Response to the Public Consultation for Approaches to Managing Personal Data in the Digital Economy
(Submitted on 21 Sep 2017)

1. Questions 1 and 2 of consultation paper

I am supportive of notification of purpose as a basis for collecting, using and disclosing personal data without consent. However, this should be subject to commercially appropriate forms/ channels of notification, and a risk-calibrated risk impact assessment by organisations.

Organisations should be allowed to objectively determine a reasonable form of notification and risk impact assessment.

PDPC should also allow organisations to seek and obtain regulatory guidance on their proposed form of notification and risk impact assessment.

2. Questions 3 and 4 of consultation paper

I am supportive of relying on legal or business purpose as a basis for collecting, using and disclosing personal data without consent and notification.

I am also supportive of the proposed conditions to the legal or business purpose basis. Organisations should be allowed to objectively determine whether (a) it would be desirable or appropriate to obtain consent, and (b) the public benefit outweighs individual risk/ impact.

3. Question 5 of consultation paper

I agree that organisations should inform affected individuals if the breach of will result in impact/ harm to the individuals. Organisations should be allowed to objectively determine whether any impact or harm will arise, and a reasonable method and form of notifying the affected individuals.

However, the requirement for organisations to inform PDPC in the event of a data breach involving 500 or more individuals is not appropriate or meaningful. The key criteria should be the *nature/ type of personal data* that has been compromised/ lost, and not the number of individuals affected.

As an example, an organisation may in error send an email with an attachment containing only the names of 500 employees to a single unintended recipient. In this scenario, it is arguable that the data breach poses little or no risk/ harm to the employees concerned. Contrast that with the scenario where an email with an attachment containing the names, NRIC numbers, residential addresses, telephone numbers and salary details of 10 employees is sent in error to an unintended recipient. In the latter scenario, the nature/ type of data is sensitive and personal, and the disclosure would foreseeably pose material risks/ impact to the 10 employees.

4. Question 6 of consultation paper

I am supportive as the proposal avoids the need for duplicative notification.

5. Question 7 of consultation paper

I am supportive of the proposed exceptions, particularly the technological protection/ encryption exception.

6. Question 8 of consultation paper

Organisations should inform affected individuals "as soon as practicable", and be allowed to reasonably and objectively determine what is "as soon as practicable".

As for informing PDPC, the proposed timeframe of within 72 hours is fine if PDPC does not require full and/or extensive details. Informing PDPC within 72 hours, without any substantive details of the data breach because investigations are on-going, would not be meaningful to both PDPC and organisations.

Organisations should be required to inform PDPC within 72 hours that a data breach has occurred, and state the status of its investigations. If investigations are still on-going, PDPC should allow the organisation to properly complete its investigations before providing the details required by PDPC.

7. General

a. Risk and impact assessment

The consultation paper mentions a data protection impact assessment ("DPIA"). In this regard, the "Guide to Data Protection Impact Assessments" to be issued by PDPC should ideally be non-binding, and contain user-friendly guidelines and templates for the conduct of DPIAs, risk mitigation measures to be taken by organisations etc.

b. Costs and burden of regulatory compliance

In terms of personal data compliance, it is necessary for PDPC to establish regulatory safeguards and obligations, and for organisations comply with the PDPA.

However, PDPC should be mindful to not impose overly or excessive compliance requirements on organisations. With the general economic slowdown, increasing costs of doing business, and weak consumer sentiment, companies in Singapore have many challenges to deal with to keep their businesses viable.

A light-touch and commercially sensible approach towards regulatory compliance would help facilitate and encourage personal data compliance by organisations. PDPC can also help organisations to comply with their obligations under the PDPA in a commercially expeditious and sensible manner. In this regard, organisations would look forward to the proposed resources to be issued by PDPC (eg, DP starter kit).