NUHS
National University
Health System

PDPC's Public Consultation on Approaches to Managing Personal Data in the Digital Economy

Feedback provided by the National University Health System Legal Office

5 October 2017

Contact

Simon Cheong
Group General Counsel
National University Health System Pte. Ltd
(Co. Registered No: 200801778C)
1E Kent Ridge Road,
NUHS Tower Block,
Level 13, Singapore 119228
D: 6772 7889 M: 90180507 F: 6778 2760
Email: simon_cheong@nuhs.edu.sg

Reshna Shah
Senior Legal Counsel
D: 67161952
Email: shah_reshna_shantilal@nuhs.edu.sg

NUHS
National University
Health System

5 October 2017

To : The Personal Data Protection Commission

Re: Public Consultation For Approaches To Managing Personal Data In The Digital Economy - Issued 27 July 2017

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

This option may be preferable from an organisation's operations perspective as it may streamline processes. However, there are some uncertainties that need to be addressed if the proposal is implemented, which we have briefly stated below for PDPC's consideration.

It appears that individuals may not have much control over their personal data because once an organisation gives notification they will be able to collect personal data irrespective of whether the individual consents or not. Unless an individual objects to the collection of his data, withdrawal of consent will not be applicable. It may become impractical for organisations to allow individuals to opt out if they do not wish the organisation to collect their personal data and administratively burdensome to implement.

There is a possibility that organisations may not provide adequate notification to individuals for the purpose of collection of their personal data. If organisations are required to perform their own assessment of risk impact to the individuals, this can be very subjective and can vary from one organisation to another. Organisations accountability becomes an issue. How are organisations supposed to be held accountable if an individual complains that proper notification was not provided? PDPC will need to provide guidance to organisations on assessing risk of impact or harm to affected individuals.

The PDPA has been in effect for 3 years and most organisations have put in place processes to obtain consent (i.e. if deemed consent does not apply) prior to collecting, using or disclosing an individual's personal data. Organisations have already allocated considerable financial and manpower resources to change processes in order to comply with the existing PDPA consent, notification/purpose obligations. Organisations will be compelled to review and change their processes again.

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)?

Although this proposal appears to be a balanced approach it may pose implementation problems. It appears that under this proposal individuals shall be able to retain control over their personal data as their consent would be necessary in most circumstances prior to the collection, use and disclosure of their personal data by an organisation. At the same time organisations will be able to collect use and disclose data when it is impractical to obtain consent and if there is no adverse impact to an individual.

However, when conditions are imposed, it may become too restrictive to implement. Conditions imposed may require an additional layer of compliance. Organisations will need to ascertain the criteria of when it is deemed to be "impractical to obtain consent" and "adverse impact" before invoking this proposal. This can be very challenging from an operational and interpretation perspective and PDPC will need to provide examples and guidelines for this purpose.

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?

This exception would be welcomed as organisations would be able to share/ disclose personal data amongst their own subsidiaries, business entities and departments without having to obtain further consent from individuals. Hopefully, under this exception, organisations are also able to share data with public agencies upon the public agency's request without having to obtain further consent from the individuals. However, PDPC may need to provide sectorial guidelines by providing examples on when this exception can be invoked. "Legal" and "Business Purpose" may need to be defined.

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)?

Preference is not to have conditions imposed to avoid being too restrictive in the implementation of this exception.

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 feel that there should not be a two tier approach for reporting data breaches. Only data breaches which pose a risk of impact or harm to the affected individuals should be reportable and this should be subject to a threshold of 500 or more. Data breaches that do not pose any risk of impact to the affected individual should not be reportable even if scale of the data breach is significant. PDPC will need to provide guidance to organisations on assessing risk of impact or harm to affected individuals.

The consultation paper does not address what are reportable breaches. It provides a general statement that data breaches that involve NRIC numbers, health information, financial information or passwords would be considered to pose a risk of impact or harm to the affected individuals and should

be reportable. Not all data breaches should be reportable. For example an invoice sent to a wrong individual due to a clerical error is a common incident in most organisations and such a data breach should not be reportable. These are day to day operational matters which organisations should resolve by changing their processes. If mandatory reporting is introduced then PDPC should work with specific industries to identify the types of data breaches relevant to the industry that should be reportable. Otherwise, it will become an overly onerous regulatory burden on businesses in Singapore.

PDPC has also stated that notifying affected individuals will enable them to protect themselves from risks or impact of the data breach. There is no clarity on how individuals may be able to protect themselves? On the contrary, individuals may become disgruntled and this may have a negative impact on the organisation.

Also, the consultation paper does not address the impact on organisations of mandatory notification of data breaches. Will this open floodgates to legal suits or class actions against organisations? What support will PDPC provide to organisations?

Mandatory data breach notification will also mean that organisations will have to expend more dedicated resources in addition to their own escalation processes for handling data breaches. PDPC should take this into consideration, particular for small to medium size organisations who may not be in a position to allocate resources and propose solutions to help them. Also, most DPOs and their representatives will need guidance / training to comply with this obligation.

The consultation paper is also silent on the penalties that will be imposed on organisations who breach this obligation. It is important to understand what are the repercussions to organisations if they fail to report a data breach.

Question 6: What are your views on the proposed concurrent application of PDPA's data breach notification requirements with that of other laws and sectorial regulations?

Need industry specific examples to better understand the application of concurrent laws.

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?

The proposed cap of 72 hours to report to PDPC may not give organisations enough time if they need to confirm the breach and obtain the necessary details of the incident. Organisations upon request to PDPC should be given more time if need be.

The proposal to notify individuals based on "as soon as practicable" gives more leeway to organisations. Organisations would usually need the time to confirm and obtain the necessary details of the breach before the individuals are notified.