RESPONSE TO CONSULTATION PAPER

Consultation topic:	Public Consultation for Approaches to Managing Personal Data in the Digital Economy
Name[1]/Organisation: [1]if responding in a personal capacity	St. James's Place International plc (Singapore Branch)
Contact number for any clarifications:	+65 6390 4736
Email address for any clarifications:	Reagan.Koh@sjp.ie

General comments:

In view of global developments and technological advances, we welcome the review of the Personal Data Protection Act 2012 (the "PDPA"). We are broadly supportive of the proposals presented but would like to seek clarification and the PDPC's consideration in respect of certain proposals as detailed below.

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

No comments.

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)?

We wish to seek clarification on the terms used in the 2 criteria, i.e. "impractical" and "adverse impact" as organisations may adopt different interpretations and hence, exercise their own discretion in implementing the proposal. It would be useful if illustrations could be provided. For example, under what circumstances would organisations deem as impractical to obtain the consent and to what extent shall be the impact on the individual to justify the exemption from obtaining the consent.

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?

No comments.

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)?

Similar to Question 2 above, we wish to seek clarification on several terms/phrases such as "not desirable or appropriate", "benefits to the public" and "adverse impact or risks".

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?

Risk of impact or harm to affected individuals

The requirement of notifying both Personal Data Protection Commission ("PDPC") and affected individuals of a data breach that poses any risk of impact or harm to affected individuals without considering the materiality of the data breach might be too onerous on the organisation, especially in situations where the impact or harm to the individuals is minimal or insignificant. An example of such situation is when the data breach has been discovered early and corrective actions have been taken to mitigate the risks to the individuals.

In view of the above, we would like to propose for PDPC to consider materiality of the data breach as a criterion for notification. PDPC could provide guidance on the assessment of materiality in the guidelines the PDPC intends to develop and issue.

Significant scale of breach

The figure "500" is arbitrary and may not be indicative of the materiality of the data breach or any systemic issue within an organisation.

We would like to propose for PDPC to consider materiality as the criterion of notifying PDPC instead of the use of an arbitrary number. Similarly, PDPC could provide guidance on the assessment of materiality in the guidelines the PDPC intends to develop and issue.

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?

PDPC's proposal of concurrent notification imposes additional compliance burden on organisations which already have other notification/reporting requirements to comply. Should PDPC's proposal materialise, organisations will be required to set up additional operational workflows for each of these requirements.

We wish to highlight that organisations faced with a data breach would be in crisis-resolution mode, and resources should be directed at managing and resolving the breach, rather than managing requests for information from multiple regulators/authorities.

In the recent proposed Cybersecurity Bill, the Ministry of Communications and Information ("MCI") and Cyber Security Agency of Singapore ("CSA") have proposed to appoint Assistant Cyber Commissioners or "Sector Leads", i.e. the lead government agency in charge of each sector (e.g. Monetary Authority of Singapore) to help to cut down on the compliance burden on organisations when dealing with cybersecurity issues.

In view of the above, we would like to propose that the PDPC considers aligning its approach with the MCI's and CSA's proposed Cybersecurity Bill and appoint liaisons that are officers from "Sector Leads" to prevent wastage of resources on concurrent reporting to various regulators on overlapping matters.

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

No comments.

Question 8: What are your views on the proposed time frames for data breach notifications to affected individuals and to PDPC?

No comments.

Other Comments:

Paragraph 6.6 – Obligations of Data Intermediary

We wish to seek clarification on Paragraph 6.6 of the Consultation Paper where the PDPC proposes that an organisation's data intermediary ("DI") is required to ***immediately*** inform the organisation when there is a data breach.

We are of the view that it is not feasible for the DI to inform the organisation immediately as time is required for the DI to investigate and assess a data breach prior to escalating the matter to the organisation. We believe that a more practical approach would be to require the DI to inform the organisation as soon as practicable when it experiences a data breach. A reasonable time cap could be imposed to ensure that the organisation is able to undertake expedient assessments to determine whether the data breach meets the criteria for breach notifications under the PDPA and any other law, as well as to take timely remedial actions to mitigate any risks of harm arising from the data breach.