

# Feedback on the Public Consultation on the Draft Personal Data Protection (Amendment) Bill

28 May 2020

Zhi Hao, Yong  
Data Protection Officer, Singapore  
([Singapore.Privacy@sc.com](mailto:Singapore.Privacy@sc.com))

## Statement of interest

Standard Chartered Bank (“SCB”) would like to thank the Ministry of Communications and Information (“MCI”) and the Personal Data Protection Commission (“PDPC”) for the opportunity to provide feedback on the draft Personal Data Protection (Amendment) Bill (“Proposed Bill”). SCB generally supports the proposals to enable meaningful consent, increase consumer autonomy and strengthen accountability.

## Summary of major points

- Section 15(4): The proposed deemed consent by contractual necessity provision should clarify on the collection, use and/or disclosure of personal data by multiple downstream organisations (instead of just organisation B) that may be reasonably required to fulfil the contract between the individual and organisation.
- Section 24: “Loss of any storage medium or device on which personal data is stored” is an example of a circumstance which may result in unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks. As organisations could have implemented mitigating measures (e.g. encryption technology), such examples would be better provided for under the Advisory Guidelines or Other Guides.
- Section 26B.–(1)(b): Propose to refine the mandatory notification requirement to only include breaches which affect, or, if the actual number is not yet known, are likely to affect not fewer than the prescribed minimum of individuals and arise from systemic issue(s).
- Section 26B.–(2): The assessment whether a data breach is likely to result in significant impact on individuals would depend on the circumstance or context of the case. Hence, the classes of personal data, which may result in significant harm to the individuals, would be better provided for in the Advisory Guidelines as part of organisations’ assessment.
- Section 2 of the Second Schedule-Part 2: SCB would like to seek clarification if organisations may rely on the business improvement exception:
  - to disclose personal data to entities within its group structure (e.g. subsidiaries of the organisation’s holding company) and external organisations (e.g. vendors) without individuals’ consent for business improvement purpose; and
  - for entities within its group structure and external organisations to collect and use personal data without individuals’ consent for business improvement purpose.

## Comments

### **1) Deemed Consent by Contractual Necessity**

**Reference to provision in the Proposed Bill:** Section 15(4)

**SCB Response:**

We understand that the intention of extending deemed consent by contractual necessity is to allow the organisation (which an individual has provided personal data to for the purpose of a transaction) to disclose the individual's personal data to downstream organisations where the disclosure (and collection and use) are necessary to fulfil the contract between the individual and the organisation.

However, we note that Section 15(4) only prescribes the allowance for B to disclose personal data. It is common in today's digital economy for transaction processing to reasonably require the processing of personal data by multiple downstream organisations.

In view of the above, we propose for Section 15(4) to further prescribe the subsequent collection, use and disclosure of personal data to downstream organisations (beyond B) where it reasonably necessary for the performance of the contract between P and A.

### **2) Protection of Personal Data**

**Reference to provision in the Proposed Bill:** Section 24

**SCB Response:**

Section 24(b) of the Proposed Bill requires organisations to put in place reasonable security arrangements to prevent the loss of any storage medium or device on which personal data is stored specifically under the PDPA. We are of the view that this describes an example of a circumstance which has the potential to result in unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks. Furthermore, a loss of storage medium or device on which personal data is stored may not lead to unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks, if the organisation has put in place mitigating measures, such as encryption technology.

Hence, we propose that the example of a loss of any storage medium or device on which personal data is stored could be provided for in the Advisory Guidelines or Other Guides (instead of the Proposed Bill).

### **3) Mandatory Data Breach Notification**

**Reference to provision in the Proposed Bill:** Section 26B.–(1)(b) and 26B.–(2)).

**SCB Response:**

We note that the PDPC's intention for requiring data breaches affecting not fewer than the minimum number of individuals prescribed under Section 26B.–(1)(b) derives from the risk that such breaches could indicate a systemic issue within the organisation, which may require PDPC's further investigation and guidance on appropriate remedial actions. Noting this, we propose the mandatory notification requirement be refined to apply to breaches which affect,

or, if the actual number is not yet known, are likely to affect not fewer than the minimum number of affected individuals prescribed and arose from a systemic issue.

We agree that certain classes of personal data could be more sensitive and may result in significant harm to the individuals should there be unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks. However, we also view that it does not always necessarily mean that a data breach involving certain classes of personal data would be likely to result in significant harm to the individual. The context or circumstance in which these classes of data might harm an individual would be important in assessing if significant harm is likely to arise. Hence, we propose that the class of personal data should be prescribed in the Advisory Guidelines (instead of the Proposed Bill) as part of an organisations' assessment if the data breach would be likely to result in significant harm to the individual.

#### **4) Business Improvement Exception**

**Reference to provision in the Proposed Bill:** Section 2 of the Second Schedule-Part 2

##### **SCB Response:**

We note that the proposed business improvement exception allows organisations to use personal data about individuals for the business improvement purposes set out in Section 2 of the Second Schedule-Part 2. We also note in the consultation paper that the intent is also for this exception to apply to a group of companies (e.g. subsidiaries of the organisation).

For many organisations which operate in or as part of a group structure, there may be entities within the group structure (e.g. subsidiaries of the organisation's holding company) which undertake such activities on behalf of the organisation. We hope that the Proposed Bill (or the Advisory Guidelines) will confirm that organisations may rely on the business improvement exception to disclose personal data to entities within their group structure without individuals' consent and for the collection and use of personal data by entities within their group structure without an individual's consent for business improvement purpose.

Furthermore, many organisations may engage external organisations (e.g. vendors) with the professional expertise to harness more in-depth insights on an organisation's customers, which the organisation may not be able to achieve. Hence, we would like to propose for the business improvement exception to also allow an organisation to disclose personal data to external organisations (e.g. vendors) without individuals' consent and for the collection and use of personal data by these external organisations without individual's consent for business improvement purpose.

Such collection, use and disclosure of personal data could be subject to similar conditions set out in the proposed research exception (e.g. that the business improvement purpose cannot be reasonably accomplished unless the personal data provided is individually-identifiable) to ensure that the collection, use and disclosure of personal data are proportionate to the business improvement purposes.