M1'S RESPONSE TO PDPC'S PUBLIC CONSULTATION ON APPROACHES TO MANAGING PERSONAL DATA IN THE DIGITAL ECONOMY

This paper is prepared in response to PDPC's Public Consultation document dated 27 July 2017 and represents M1's views on the subject matter. Unless otherwise noted, M1 makes no representation or warranty, expressed or implied, as to the accuracy of the information and data contained in this paper nor the suitability of the said information or data for any particular purpose otherwise than as stated above. M1 or any party associated with this paper or its content assumes no liability for any loss or damage resulting from the use or misuse of any information contained herein or any errors or omissions and shall not be held responsible for the validity of the information contained in any reference noted herein nor the misuse of information nor any adverse effects from use of any stated materials presented herein or the reliance thereon.

Introduction

1. M1 is Singapore's most vibrant and dynamic communications company, providing mobile and fixed services to over 2 million customers. With a continual focus on network quality, customer service, value and innovation, M1 links anyone and anything; anytime, anywhere.

M1's view on the Proposed Amendments to the PDPA

2. M1 supports the development of a proportionate and stable regulatory environment as it will catalyse a sustainable and growing info-communications industry where long term planning and decisions can be undertaken.

3. M1 welcomes the opportunity to submit our comments to PDPC's public consultation on the proposed amendments to the PDPA. We believe that it is timely to review the PDPA to ensure that the regulatory environment keeps pace with the needs and challenges presented by the emerging Digital Economy.

4. M1's specific comments on the PDPA's consultation are set out in the following sections.

PART II: ENHANCED FRAMEWORK FOR COLLECTION, USE AND DISCLOSURE OF PERSONAL DATA

Notification of Purpose

Question 1: *Should the PDPA provide for Notification of Purpose as a basis for collecting, using and disclosing personal data without consent?*

Question 2: *Should the proposed Notification of Purpose approach be subject to conditions? If so, what are your views on the proposed conditions (i.e., impractical to obtain consent and not expected to have any adverse impact on the individual)?*

1. M1 supports the PDPC's proposal for organisations to provide for Notification of Purpose as a basis for collecting, using and disclosing personal data without consent. In today's digital age, there are numerous ways through which personal data can be collected, and it would not be practical for organisations to obtain consent of each individual for the collection, use or disclosure of their personal data.

2. While it would be reasonable to subject the use of Notification of Purpose to certain conditions, the PDPC could provide further clarifications and guidance on those conditions. For example, it is not clear what situation would constitute an adverse impact on the individuals, and what should the proposed risk and impact assessment entail. This will allow organisations to better understand their obligations with respect to collecting, using and disclosing personal data under the Notification of Purpose.

Legal or Business Purpose

Question 3: *Should the PDPA provide for Legal or Business Purpose as a basis for collecting, using and disclosing personal data without consent and notification?*

Question 4: *Should the proposed Legal or Business Purpose approach be subject to conditions? If so, what are your views on the proposed conditions (i.e., not desirable or appropriate to obtain consent and benefits to the public clearly outweigh any adverse impact or risks to the individual)?*

3. M1 supports the PDPC's proposal for organisations to rely on Legal or Business Purpose as a basis for collecting, using and disclosing personal data without obtaining consent from and notification to individuals.

4. Similarly, we are of the view that it would be useful to have greater clarity and guidance provided on the proposed conditions that would govern the use of Legal or Business Purpose as a basis for collecting, using and disclosing personal data.

PART III: MANDATORY DATA BREACH NOTIFICATION

Data Breach Notification

Question 5: *What are your views on the proposed criteria for data breach notification to affected individuals and to PDPC? Specifically, what are your views on the proposed number of affected individuals (i.e., 500 or more) for a data breach to be considered of a significant scale to be notified to PDPC?*

Question 6: *What are your views on the proposed concurrent application of PDPA's data breach notification requirements with that of other laws and sectoral regulations?*

5. PDPC has proposed to mandate the requirement for organisations to notify PDPC when a data breach incident that is of a significant scale (involving 500 or more affected individuals) has occurred. PDPC has also proposed that organisations could notify PDPC concurrently with the sectoral regulator or law enforcement agency in accordance with the notification requirements under other written law.

6. The PDPC's intent to streamline the requirements for organisations to notify PDPC on data breach incidents is laudable. However, further clarification is necessary in the following instance. Apart from notification to the regulators when a service outage incident has occurred, there are other requirements such as providing regular status updates to the regulators on the service restoration. In the event that there are no further data breaches in the incident, are organisations expected to notify PDPC of such status updates as well?

Obligations of Data Intermediary

7. PDPC has proposed that where an organisation's data intermediary ("DI") experiences a data breach, the DI would be required to immediately inform the organisation that it processes the personal data on behalf of, regardless of the risk of harm or scale of impact of the data breach. From a practical point of view, it may be reasonable to allow the DI to notify the organisation as soon as practicable, not later than 24 hours.

8. Additionally, in the event that a DI fails to notify and provide the relevant information to an organisation, resulting in the organisation failing to meet PDPC's notification requirements, we like to seek PDPC's clarification on whether the organisation may be absolved from the non-compliance in this aspect.

Exceptions and Exemptions from Breach Notification

Question 7: *What are your views on the proposed exceptions and exemptions from the data breach notification requirements?*

9. PDPC has proposed for the exclusions under Section 4 of the PDPA, namely where provisions of other written law are inconsistent with the proposed breach notification provisions

under the PDPA, to apply to the proposed breach notification provisions. We would like to seek PDPC's confirmation that in the instance of such an inconsistency, the provisions of other written law will take precedence over M1's obligations under the PDPA.

10. PDPC has also proposed for a technological protection exception to be provided to the requirement to notify affected individuals, where the breached personal data is encrypted to a reasonable standard. We would request further clarity on what the PDPC would deem as "reasonable standard".