SYMANTEC COMMENTS ON PUBLIC CONSULTATION BY SINGAPORE'S PERSONAL DATA PROTECTION COMMISSION ON APPROACHES TO MANAGING PERSONAL DATA IN THE DIGITAL ECONOMY

Comments

We at Symantec appreciate the opportunity to provide comments on public consultation by Singapore's Personal Data Protection Commission (PDPC) for approaches to managing personal data in the digital economy.

The fact that this consultation is being undertaken barely three years after the Personal Data Protection Act (PDPA) came into effect from 1 July 2014, demonstrates PDPC's readiness to keep abreast of rapid changes caused by technological innovation and new policy scenarios unfolding.

Kindly allow us to respond to the respective questions outlined in the consultation paper below.

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

Yes.

As the consultation paper rightly notes there are situations where relying on consent as the only basis for collection, use and disclosure of personal data is impractical and/or undesirable. In other jurisdictions as well, consent is not the only legal basis for data collection. It is, therefore, important to ensure that such flexibility also exists in Singapore.

Moreover, the ubiquitous presence of technology and network connectivity calls into question whether consent can be even easily and practically collected from consumers or whether such consent is sufficiently informed.

The Notification of Purpose basis would help strike a finer balance between an individual's right to retain control over their personal data and the need for organisations to collect, use and disclose person data in fair and appropriate circumstances.

Finally, we suggest that PDPC should make it clear whether the regime intends to give individuals a right to object to and/or challenge whether the notification of purpose is valid, and if so when and how such objection or challenge should be raised and resolved.

Generally speaking, laws in other jurisdictions that permit collection via notification also specify an opt-out regime or provide that an individual may seek access to, correction and/or deletion of their personal information (see for example the approach under British Columbia's Personal Information Protection Act where individuals would be given a reasonable opportunity to decline when notified of the purposes of the intended collection, use or disclosure).

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.

Even if consent is not used as the basis for collection, the purpose for which the personal data is collected needs to be limited, specific, proportionate and disclosed to the data subject. Reasonable conditions are necessary to ensure that the proposed notification of purpose approach is not abused and used as an excuse by organizations to bypass the generally recognized need for consent.

The conditions currently proposed are logical and fair. However, there needs to be clearer guidance from the PDPC on when organisations can rely on the Notification of Purpose approach without consent. In particular:

- **(i) the level of "impracticality" required for notification of purpose to be sufficient; and**
- **(ii) level of adverse impact on individuals to render the notification of purpose invalid.**

We note that ambiguity in this regard has been a problem in other jurisdictions.

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.

Indeed, there are situations where either seeking consent is undesirable or where the benefits to public at large significantly outweigh the adverse impact or risk to an individual. For example, there can be situations where cybersecurity providers need to share data with each other to deal with cybercrimes.

This would also bring the Singapore regime into closer alignment with the approach in other jurisdictions (e.g. the concept of "legitimate interest" exception under the EU data protection regime).

It should be noted, however, that collection for "business purpose" should not be used as an excuse to justify (a) collection or (b) business practices that are questionable or that may substantially harm the privacy of individuals.

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. The proposed Legal or Business Purpose approach should be subject to conditions.

However, there needs to be more specificity on the conditions currently proposed:

- **(i) concepts on "desirability" and "appropriateness" are subject to different interpretations and may lead to uncertainty and confusion for organisations;**
- **(ii) the level of adverse impact that must bear upon on individuals to render the Legal and Business Purpose invalid is also unclear.**

We suggest that when considering "desirability", factors such as cost, state-of-the-art technology and the proportionality of the effort needed to obtain consent should be carefully considered by the PDPC in specifying and interpreting the applicable criteria.

Finally, we think that there should be a requirement for organisations to provide a written statement or evidence, if requested by PDPC, which formally demonstrates the reason(s) for collection and use under this mechanism. This appears to be the Data Protection Impact Assessment alluded to by the PDPC. We look forward to the publication of the "Guide to Data Protection Impact Assessments (DPIAs)", preferably after a separate public consultation for the same.

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?

According to Symantec's Internet Security Threat Report, 1.1 billion identities were exposed globally in 2016, almost double as compared to 2015. Almost 40% of information lost in data breaches in 2016 was personal information. This brings into sharp focus the importance of data breach notifications.

<u>Proposed criteria for mandatory breach notification</u>

(1) Where data breach poses any risk of impact or harm to the affected individuals

This criterion does reflect the policy behind the mandatory data breach notification, which is to keep PDPC informed in a timely manner where the data breach might cause public concern or where there is a risk of harm to a group of affected individuals.

However, the term "*<u>any</u> risk of impact or harm to the affected individuals*" is unclear, potentially very broad and far-reaching.

We would suggest the following:

(i) **Clarify the applicable standard in assessing the risk of impact or harm (e.g. Australian approach - "*a reasonable person would conclude that the access, disclosure, or loss is likely to result in serious harm to any of the individuals to whom the information relates").***

(ii) **Obligation to notify should only be triggered in circumstances where it is "*<u>likely to result in significant impact or risk</u> of harm*", instead of "*<u>any</u> risk of impact or harm"*, to avoid imposing overly onerous regulatory burdens on organisations to report insignificant data breaches.**

(iii) **Provide guidance or specify in the Act the types of data breaches, which would ordinarily be considered to trigger the notification obligation (e.g. data breaches involving personal data such as Identification Card number, health information, financial information or passwords).**

(2) Where scale of data breach is significant (i.e. involving 500 or more affected individuals)

Imposing a numeral threshold may not be feasible and appropriate as there is no one-size-fits-all figure to suit all industries and contexts (e.g. banking sector where 500 or more affected individuals would be met easily vs. the healthcare sector).

A data breach impacting 50 people that would compromise the full details of their medical history may prove significantly more damaging than a data breach impacting 600 individuals in which their names and addresses are compromised.

We think that it would be preferable to factor in the level of risks associated to the breach (irrespectively of the number of individuals), instead of specifying a numeral threshold to trigger a data breach notification. Hence, we think that there should be a requirement for organisations to provide a written statement or evidence, if requested by PDPC, which formally demonstrates the reason(s) for not providing notification.

<u>Other general comments on mandatory breach notification:</u>

Disclosure of Personal Data to PDPC

In certain circumstances, disclosing that the breach has occurred may necessarily involve the disclosure of personal data and other information. While there would usually be a confidentiality exception in the contract with the customer for disclosure required by law, it would be helpful if the PDPA makes it clear that organisations are legally obliged to notify PDPC of such data breach, even if it entails the disclosure of personal data and other information.

Guidelines on minimum security requirements

Finally, we wish to highlight that, for the breach notification obligation to be truly effective, data controllers need to be able to detect breaches in a timely manner. We suggest setting out guidelines for data controllers on the basic security requirements that they must put in place to help them protect personal data and detect breaches (e.g. if an organisation is collecting passwords, the same must be subject to a certain minimum level of encryption).

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?

To the fullest extent possible, the breach notification obligation under the PDPA should be aligned with those under other sectoral regulations (if any), to avoid unnecessary duplication, ambiguity and confusion.

We therefore welcome the suggestion that the notification requirements under the PDPA would be met if:

(i) the organisation submits to the PDPC the same notification or copy the PDPC in its notification to the sectoral or law enforcement agency; and

(ii) the organisation notifies the affected individuals according to the requirements under another written law and informs PDPC of the data breach.

The PDPA should explicitly provide that it is intended to be the overarching data protection law in Singapore. For compliance and efficiency purposes, it would also be helpful to have a schedule to the PDPA that sets out other sectoral laws and regulations that require notification, as well as the circumstances (if any) in which notification under the PDPA trumps the notification requirements under other sectoral laws/regulations (i.e. hierarchy of notification obligations).

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

The proposed exemptions are reasonable and aligned with global best practices.

As for the Technological Protection Exception (where the breached personal data is encrypted to a reasonable standard), our comments are as follows:

First, there needs to be clear guidance on what constitutes such "reasonable standard".

Second, we would highlight that the effectiveness of the encryption technology is dependent upon the size and control of the encryption keys, as well as the implementation of the same.

The technological protection exception should only apply if the organisation has adopted (and can demonstrate) sound security baseline practices and comprehensive deployment of security technologies in a defense-in-depth architecture.

Without a clear link between baseline security and the obligation to notify security breaches, there is a risk that this provision results into less protection for the data and this exception can be misused.

Third, we would suggest that specific powers be vested with the PDPC to give an exemption from notification requirements where it is satisfied that it is reasonable to do so (on a case by case basis).

For example, if an organisation has taken remedial action to rectify an eligible data breach or potential eligible data breach, and a reasonable person would conclude that such data breach is not likely to result in serious harm, the Commission may grant an exemption such that the organisation is not required to notify the affected individuals. This would incentivize organisations to take pro-active measures for securing and protecting personal data.

We believe that the PDPC should commit to a conciliatory approach to encourage organisations to work together with the PDPC towards a remedy in the event of a data breach.

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

Notifying individuals and PDPC

We think that the proposed time frame to notify PDPC ("*within 72 hours from the time an organisation becomes aware of the data breach*") and individuals ("*as soon as practicable*") is in line with the approach adopted in several other jurisdictions.

However, we suggest that the PDPA should be clear in this aspect that it is referring to a confirmed data breach involving "personal data" or "sensitive data", and not either (a) a suspected data breach; (b) a threatened data breach; or (c) a loss of data that does not involve personal data.

Organisations may become aware of a suspected breach, then have to undertake investigations to confirm whether an actual breach has occurred, whilst undertaking timely technical remediation.

In summary, we believe that the time frame should only run when (i) an organisation becomes aware of a confirmed breach involving personal / sensitive data; and where such breach poses a real risk of serious harm to the affected individual(s).

Finally, we note that the time taken for an organisation to detect a data breach will vary, depending on the technological tools in place, the organizational processes and skill sets.

Conclusion

We sincerely hope that our comments would be found relevant and useful. As indicated already in our response all the areas we have provided comments on are areas that we have significant experience on a global scale.

We also appreciate PDPC's preference for obliging the organizations to undertake due diligence with respect to Risk and Impact assessment for the proposed measures rather than being extremely prescriptive about how and what the organizations should do and don't do.

We would be happy to share some additional information on the statistics we have referred to and to follow up and discuss them in more detail either in face to face meetings or by providing additional submissions on any of these points.

Point of Contact in Symantec

For any further query related to this submission, please contact:
Deepak Maheshwari, Director – Government Affairs, India & ASEAN
Email: deepak_maheshwari@symantec.com