to clarify that 'deemed consent' would be applicable to all activities with the exception of direct marketing, if specified conditions are met. Section 17 of the PDP Amendment Bill makes reference only to research and legitimate business interests which may be an unintentionally narrow scope.

In particular we would like to seek clarification that 'deemed consent by contractual necessity' will apply to the disclosure and use of data relating to KYC and anti-money laundering and fraud where an organisation enters into contracts to outsource the processing of personal data for such purpose, and sub-processors. This is critical to financial institutions in their effective compliance to regulatory obligations in offering banking and financial services to customers.

Specific provision of the draft PDP (Amendment) Bill

First Schedule Part 3 (2) and (3)

For the collection, use or disclosure of personal data considered in the legitimate interests of the organisation, the organisation must conduct an assessment, before collecting, using or disclosing the personal data (as the case may be), to assess any likely adverse effect to the individuals and determine that the benefit to the public outweighs any likely residual adverse effect to the individual.

The additional exceptions to the consent requirement introduced by PDPC are welcome and are similar to frameworks implemented in other jurisdictions to support the increasing use of technology and innovative applications of data.

Organisations should have in place group policies and risk management frameworks in order to demonstrate accountability in protecting the personal data of customers as appropriate, in line with the accountability principles laid out.

We would like to clarify that the requirement to perform a risk assessment prior to collecting, using or disclosing personal data for legitimate interest of the organisation can be conducted on a use case or dataset basis, and not expected per individual and instance.

We propose that guidance is provided on how organisations can identify and mitigate any likely adverse effects on affected individuals and assess the risk against benefits. This guidance could also address where there are extraordinary considerations or client groups that warrant an individual-level risk assessment.

A balanced risk-based approach to enable the use of personal data for legitimate business interest or research will yield direct benefits to improve range and accessibility of products, as well as improvements to fraud detection and anti-money laundering, which will outweigh any adverse impact on the individual.

Specific provision of the draft PDP (Amendment) Bill

New First Schedule on Collection, use and disclosure of personal data without consent

Repeal of Second, Third and Fourth Schedules and substitution of new Second Schedule - Additional bases for collection, use and disclosure of personal data without individual's consent

We noted revisions in the PDP Amendment Bill to streamline exceptions to consent. We would like to seek clarification that organisations can continue to rely on existing exceptions to the consent requirement for collection, use and disclosure of personal data.

Notification of Data Breaches

Specific provision of the draft PDP (Amendment) Bill

Section 26B: Notifiable Data Breaches

A data breach is a notifiable data breach if it affects not fewer than a minimum number of persons and is deemed to be likely to result in significant harm if it affects any prescribed class of personal data relating to the individual.

It was indicated in the consultation paper that PDPC will prescribe in regulations the numerical threshold on what constitutes "a significant scale" in terms of the number of individuals affected in a data breach. We propose that the determination should be risk-based rather than based on a numerical or other fixed criteria (e.g. number of transactions or transactional values) to be effective and capture relevant incidents across industries. This would allow proportionate approaches across different-sized organisations and include new market entrants which could be even more exposed to cyber and ICT risks.

In addition to the required assessment of the significance of harm to the affected individuals, significance could be risk-assessed on other factors. This could include the level of disruption or resulting threat from the breach in confidentiality, integrity of information assets and impact to markets, and be aligned with organisations' risk framework.

Specific provision of the draft PDP (Amendment) Bill

Section 26D: Duty to notify occurrence of notifiable data breach

(1) Where an organisation assesses, in accordance with section 26C, that a data breach is a notifiable data breach, the organisation must notify the Commission as soon as is practicable, but in any case no later than 3 days after the day the organisation makes that assessment.

In the consultation paper it is proposed that organisations must notify PDPC no later than three calendar days after determining that a data breach meets the notification criteria. We respectfully submit that the specified timeline be three business days, to assist organisations in allocating the operational demands necessary to comply with requirements.

Specific provision of the draft PDP (Amendment) Bill

Section 26D: Duty to notify occurrence of notifiable data breach

(6) An organization must not notify an affected individual if a law agency so instructs or the PDPC so directs

Organisations are required to notify PDPC and affected individuals of data breaches which meet the notifiable criteria. The proposed timeline and provisions require that organisations notify PDPC before or at the same time as affected individuals, and that PDPC may instruct not to notify affected individuals.

We seek clarification on the reasons and circumstances where PDPC would prevent organisations from informing affected individuals, whether due to public or national safety for example.

We appreciate the urgency of notifying affected individuals as soon as practicable of breaches in their personal data and this will allow organisations to carry out remedial measures to mitigate consequences and scope of impact of any breach.

It may not be practicable for PDPC to advise organisations not to inform affected individuals where organisations notify both the PDPC and affected individuals at the same time. The proposed requirements encourage organisations to await a decision from the PDPC (or law enforcement agency) before proceeding to notify individuals and conflicts with requirements to inform affected individuals as soon as practicable. We noted that the intention behind the expedient notification of PDPC is so that PDPC may assist affected individuals who contact PDPC once they are notified. Nonetheless, to enable organisations to mitigate the impact of data breaches on individuals, we recommend that organisations are allowed to prioritise the notification of affected individuals and carry out appropriate remedial measures.

At the same time, we seek guidance from PDPC on the conditions such that affected individuals should not be notified and factors to consider to guide organisations when to seek clarification from the PDPC.

Data Portability

Specific provision of the draft PDP (Amendment) Bill

Section 28

(d) confirm the refusal to transmit the applicable data, or direct the organisation to transmit the applicable data, in the manner and within the time specified by the Commission.

PDPC will have the power to review an organisation's refusal to port data and may direct an organisation to port or confirm a refusal to port data.

We would like to seek clarification on when PDPC will exercise its power to review refusals for data porting and how the review process will be implemented. Upon notification by organisations to individuals of a refusal to port data, individuals may request for a review by PDPC. We propose that a timeframe should be imposed for applications by individuals to the PDPC for review and outline criteria for appeals. This would discourage a

disproportionate number of appeals and reviews to be undertaken by PDPC, and reduce any requirements for organisations to provide information to justify refusal of a porting request.

Clarity around the review process would assist organisations in managing customer relationships and also manage requirements for preservation of personal data while the reconsideration request is processed by PDPC or pending other options for recourse.

Enforcement

Specific provision of the draft PDP (Amendment) Bill

Section 29 Financial penalties

For any breach of an organization with an annual turnover exceeding S$10 million, they will be fined up to S$ 1 million or 10% of their annual turnover whichever is higher.

We noted that the increased financial penalties proposed strengthen enforcement and complement the principles-based approach to strengthen the accountability of organisations.

We seek clarification on the breaches where PDPC will apply the highest level of financial penalties and its consideration of factors in making the determination. We respectfully submit that PDPC considers the severity of impact to affected individuals and the public, as well as remedial actions taken and mitigating measures taken by the organisation. Consideration should also be given to data breaches which occur due to lapses by data intermediaries and where the organisation has reasonable governance and oversight framework in place.

The above would provide reassurance to organisations that the significantly higher penalties would not apply for any and every breach.