Prudential Assurance Company Singapore (Pte) Limited's response to Public Consultation on Approaches to Managing personal Data in the Digital Economy

Submission date: 05th October 2017

Contact Person: Compliance
Email: Data.Privacy@prudential.com.sg

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

Yes. In particular, we agree with the PDPC's observations in paragraph 2.3 that the lengthy or broadly worded notices may not allow the individual to provide meaningful consent. In the context of insurance forms, the content of the form is already very lengthy – the addition of lengthy PDPA notifications worsens this problem.

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)?

Yes. The proposed Notification of Purpose approach should be subject to conditions. Proposed conditions are when it is impractical to obtain consent and not expected to have any adverse impact on the individual.

In complying with the 2nd limb of the conditions (i.e. not expected to have any adverse impact on the individuals), it would seem that some form of risk and impact assessment would need to take place (as elaborated on in paragraph 3.10). However, it is unclear how extensive such an assessment should be. It would be helpful if the PDPC could provide an example highlighting the extensiveness expected of organisations when conducting such risk assessments. It would also be helpful if the PDPC could provide a few illustrative examples as to what constitute "measures to mitigate the risks when relying on Notification of Purpose…"

As for the first example in paragraph 3.11, this seems to be a very rare occurrence – where the organization does not even collect the contact information of its customers. In order to clarify, is it the PDPC's view that if the organization actually had the contact information of its customers, the PDPC would expect the organization to obtain fresh consent from such customers, instead of relying on the Notification of Purpose approach (as detailed in paragraph 3.11)?

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?

Yes. We agree that collection, usage and disclosure for personal data without consent and notification should be provided for Legal or Business Purpose.

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)?

Yes. We agree that when it's not desirable or appropriate to obtain consent and benefit s to the public (or a section thereof) clearly outweigh any adverse impact or risks to the individual.

However, we would like to clarify on the 2nd limb of the conditions. The use of the word "clearly" seems to suggest that the balancing exercise goes beyond that of a simple weighing on a balance of probabilities. May we clarify whether the PDPC intends for this higher standard to be applied?

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 agree on data breach notification to be sent to affected individuals whose data allows identifying the individuals. We agree on the proposed number of more than 500 affected individuals 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?

We agree on the proposed concurrent submission of data breach notification to the law enforcement agency and PDPC.

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

We agree on the technological protection exception and the law-enforcement exception.

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

Our processes may involve data intermediaries and with complex system structure, to assess the extent of the breach impact would require more time than the proposed 72 hours, we would proposed the notification period to be of no later than 5 business days.