Public Consultation for the Personal Data Protection Act - Singapore Airlines Limited

S/N	Question	Comments / Suggestions
Enhanced framework for collection, use and disclosure of personal data		
1	**Question 1:** *Should the PDPA provide for Notification of Purpose as a basis for collecting, using and disclosing personal data without consent?*	We agree with the proposed amendment as it is likely to result in significant benefits for organisations. It is our understanding that the intents and spirits under the PDPA in respect of maintaining consent for the collection, use and disclosure of personal data won't be undermined in any material manner. We would suggest that the PDPC provides more guidance on (i) situations where it is impractical to obtain consent, (ii) identify the adverse impacts on individuals, and (iii) the appropriate measures that organisations should take to mitigate the risks. It would also be useful to receive more guidance as to the procedure for such notification (e.g. timeline, etc.)
	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)?*	Conditions are good to have, perhaps they may serve as indication as to the Commission's expectations. We would humbly submit for the Commission's consideration to set out additional conditions, other than those mentioned, e.g. when consent has already been previously obtained by a counterparty.
2	**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?*	We agree with the proposed amendment. However, having to conduct a risk and impact assessment, such as a DPIA, might not always be appropriate and practical, and in particular when the request for such processing stems from a legal requirement. PDPC should provide more guidelines as to when a risk assessment should be performed.

S/N	Question	Comments / Suggestions
	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)?*	We would suggest that instead of imposing conditions, the Commission may consider setting out instances where reliance may be made on the proposed Legal or Business Purpose approach, e.g., to prevent fraudulent activities be specified in the Act. We also note that a risk and impact assessment is likely be required for this proposed approach.
Proposed mandatory data breach notification regime		
3	**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?*	We generally do not have any objection to the criteria. We would, however, wish to have the following recommendations: • For greater flexibility for the organisations, particularly those who handle the personal data in a large scale, perhaps instead of imposing a prescribed number of affected data subjects, a more qualitative criteria (e.g. % of the customers) may be more preferred. • PDPC should provide more guidance as to the type of harm that will trigger the breach notification. • We note that criteria (i) and (ii) are not cumulative since a breach notification is required as long as 500 individuals are affected although there is no impact or harm to the affected individuals. In this regard, PDPC should also provide guidance as to the number of affected individuals for the assessment of criterion (i). • Finally, PDPC should set out the actions which an organisation and/or the PDPC may take, following notification of a data breach.

S/N	Question	Comments / Suggestions
4	**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?*	Data breach is a serious matter as it may potentially result in serious harm to individual. PDPC should act as single data breach notification party, or at least absorbing some coordinating role, so that organisations need not notify all other Singapore agencies separately.
5	**Question 7:** *What are your views on the proposed exceptions and exemptions from the data breach notification requirements?*	PDPC should provide with a list of exceptions and exemptions and related guidelines Because of the nature of the event, organisations should be able to self-assess whether they fall within an exception or exemption situation. PDPC should not require a formal application process.
		We agree that PDPC should not impose a time cap for breach notifications to all affected individuals.
6	**Question 8:** *What are your views on the proposed time frames for data breach notifications to affected individuals and to PDPC?*	We are generally agreeable to the 72 hours time frame for organisations (from the time the organisation is made aware of the breach). That said, we would suggest that when the breach was caused by an intermediary, the time frame should run from 72 hours from the time the data intermediary provides the organisation with a report on the full extent of the breach. The data intermediary should also be required to notify the organisation immediately upon discovering the data breach. PDPC should indicate a list of information that should be provided by the organization. For avoidance of doubt, this list should be indicative only and organisations should not be penalized if only preliminary information can be provided to PDPC at this stage.