Response to Consultation on Personal Data Protection (Amendment) Bill, including related amendments to the Spam Control Act

28 May 2020

Overview

1. We thank MCI/PDPC for the opportunity to provide feedback on the subject.

2. DBS welcomes the recalibration towards meaningful consent and the introduction of the new exceptions for the collection, use and disclosure of personal data along with their emphasis on strengthening organization's accountability.

3. We view these enhancements to be timely and will better enable organizations to take on challenges in the face of rapidly evolving technology and business landscapes.

4. Our provided comments and proposals are geared towards their practical applications by organizations as well as to clarify and align the legislative construct within the proposed Bill based on our understanding of MCI/PDPC's regulatory intentions.

Part II : Strengthening Accountability

No.	Reference in Consult/Bill	Comments
1	**Para 18 of Consult** MCI/PDPC also intends to prescribe in Regulations categories of personal data which, if compromised in a data breach, will be considered likely to result in significant harm to the individuals. This makes clear the types of data breaches that organisations will be required to notify affected individuals. Several jurisdictions have adopted a similar "whitelist" approach for data breach notification to affected individuals and/or the authorities. Examples of data categories prescribed by other jurisdictions include social security numbers, drivers' licence numbers, state identification numbers, credit/debit card numbers, health insurance information and medical history information.	1) In line with the shift towards a risk-based, accountability approach, "categories of personal data" should be assessed with other contextual factors to enable a well-considered assessment of whether the data breach is likely to result in significant harm to affected individuals. To illustrate, where such data is disclosed without any unique identifiers or not accompanied by other essential attributes, it may not identify specific individuals nor be meaningful to the third party and is therefore not likely to give rise to significant harm to individuals involved. 2) We propose that organizations can continue to incorporate contextual considerations such as the following in making their assessments notwithstanding that such categories of personal data are involved: • Ease of identification of affected individuals – Whether the third party can readily identify the data types or the specific individuals including when referenced with publicly available records. E.g. where data type involved a string of numbers, it may not be readily inferred by the third party what is the data type involved or the individual; whilst to the organization these would be. Consideration should also be given if the data involved was securely encrypted or protected, rendering it unintelligible to the third party. • Likelihood of harm - Whether the divulged information can singly cause harm without other essential attributes present. For example, credit card numbers or account numbers alone without other authentication means e.g. Card Verification Number, credit card expiry date, 2-factor authentication, may not result in harm to affected individuals as fraudulent transactions cannot occur without the necessary authentication. Similarly, for account numbers, there are established verification checks and procedures to ascertain the account holder identity and authenticity of instructions received. • Relationship with the recipient – In situations where personal data was erroneously sent to an unintended recipient, the organisation may have a trusted and ongoing relationship with recipient which gives the organisation reasonable assurance that the recipient will comply with the instructions to delete the data that was erroneously received. Where so, the risk or likelihood of significant harm to individuals is greatly mitigated as the incident can be deemed to be effectively contained. The converse would be true where personal data is exposed to a possibly malicious actor and affected individuals would be placed at greater risk of harm. 3) We propose that these contextual considerations be applicable for incidents involving significant scale as well as where reporting is made given their unavailability, this will enable MCI/PDPC to better risk-focus on the specific sectors in upholding data protection standards as set out in para 16 of the Consult. 4) Furthermore, given the varying degrees of harm, we request MCI/PDPC to share its considerations or examples for assessing the levels of significance of harm involved such that there will be greater consistency and application by organizations in this approach. 5) With the understanding that the proposed breach notification requirement does not affect equivalent obligations that organizations have under other existing sectoral laws, we ask that further considerations to be given to streamlining reporting between regulatory agencies where possible.

Part II : Strengthening Accountability

No.	Reference in Consult/Bill	Comments
2	**26A of Bill** "data breach", in relation to personal data, means — (a) the unauthorised access, collection, use, disclosure, copying, modification or disposal of personal data; or (b) the loss of any storage medium or device on which personal data is stored in circumstances where the unauthorised access, collection, use, disclosure, copying, modification or disposal of the personal data is likely to occur	1) With respect to the proposed definition of "data breach", we note that other similar laws use a more abridged definition and generally define data breach as a breach of security safeguards resulting in unauthorised access, disclosure, modification or loss of personal data. 2) From a technical reading, it is possible for "unauthorised accesses" with no data exfiltration to remain lawful but a non-adherence to internal access management procedures as organisations often restrict employee accesses on a need-to basis that is stricter than the regulatory and contractual requirements. 3) Given these, we request MCI/PDPC clarify that "unauthorized access" is to be read in tandem with their security safeguards in place. Additional references to clarify what would or would not be construed as "unauthorized access" would be helpful to steer and enable a greater consistency by organizations to capture the intended data breaches. 4) For greater comparability with similar jurisdictions, we propose that MCI/PDPC to consider keeping the regulatory criteria of data breach within the construct of (a). Where MCI/PDPC remains minded for (b) to be included in the regulatory definition, we request clarifications on the circumstances envisaged for "unauthorized collection, modification" with the loss of such storage medium or device as organizations would be obligated to perform assessments against them where this is included within the regulatory criteria.

Part II : Strengthening Accountability

No.	Reference in Consult/Bill	Comments
3	**26E of Bill** "Applicable data", in relation to a porting organisation, means any personal data in the possession or under the control of the porting organisation that is, or belongs to a class of personal data that is, prescribed;	1) We understand that MCI/PDPC intends for Data Portability Obligation to include "user provided data" and "user activity data". We propose that these be reflected in the definition of applicable data to avoid ambiguity in its intended scope. We propose the following for consideration: *"applicable data", in relation to a porting organisation, means any user provided data or user activity data in the possession or under the control of the porting organisation that is, or belongs to a class of personal data that is, prescribed."* 2) Extending, we propose for the definition of user activity data to be reconsidered to avoid ambiguity that may be associated with derived data or materials produced by the bank for risk assessment purposes as a result of its current proposed qualification that it comprise those "created in the course of or as a result of". To illustrate, credit risk assessment information about an individual's utilization of the bank's credit financing products should not fall within scope of user activity data even though these are "created in the course of or as a result of" the individual's use of the bank's products. We believe this application is consistent with MCI/PDPA's intention not to include such in the Data Portability Obligation. We propose the following revised definition for MCI/PDPC's consideration: *"user activity data", in relation to an organisation, means personal data about an individual that shows the individual's use of product or service provided by the organization."*

Part II : Strengthening Accountability

No.	Reference in Consult/Bill	Comments
4	**35B of Bill** If — (a) an individual discloses, or the individual's conduct causes disclosure of, personal data in the possession or under the control of an organisation or a public agency to another person; (b) the disclosure is not authorised by the organisation or public agency, as the case may be; and (c) the individual does so — (i) knowing that the disclosure is not authorised by the organisation or public agency, as the case may be; or (ii) reckless as to whether the disclosure is or is not authorised by the organisation or public agency, as the case may be, the individual shall be guilty of an offence and shall be liable on conviction to a fine not exceeding $5,000 or to imprisonment for a term not exceeding 2 years or to both.	1) Given there may be employees in specific functions that may be required to handle high volumes of client information in the ordinary course of their daily work as compared to other functions of the organization e.g. Operations, we consider that inadvertent disclosures should be looked upon sympathetically. This will also enable organizations to continue hiring and groom talents in these functions and the individual without undue fear of developing themselves in these specializations, while reinforcing the need for proper accountability at both organization and individual levels.

Part IV : Increasing Consumer Autonomy

No.	Reference in Consult/Bill	Comments
5	**Para 45 of Consult** To ensure that the compliance burden is reasonable for organisations, the Data Portability Obligation will be scoped to the following: a) User provided data (i.e. data that is provided to the organisation, such as name, contact information, credit card details, delivery address) and user activity data (i.e. data about the individual that is created in the course of or as a result of the individual's use of any product or service, such as transactions, data collected by wearables and sensors) held in electronic form, including business contact information.	1) We urge MCI/PDPC to reconsider the proposal for Business Contact Information ("BCI") to be covered by the Data Portability Obligation. BCI is provided by an individual in a corporate relationship capacity and allowing BCI to be ported for domestic/personal needs would be incongruent with the initial purpose for which the BCI was provided.
6	**Para 47 of Consult** To provide greater certainty for compliance, the Data Portability Obligation will only come into effect with the issuance of Regulations. The Regulations will prescribe requirements that apply to the porting of specific datasets. PDPC will work with the industry and relevant sector regulators to develop the requirements to be prescribed in the Regulations. PDPC intends to prescribe the following in the Regulations	1) We are mindful that there could be further clarifications beyond the stated (a)-(d), that would be useful to help parties involved better understand and address how the risks associated with data portability e.g. data integrity and security risks are being apportioned. These ensuing considerations may be relevant for inclusion to the eventual Regulations to ensure a consistent application of the data portability obligations and equitable grounds for the individual and organizations involved. Where appropriate, we look forward participating in these deliberations.

Part VI : Others

No.	Reference in Consult/Bill	Comments
7	**Para 76 of Consult** To ensure organisations remain accountable for personal data in their possession or under their control, organisations will still be required to provide individuals with access to derived personal data. Organisations are to also provide the individual with 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.	1) We strongly recommend that MCI/PDPC retain its earlier decision to exclude "derived personal data" from the Access obligation. The stated intent of "ensuring organisations remain accountable for personal data in their possession or under their control" is already addressed by other data protection obligations. Preserving the right for individuals to access "derived personal data" may invariably undermine the intent for excluding derived data from the Data Portability obligation. 2) For instance, KYC processes are undertaken by financial institutions to gain a reasonable understanding of the customers for anti-money laundering and countering the financing of terrorism purposes. Data associated with KYC processes is not only proprietary in nature but serves a wider purpose of safeguarding the integrity of Singapore's financial system. Disclosing such "derived personal data" to bad actors who can reverse engineer and gain a better understanding of the financial institutions' controls to avoid detection could undermine the safety and soundness of the financial system. The same could be said of other areas such as a financial institution's credit risk management standards. 3) The "derived personal data" is also the intellectual property of the organisation and there is significant commercial sensitivity associated with them, which under the proposed Bill, can now be obtained by an individual and passed on to other organisations. This could stifle data-driven innovation. 4) Accordingly, we respectfully recommend the exclusion of derived data from the Access obligation.

<END>