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?

Para 3.17 of the Consultation paper provides that:

"As a safeguard for individuals, PDPC proposes for organisations that wish to collect, use or disclose personal data without consent and notification for a Legal or Business Purpose, to undertake measures to identify and minimise the risks to the individual from the collection, use or disclosure of personal data. In this regard, a risk and impact assessment, such as a DPIA, will need to be conducted to assess the risks and impact of the intended collection, use or disclosure of personal data to the individual."

1. We should be grateful if the PDPC clarify: When data is shared among different organisations for a Legal or Business Purpose (eg. within an industry body, with each member contributing data in their respective possession), who would be responsible and accountable for the DPIA, and would this DPIA be taken to bind each of the contributors?

2. We should also be grateful if the PDPC would clarify whether the proposed exemption will extend to the collection, use or disclosure of personal data of individuals who may not be the specific subject of the relevant Legal or Business Purpose (eg. possible/ suspected victims of fraud)?

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?

3. We should be grateful if the PDPC would provide detailed and specific guidance on the basis of the risk assessment to be undertaken.

    a. We agree that a data breach that involves personal data such as NRIC number, health information, financial information or passwords would be considered to pose a risk of impact or harm to the affected individuals and that notifying affected individuals will enable them to take the necessary steps to protect themselves from the risks or impact from the data breach.

    b. However, it is also possible that the inadvertent or unintended disclosure of say, just e-mail and telephone number without more may nonetheless expose the affected individuals to identity theft through phishing/ malware. Would this risk be deemed significant enough to warrant notifying affected individuals?

4. We should be grateful if the PDPC would consider more than one metric for the determination of what would qualify as a significant breach. For example:

    a. A data breach arising from a cyber-attack may be considered significant no matter how much persona data was compromised.

    b. A string of data breaches over a short period of time may need to be considered in totality and not as individual incidents.

    c. A data breach that resulted in the disclosure of the sensitive personal data of, say 50 affected

individuals (ie. NRIC number, health information, financial information or passwords) may be more significant than a data breach that resulted in the disclosure of say, just the telephone number of >500 affected individuals without more.

d. It may be useful to apply a benchmark to determine significance: 500 out of a database of say 500,000 data owners may not be as significant as 500 out of a database of say 5,000 data owners.

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

Para 6.10 of the Consultation Paper provides for a "technological protection exception, where the breached personal data is encrypted to a reasonable standard".

5. We should be grateful if the PDPC would clarify whether this exception would apply to data that is encrypted whilst in storage but which is compromised whilst in transmission (ie. when said data is in clear).

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

6. We applaud the PDPC's intention not to prescribe a specific time frame beyond 'as soon as practicable' to notify affected individuals. No two sets of circumstances surrounding a data breach will be identical, and the impacted organisation will need some lead time to undertake requisite analysis, determine impact, confer with the authorities or regulators (if applicable), establish a communication plan, mobilise resources, etc before notification can be effected in a manner that will minimise confusion and panic.

7. In relation to the proposed time frame to notify the PDPC no later than 72 hours from the time an organisation is aware of the data breach. For breach notifications to PDPC, we should be grateful if the PDPC would clarify when the 72 hours will start to count, bearing in mind:

   a. In the context of a cyber-crime, it may take several weeks, if not months, after the event before the data breach is discovered.

   b. Thereafter, it may still take several weeks of forensic work before it can be conclusively determined if the data breach resulted in any loss of data.

Additional Question

8. We should be grateful if the PDPC would provide some guidance on what would constitute an appropriate discharge of the obligation to notify affected individuals. Specifically:

   a. Would a media statement without more be considered sufficient (bearing in mind that not all impacted organisations may wish to issue a media statement)?

   b. If affected individuals are to be notified by telephone:
      (i) How many unsuccessful attempts should the organisation make before it is deemed

to have discharged the obligation to notify the relevant affected individual?

(ii) Does the organisation have an obligation to ascertain if the telephone number still belongs to the affected individual?

(iii) How should the organisation deal with telephone numbers that are no longer current?

c. If affected individuals are to be notified by e-mail:

(i) Does the organisation have an obligation to ascertain the currency/ validity of the e-mail in question?

(ii) Does the organisation have an obligation to ascertain if the e-mail is read?

(iii) How should the organisation deal with e-mails that are no longer current?