Memorandum

5 October 2017

To	Personal Data Protection Commission ("**PDPC**")
From	secretariat@scca.org.sg
Direct Line	(+65) 6636 3628

Singapore Corporate Counsel Association Response to the PDPC Public Consultation dated 27 July 2017

Dear Sirs and Mesdames

We enclose our response to the PDPC public consultation for approaches to managing personal data in the digital economy (the "**Consultation**").

This response does not represent the position of the entire membership of SCCA, nor that of any company for which SCCA members act as in-house counsel. It is recognised that a number of SCCA member companies may have provided comments to the Consultation directly or through other organisations/representatives. For the purposes of this response, "members of SCCA" refer to only those members who contributed views to SCCA, which have been collated in this response.

Where SCCA has not responded to any proposed amendment or issue in the Consultation, this should not be taken as any indication that SCCA has agreed, accepted or adopted the same. SCCA is not in a position to express any comment or response because feedback has not been obtained or forthcoming.

We thank the PDPC for the opportunity to comment on the proposed amendments to the Personal Data Protection Act 2012 (the "**PDPA**") presented in the Consultation, and would welcome any further dialogue with the PDPC on any of the points we have raised.

Please contact secretariat@scca.org.sg or Adrian Fisher (adrian.fisher@linklaters.com) should you have any questions.

Singapore Corporate Counsel Association

Part I: Enhanced framework for collection, use and disclosure of personal data

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

We welcome the PDPC's proposal to broaden the bases under which organisations may collect, use and disclose personal data without obtaining consent from individuals.

We think that the Notification of Purpose is an appropriate basis under which organisations may collect, use and disclose personal data without obtaining consent from individuals. Other jurisdictions with data privacy regimes of more than 10 years, such as the Australian Federal Privacy Act 1988 (Cth) and the Hong Kong Personal Data (Privacy) Ordinance, are already allowing organisations to collect their personal data without consent by notifying the individuals of the purposes of the collection, use or disclosure.

Furthermore, this new basis is not without checks on organisations, as organisations are required under the PDPA to only collect, use and disclose personal data for purposes that a reasonable person would consider appropriate in the circumstances and the individual would still have the ability to opt out of a particular use, collection or disclosure (as mentioned in paragraph 3.9 of the Consultation).

In a digital economy where a consent based approach for collection, use and disclosure of personal data has proved to be challenging for organisations, the introduction of the Notification of Purpose basis would allow organisations to adapt to the fast-changing digital environment and maximise the potential in personal data collected without going through the burdensome process of obtaining new consents.

Question 2. Should the proposed Notification of Purpose approach be subject to conditions (i.e. impractical to obtain consent and not expected to have any adverse impact on the individual)?

General comments

In jurisdictions such as Australia and Hong Kong, an organisation can collect personal data by notifying the individuals of the purpose of collection, use or disclosure of their personal data without consent and without being subject to the conditions as proposed in the Consultation.

The conditions that are proposed to be attached to the Notification of Purpose option (as discussed further below) are broadly worded. This may have the unintended consequence of organisations, in an attempt to satisfy these conditions, taking a conservative view on when they apply and therefore continuing the current phenomenon of organisations resorting to lengthy and verbose consent statements when obtaining consent from individuals.

We respectfully submit that the PDPC consider removing the conditions attached to the Notification of Purpose approach in line with that taken in other jurisdictions that have applied the Notification of Purpose option.

If this approach is not accepted, we include comments below on the PDPC's proposed conditions.

Impractical for organisations to obtain consent

The application of the conditions as currently proposed is unclear. In particular, the concept of "impracticality" is nebulous and many organisations would struggle to determine what would constitute an "impractical" situation to obtain consent. In a digital environment where information may be collected through various means and from a large number of individuals, it may be difficult to objectively assess whether or not it is "impractical" to obtain consent. Other jurisdictions which use the Notification of Purpose option also do not include this condition.

We respectfully submit that the PDPC consider not to include such a condition in the proposed Notification of Purpose approach, or in the alternative, to provide detailed guidance on interpreting this condition. The SCCA would be happy to be involved in preparing guidelines on this issue.

Not expected to have any adverse impact on individuals

The condition that the collection, use or disclosure of personal data must not be expected to have an "adverse impact" on the individuals would also be difficult for organisations across the board to apply consistently.

It is unclear as to what would constitute an "adverse impact" on individuals. Would the test be a subjective one or an objective one? Some members of the SCCA are concerned that if a subjective interpretation of this condition is adopted, the wording "adverse impact" may be interpreted very broadly to prevent organisations from relying on this Notification of Purpose approach, even though the purpose has been notified to the individual in accordance with the PDPA. In addition, where a large and disparate group of individuals are involved, it would also not be possible to apply a subjective test as the circumstance of each individual may not be known to the organisation. The risk of there being an adverse impact on individuals is also mitigated by the inclusion of an opt-out mechanism, which the SCCA supports. In effect, if organisations provide adequate notification to individuals (which they should do to obtain the benefit of the Notification of Purpose option), an individual will then be free to decide whether or not to allow an organisation to use their personal data for that purpose.

We respectfully submit that the PDPC consider such a condition be removed from the proposed Notification of Purpose approach, or in the alternative, include objective criteria that organisations may use to assess whether or not there is an adverse impact and examples of such "adverse impact".

Risk and impact assessment

The proposed requirement on organisations to conduct a risk or impact assessment is a concern for the following reasons.

Firstly, it is unclear as to what the risk and impact assessment entails and the consequence for an organisation that fails to conduct the assessment properly. For example, will the organisation

be subject to a fine or sanctions from the PDPC, or will failure to conduct the assessment mean that the organisation is unable to rely on the Notification of Purpose approach?

Secondly, the proposed requirement would impose additional administrative burden on the organisations, particularly on smaller organisations. Where an organisation's use of personal data may be very small scale (e.g. just relating to a single individual), to carry out a formal risk assessment for every situation would be disproportionate. Many members of the SCCA are concerned that smaller organisations in Singapore may struggle with such a proposed requirement, particularly when it is unclear as to how extensive this assessment would need to be.

Thirdly, organisations regulated by other laws and sectoral regulations are already required to provide risk and impact assessments to the relevant regulators, such as under the Technology Risk Management Guidelines issued by the Monetary Authority of Singapore ("**MAS**"). While the purpose of the proposed amendments is to ease the administrative burden of obtaining consents currently required to use personal data, the mandatory risk and impact assessments may be seen as a step backwards, imposing additional administrative and compliance obligations on organisations, particularly if the Notification of Purpose option is conditional on the risk and impact assessment.

We respectfully submit that the PDPC consider removing the requirement on organisations to conduct a risk and impact assessment when relying on the Notification of Purpose approach.

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 welcome the proposed Legal or Business Purpose approach.

The Legal or Business Purpose is an appropriate basis under which organisations may collect, use and disclose personal data without obtaining consent from individuals. Organisations should be allowed to collect, use and disclose personal data under circumstances which are necessary for the legitimate interests of the organisations. It is also used in other jurisdictions, particularly the United Kingdom and the EU, and would therefore align the PDPA with the laws of other significant economies.

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)?

General comments

The conditions attached to the Legal or Business Purpose are open to many interpretations which may result in inconsistent interpretations by organisations. Members of the SCCA have also expressed concern that organisations would have difficulties satisfying both conjunctive conditions.

Not desirable or appropriate to obtain consent

We would be grateful if the PDPC would provide more clarity on the situations where obtaining consent would not be "desirable or appropriate". Except in the most obvious situations, such as the example cited in paragraph 3.16 of the Consultation, there are many other situations where it may be considered undesirable or inappropriate to obtain consent but where, without further guidance, organisations may be tempted to take a conservative view to ensure compliance with the PDPA. High operation costs or unduly burdensome logistics may be regarded as "undesirable" for organisations to obtain consent.

We respectfully submit this condition should be removed from the proposed Legal or Business Purpose approach. While the SCCA believes removing this condition is the preferable approach, if the condition remains, the SCCA submits that the PDPC should release detailed guidance on interpreting this condition with examples of situations where obtaining consent would not be "desirable or appropriate".

Benefits to the public outweigh any adverse impact or risks to the individual

The condition that the "benefit to the public" of the collection, use or disclosure of personal data must "clearly outweigh any adverse impact or risks to the individual" is a high threshold for organisations to meet. Without clear guidance, it is difficult for an organisation to determine whether its use of personal data will "clearly" benefit the public.

The PDPC suggests that the Legal and Business Purpose basis is intended to broaden the circumstances for which an organisation may collect, use or disclose personal data without consent under the PDPA. However the word "clearly" suggests that this condition can be satisfied only in obvious circumstances, such as where national security or other public interests are involved. Some SCCA members have expressed concerns that they would not be able to rely on this basis in situations falling short of these obvious circumstances as a result.

Similarly, the reference to reliance on the Legal or Business Purpose only being allowed where the benefit to "the public (or a section thereof)" outweighs the risk to the individual will be difficult to apply in practice. This condition is also in some ways counter to the principle behind the Legal or Business Purpose as an organisation's legal or business purposes will not always be completely aligned with the public interest. The SCCA submits that the more appropriate threshold for this condition is that the legal and business purpose of the organisation must not be outweighed by the interests of the relevant individual. This would align with the position in the General Data Protection Regulation (2016/679) ("**GDPR**").

We respectfully submit that the threshold for this condition to apply should be reformulated. Particularly, the SCCA submits that the condition should apply if an organisation's legal or business purpose is not outweighed by the interests of the relevant individual. If this approach is adopted, we would be grateful if the PDPC could provide examples and guidance of Legal and Business Purposes, similar to the examples of legitimate interests of a data controller found in Recitals 47 to 50 of the GDPR.

Overseas transfer of personal data and cloud

Cross-border transfer of personal data is ubiquitous in the current digital economy. One SCCA member raised a question on whether a cross border transfer of personal data or a transfer of personal data to cloud service providers with overseas storage facilities would fall within the definition of a "business purpose", such that the Business Purpose basis would be an exemption for the cross-border obligations under the PDPA.

We would be grateful if PDPC would provide more guidance on the scope and interpretation of the Business Purpose, particularly with respect to cross-border transfer of personal data and the conditions on cross border transfer of data under the Personal Data Protection Regulations 2014.

Adverse impact and risk and impact assessment

Our comments outlined above in our response to Question 2 with respect to the use of the words "adverse impact" and the proposed risk and impact assessment would apply here as well.

Part II: Mandatory data breach notification

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 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?

Definition of "data breach"

"Data breach" is currently not defined in the PDPA or the proposed amendment, although it is briefly defined in the PDPC's Guide to Managing Data Breaches dated 8 May 2015 as the unauthorised access and retrieval of information that may include corporate and personal data. Under the GDPR, a "personal data breach" is defined as a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. If a mandatory data breach notification obligation is to be included in the PDPA, we would be grateful if the PDPC would provide a definition of what constitutes a "data breach". This would provide clarity for organisations when determining whether the occurrence of a particular event would constitute a "data breach" that may require notification to the PDPC and/or other parties. We would be happy to suggest a definition to the PDPC.

Clarity on "risk of impact or harm to affected individuals"

We appreciate the useful notes in the Consultation which clarify the types of data that would be considered to pose a "risk of impact or harm to affected individuals". However, as currently proposed, this criterion imposes a very low threshold on notification. The SCCA submits that the criterion be amended to refer to a data breach "that a *reasonable person* would consider is likely to result in a serious harm to affected individuals", as has been adopted in the recent amendments to the Australian Privacy Act 1988. A number of relevant factors may be included for organisations to assess whether "serious harm" is likely, including the kind of information in

question, sensitivity of the information, the security protections in place, the type of person or people who obtained the information and the nature of the harm.

Qualitative vs quantitative criteria

We respectfully submit that imposing qualitative criteria (as is already introduced by the first criterion proposed by the Consultation and mentioned above) for breach notification would be more appropriate than a quantitative measure. A quantitative measure is only one of the ways to analyse the risk and impact of a data breach. Imposing a quantitative threshold for mandatory notification trigger is inappropriate. This is akin to having a "one size fits all" model for all organisations but in reality, the risks of data breach associated with one organisation would differ (and in some cases significantly) from another. Other factors to be considered include nature of personal data and the individuals affected.

Some SCCA members noted that imposing a quantitative threshold of 500 affected individuals for notification would mean large organisations that handle significant amounts of data would be required to notify all or nearly all occurrences of data breach. This is because few data breach of these organisations would involve personal data of fewer than 500 individuals. On the other hand, small organisations may suffer serious data breaches but not meet the threshold simply because of the smaller size of their operations or customer base. The effect of this quantitative threshold would impose the burden of notification on only large organisations, while exonerating smaller organisations from making such notifications.

It is also worth considering the data that the quantitative criterion is associated with. We would be grateful if the PDPC could clarify if the 500 affected individual criterion is to be associated with only structured records of these individuals but not just contact details. Otherwise, every loss of a mobile device will be caught as it is likely that such a mobile device would contain email addresses of more than 500 individuals.

We respectfully submit that the PDPC delete the second criterion for notification of data breach and rely simply on the first criterion (with our suggested amendments), which refers to the risk of impact or harm on individuals.

Consequences for failure to notify

We respectfully submit that the PDPC set out clearly the consequences of an organisation failing to comply with the mandatory data breach notification obligation.

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?

There is a concern that the proposed concurrent notification to the PDPC or other sectoral regulators (such as the MAS) may impose more onerous reporting requirements on the organisation due to more stringent notification requirements imposed under other laws or sectoral regulations.

For example, under the MAS Notice 127, financial institutions are required to notify the MAS as soon as possible but not later than 1 hour of an event involving a system which compromises

the security, integrity or confidentiality of customer information. If a data breach of this nature occurs, the organisation would need to notify the MAS within 1 hour (i.e. within the same time frame and in accordance with the notification requirements under MAS Notice 127), even though the current proposed allowable notification time frame under the PDPA regime is 72 hours from the time the organisation is aware of the data breach. The notification requirements under the other written law may not be relevant to the notification requirements for a data breach under the PDPA.

Due to the concurrent notification requirement, the organisation would also need to work closely with both regulators for the same data breach. This would be an additional burden on the organisation for the same data breach. Where an organisation works with more than one regulator to manage the same data breach incident, there may be conflicting instructions or directions provided by different regulators.

We respectfully submit that the PDPC consider where an organisation has made a data breach notification to a regulator other than the PDPC, the organisation is not required to notify the PDPC or if notification is required, the organisation is only required to work with one regulator to manage the data breach incident.

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

Law-enforcement exception

Personal data in a digital economy, particularly with the increasing use of cloud, is no longer kept within a single jurisdiction. Organisations often need to grapple with the challenges in the application of the laws of other jurisdictions, including investigations of foreign law enforcement bodies or regulators on the personal data that they control or possess.

We would be grateful if the PDPC would provide greater clarity as to whether the "law enforcement investigations" exception would apply to law enforcement investigations occurring in other jurisdictions, thus exempting organisations from making a mandatory data breach notification where notification to affected individuals is likely to impede law enforcement investigations in any country.

Technological protection exception

We welcome the exception to notify individuals for breached personal data which is encrypted to a reasonable standard. However, we respectfully submit that the PDPC consider applying this exception to notification to the PDPC as well. If the breached personal data is reasonably encrypted, the risks associated with unauthorised disclosure of personal data will be greatly mitigated. As a result, there may not be the need or relevance for the PDPC to be notified of such a data breach.

We would be grateful if the PDPC would provide guidance on what would constitute a reasonable standard for encryption.

Security weakness exception

We respectfully submit that the PDPC consider including an exception to notification where a security weakness in the organisation is being remedied and a notification would prejudice the organisation's attempt to remedy the security weakness. Reporting on such security weakness may expose the organisation to other attacks leading to more data breaches.

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

We respectfully urge the PDPC to consider extending the 72 hours maximum period for notifying the PDPC of a data breach. Many members of the SCCA have expressed concerns that 72 hours may not be sufficient for organisations to gather information, particularly if the organisations use complicated systems to handle or store large amounts of personal data. In addition, whilst large organisations have the resources to investigate and react to a data breach that occurs over a weekend, many smaller businesses may not be able to do so.

We note that the PDPC in the Consultation appreciates that organisations may require more than 72 hours to confirm the breach and obtain the necessary details of the incident. However, the PDPC still requires such organisations to notify the PDPC with as much information as possible within the 72 hour period and provide the PDPC with the remaining information as soon as possible.

To avoid multiple incomplete notifications from organisations, we respectfully submit that the PDPC consider removing the requirement to notify within 72 hours from the time the organisation is aware of the data breach, or in the alternative extend the maximum period for notification by increasing the maximum period beyond 72 hours or at least amending it to three business days.