CLOSING NOTE ISSUED BY
THE MINISTRY OF COMMUNICATIONS AND INFORMATION AND
THE PERSONAL DATA PROTECTION COMMISSION

DRAFT PERSONAL DATA PROTECTION (AMENDMENT) BILL INCLUDING RELATED AMENDMENTS TO THE SPAM CONTROL ACT

5 OCTOBER 2020

CLOSING NOTE TO THE PUBLIC CONSULTATION ON DRAFT PERSONAL DATA PROTECTION (AMENDMENT) BILL INCLUDING RELATED AMENDMENTS TO THE SPAM CONTROL ACT

PART I: INTRODUCTION

1. The Personal Data Protection Act 2012 ("PDPA") governs the collection, use and disclosure of personal data by organisations in Singapore. Enacted in 2012, it strikes a balance between the need to protect individuals' personal data and private organisations' need to collect, use and disclose personal data for legitimate and reasonable purposes. The Do Not Call ("DNC") Provisions of the PDPA enable individuals to opt-out of receiving specified messages[1] in the form of text messages, fax messages or voice calls, sent to Singapore telephone numbers, by requiring persons to check the relevant DNC Register before sending a specified message to a Singapore telephone number[2]. The DNC Provisions and the Data Protection ("DP") Provisions came into effect on 2 January 2014 and 2 July 2014 respectively.

2. The Ministry of Communications and Information ("MCI") and the Personal Data Protection Commission ("PDPC") conducted a public consultation[3] on the draft Personal Data Protection ("PDP") (Amendment) Bill from 14 to 28 May 2020. This followed three public consultations[4] on the key policy positions between 2017 and 2019, and was intended to clarify and finalise the language in the Bill to put the policy positions into effect. MCI/PDPC received 87 responses at the close of the consultation. Please refer to MCI's website for the full list of respondents and their submissions[5].

3. Overall, respondents were generally supportive of the draft PDP (Amendment) Bill as the proposed amendments add flexibility and clarity to the PDPA.

4. Some respondents sought clarification or provided feedback on the scope and operational details of the draft provisions. MCI/PDPC intends to

[1] "Specified message" is defined in section 37 of the PDPA. Exclusions from the definition of specified messages are listed in the Eighth Schedule to the PDPA.
[2] Unless the person has obtained clear and unambiguous consent from the individual or has an ongoing relationship with the individual.
[3] The public consultation for the draft Personal Data Protection (Amendment) Bill can be found at https://www.mci.gov.sg/public-consultations/public-consultation-items/public-consultation-on-the-draft-personal-data-protection-amendment-bill.
[4] The public consultations for these proposals and responses to the feedback received can be found at https://www.pdpc.gov.sg/Guidelines-and-Consultation?type=public-consultations
[5] The responses to the public consultation on the draft PDP (Amendment) Bill can be found at https://www.mci.gov.sg/public-consultations/public-consultation-items/responses-on-draft-personal-data-protection-amendment-bill.

address these in Regulations and Advisory Guidelines after the PDPA is amended, which PDPC will continue to engage the industry to develop.

PART II: SUMMARY OF KEY REVISIONS ARISING FROM PUBLIC CONSULTATION FEEDBACK

5. MCI/PDPC's key revisions to the draft PDP (Amendment) Bill after considering the public consultation feedback are summarised below.

Increased Financial Penalty Cap

6. MCI/PDPC proposed to increase the maximum financial penalty for data breaches under the PDPA to (i) up to 10% of an organisation's annual turnover; or (ii) S$1 million, whichever is higher. The higher cap is intended to serve as a stronger deterrent and enable PDPC to take effective enforcement action based on the circumstances and seriousness of a breach, in order to uphold organisational accountability for personal data.

Feedback received

7. Approximately a third of all the respondents were concerned with the increase in the financial penalty cap, with some citing the economic downturn arising from COVID-19. Some respondents also requested for a sunrise period before the increased financial penalty cap takes effect. There were also several respondents who requested that MCI/PDPC make clear in the draft PDP (Amendment) Bill that the financial penalty cap refers to 10% of an organisation's annual turnover **in Singapore**; or S$1 million, whichever is higher.

MCI/PDPC's response

8. MCI/PDPC notes organisations' feedback and will take into account the prevailing economic situation in refining the financial penalty framework. Regardless of the higher cap, in determining the appropriate financial penalty quantum, PDPC will continue to be circumspect and guided by the facts of the individual case, as well as relevant factors including the seriousness of the breach and its impact, level of culpability, the need for deterrence, and the overall proportionality of the amount.

9. In determining the financial penalty quantum, PDPC currently considers factors such as whether the organisation took any action to mitigate the effects of the data breach and the type and nature of the personal data affected. Some of these factors are listed in the Guide on Active

Enforcement. To provide clarity and regulatory certainty, MCI/PDPC intends to set out in the PDPA a non-exhaustive list of factors that PDPC would consider and give weight to as appropriate when determining the quantum of financial penalty to impose.

10. MCI/PDPC also intends to amend the draft PDP (Amendment) Bill to expressly state that the maximum financial penalty for the DP Provisions is (i) up to 10% of an organisation's annual turnover in **Singapore**; or (ii) S$1 million, whichever is higher. MCI/PDPC intends to have tiered financial penalty caps for breaches of the DNC provisions, aligned with the egregiousness of the breach.

Business Improvement Exception

11. MCI/PDPC proposed a new exception where organisations may use personal data without consent for the following business improvement purposes: (i) operational efficiency and service improvements; (ii) developing or enhancing products/services; and (iii) knowing the organisation's customers. This provides clarity and certainty for organisations that use personal data for such purposes. MCI/PDPC also indicated its intent for this exception to apply to a group of companies (e.g. subsidiaries of the organisation).

Feedback received

12. MCI/PDPC received strong support for the proposed exception to apply to entities within a group. Some respondents cited examples where companies may leverage data for business improvement purposes within a group. These include structuring of common administrative functions and centralising research and development.

MCI/PDPC's response

13. MCI/PDPC intends to provide for the business improvement exception to apply to the collection, use and disclosure of personal data by related corporations within a group, with additional safeguards. This is in accordance with commercial reality on the ground where a group of related corporations may comprise separate legal entities but are functionally a whole due to shareholding controls.

14. In order to rely on the business improvement exception to use personal data without consent, in addition to meeting the business improvement purposes, **organisations must satisfy the following conditions**:

a) the purpose cannot reasonably be achieved without the use of the personal data in an individually identifiable form;

b) the purpose is what a reasonable person would consider appropriate in the circumstances[6]; and

c) the purpose is not for sending direct marketing messages.

15. MCI/PDPC intends to introduce the following **additional conditions** for the business improvement exception to apply **to the collection, use and disclosure of personal data within a group of related corporations**, in order to prevent misuse:

a) the personal data collected or disclosed must relate to an individual who is an existing customer of the disclosing corporation, and an existing or prospective customer of the collecting corporation. MCI/PDPC's intent is that a prospective customer refers to an individual who expresses interest in the collecting corporation's goods or services, or engages the collecting organisation on the possible purchase, hire or use of its goods or services. MCI/PDPC does not consider an individual who receives marketing materials from the collecting corporation and does not take any positive step in response to be a prospective customer; and

b) the related corporations must be bound by any contract or other agreement, or binding corporate rules requiring the collecting corporation to implement and maintain appropriate safeguards for the personal data.

Business Asset Transaction Exception

16. Some respondents requested that the business asset transaction exception go beyond the current scope on the sale of assets to include other similar transactions such as mergers and acquisitions, sale of shares, transfer of controlling power or interests, corporate restructuring and reorganisation.

MCI/PDPC's response

17. MCI/PDPC assesses that the request is reasonable and aligned with the policy intent for the exception, as obtaining consent for the collection, use and disclosure of personal data in these instances may not be meaningful/practical. Hence, MCI/PDPC intends to extend the exception

[6] Section 18(a) of the PDPA.

to include mergers and acquisitions, sale of shares, transfer of controlling power or interests, corporate restructuring and reorganisation.

Data Portability Obligation

18. MCI/PDPC proposed to introduce a new Data Portability Obligation to provide consumers with greater autonomy over their personal data. Under the Data Portability Obligation, an organisation must, at the request of an individual, transmit his/her personal data that is in the organisation's possession or under its control, to another organisation in a commonly used machine-readable format.

19. MCI/PDPC proposed for exceptions to the Data Portability Obligation to be provided, similar to the current exceptions to the Access Obligation under the Fifth Schedule to the PDPA. Further, to protect business innovation and investments by organisations, the Data Portability Obligation will not apply to personal data about an individual that is derived by an organisation in the course of business from other personal data (referred to as "derived personal data").

Feedback received

20. While the exceptions to the Data Portability Obligation were stated in the public consultation paper, they were not included in the draft PDP (Amendment) Bill. Several respondents requested for the exceptions to be expressly provided in the PDP (Amendment) Bill.

MCI/PDPC's response

21. MCI/PDPC intends to expressly provide for (i) the types of data an organisation is not required to port; and (ii) the circumstances under which an organisation is not required to port data, in a Schedule to the PDPA.

Offences for Egregious Mishandling of Personal Data

22. MCI/PDPC proposed to introduce offences to hold individuals accountable for egregious mishandling of personal data in the possession of or under the control of an organisation or a public agency. The proposed offences are for the:

    a) Knowing or reckless unauthorised disclosure of personal data;

    b) Knowing or reckless unauthorised use of personal data for a gain or to cause harm or a loss to another person; and

c) Knowing or reckless unauthorised re-identification of anonymised data.

23. MCI/PDPC proposed to provide for defences to these offences, such as where the information is publicly available; where the conduct is permitted or required under other laws; or where the conduct is authorised or required by an order of the court or in the reasonable belief, and was not reckless as to whether, the individual has the legal right to do so.

Feedback received

24. Several respondents highlighted that the drafting language was too broad and raised concerns about the potential "chilling effect" these offences would have on individuals taking on roles which handle high volumes of data or being overly cautious when they handle data. In particular, respondents sought further clarification on what would be considered conduct that is authorised, as well as the applicable defences.

MCI/PDPC's response

25. MCI/PDPC intends to clarify in Advisory Guidelines the situations that the new offences are not intended to cover. These include situations where the individuals are authorised as part of their employment to disclose, use or re-identify the data. The Advisory Guidelines will include further details on conduct that is authorised, and the various forms authorisation may take. For example, conduct that is authorised may be set out in an organisation's written polices, manuals and handbooks, or an organisation may provide ad-hoc authorisation for a specific action or activity, which should be provided by someone in the organisation who is empowered to do so or who is ostensibly empowered to do so by reason of his/her seniority or position in the organisation.

26. MCI/PDPC intends to expressly provide for additional defences for re-identification of anonymised data in the PDPA, for purposes such as testing the effectiveness of the anonymisation of personal data and testing the systems and processes to safeguard the integrity and confidentiality of anonymised information.

PART III: CONCLUSION

27. MCI/PDPC thanks all respondents for their comments to the public consultation.

28. MCI/PDPC will continue to solicit views and feedback in developing the Regulations and Advisory Guidelines to provide greater clarity on the implementation of the PDPA.