CONSUMERS ASSOCIATION OF SINGAPORE

PUBLIC CONSULTATION FOR APPROACHES TO MANAGING PERSONAL DATA IN THE DIGITAL ECONOMY

170 Ghim Moh Road
Ulu Pandan Community Building
Singapore 279621
admin@case.org.sg

21 September 2017

PREFACE

Unless otherwise stated, the definitions and abbreviations have been adapted from PDPC's public consultation for approaches to managing personal data in the digital economy ("**Consultation Paper**") issued 27 July 2017. CASE comments on questions 1, 3 and 5 are set out below.

Question 1

QUESTION 1: SHOULD THE PDPA PROVIDE FOR NOTIFICATION OF PURPOSE AS A BASIS FOR COLLECTING, USING AND DISCLOSING PERSONAL DATA WITHOUT CONSENT?

CASE Comments:

1. CASE notes that the PDPC intends to require organisations that wish to rely on the Notification of Purpose to provide appropriate notification of the purpose, use or disclosure and to allow individuals to opt out, where feasible.

2. Hence, in this respect, the Notification of Purpose is not materially different from the existing consent framework.

3. CASE notes the various challenges to obtain consent (outlined at paragraphs 2.1 to 2.5 of the Consultation Paper) and agrees that increasingly, the proliferation of verbose consent clauses and frequent taking of consent has resulted in consent fatigue.

4. The example cited by Dr Yaacob Ibrahim, Minister for Communications on 27 July 2017 and the spoof term added by Public Wi-Fi provider Purple are examples of such behaviour.

5. However, the growth of IoT devices (in particular), machine learning and artificial intelligence also provides a clear means by with organisations may obtain consumers' consent. In such applicable cases, it would be preferable if future guidelines issued by the PDPC could encourage organisations operating such devices/platforms to make a concerted effort to obtain meaningful consent from the consumers.

6. For instance and subject to how the technology develops, PDPC could make it clear that it is not considered to be "impractical for the organisation to obtain consent" where an organisation has control of the consumers access to a service (for example, while it is likely impractical for an organisation to obtain consent in the example at paragraph 3.11 of the Consultation Paper, the Notification of Purpose should not apply where the consumer has a contractual relationship with the organisation to receive goods or services through an IoT device).

7. In which case, instead of obtaining consent through verbose consent clauses, as a matter of best practice, the organisation could cater for the IoT devices to provide for the disclosure of specific personal data / data based on user selection and allow for

the selections to be updated at will (i.e. sharing of photos, location, health data based on selection of choices).

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?

CASE Comments:

1. Compared to the GDPR and the Republic of Korea's Personal Information Protection Act, the proposed Legal and Business Purpose amendment is significantly wider in implications for it also provides for the *disclosure* of personal data without any consent or notification.

2. CASE notes that currently, there are certain limited exceptions in the PDPA to allow organisation to collect, use and/or disclose personal data without consent. However, CASE is concerned that Legal or Business Purpose amendment (in particular, the business purpose) is unnecessary broad and may potentially circumvent the entire consent framework for the collection, usage and disclosure of personal data.

3. CASE notes that GDPR specifically cites direct marketing as a legitimate interest. Hence, applying the proposed conditions attached to the Legal or Business Purpose, it could be that forms of direct or indirect marketing / segmentation could fall within the Legal or Business Purpose of an organisation.

4. As such, CASE is of the view that certain activities (i.e. direct marketing or attempts to segment and market to consumers using personal data) or any activities that may have an adverse impact on the individual should be prohibited under the Legal or Business Purpose (potentially through Guidelines of the PDPC).

5. Unlike the Notification of Purpose, organisation that chooses to rely on the Legal or Business Purpose are not required to notify the individual. As such, arguably, the purpose and conditions that needs to be satisfied ought to be held to a higher threshold (and in this respect, a balancing test between the benefits to the public clearly outweighing any adverse impact or risk to the individual may not be appropriate).

6. In addition, most of the examples cited in the GDPR and the Republic of Korea's Personal Information Protection Act can be sourced to a legal purpose (i.e. as opposed to a business purpose; i.e. prevent fraud, monitoring employees for safety and the definition of a legitimate interest).

7. As such, CASE proposes to:

a) narrow the "Legal or Business Purpose" to a "Legal Purpose" only; and

b) clearly spell activities that would not qualify under the Legal or Business Purpose, such as direct or indirect marketing (taking into consideration, the potential adverse impact or risk to the individual).

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?

1. CASE supports the requirement for organisations to notify the affected individuals and PDPC in the event of a personal data breach (where applicable).

2. However, CASE is of the view that the organisation should also notify the affected individuals where the scale of the data breach is significant (i.e. involving 500 or more affected individuals) even if the data breach does not pose any risk of impact or harm to the affected individuals.

3. In the event of such systemic breaches, individuals should be notified for them to make an informed choice on the steps they wish to take, such as to withdraw consent for a particular purpose etc.