Public Consultation for Approaches to Managing Personal Data in the Digital Economy

Cover page

Baker McKenzie. Wong & Leow (**Baker McKenzie**) welcomes the opportunity provided by the Personal Data Protection Commission to provide feedback on the proposed "Approaches to Managing Personal Data in the Digital Economy".

Our submission may be disclosed publicly by the PDPC.

Our contact details can be found below if you have any queries.

Ken Chia
Principal
ken.chia@bakermckenzie.com
+65 6434 2558

Anne Petterd
Principal
anne.petterd@bakermckenzie.com
+65 6434 2573

Baker & McKenzie.Wong & Leow

A member of Baker & McKenzie International, a Swiss Verein
Reg. No. 200010145R
8 Marina Boulevard
#05-01 Marina Bay Financial Centre Tower 1
Singapore 018981
Main: +65 6338 1888
Fax: +65 6337 5100

Comments

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

1.1 At paragraph 3.8, PDPC is proposing a "Notification of Purpose" basis for an organization to collect, use and disclose personal data where:

(a) it is impractical for the organization to obtain consent (and deemed consent does not apply); and

(b) the collection, use or disclosure of personal data is not expected to have any adverse impact on the individuals.

1.2 Prior to the PDPA providing the Notification of Purpose basis for collecting, using and disclosing personal data without consent, we are of the view that PDPC should clarify:

(a) The intent of this approach

(i) Whether the Notification of Purpose is intended to be another exception to the general consent requirement or an alternate basis for the processing of personal data.

Currently, s17 PDPA provides that an organisation may collect, use and disclose personal data about an individual, without consent or from a source other than the individual, only in the circumstances and subject to any condition in the Second, Third and Fourth Schedules.

It is the intention that the Notification of Purpose basis be another exception in the Second, Third and Fourth Schedules, or that s17 be amended?

If so, will the Consent Obligation in s13 also be amended to become a "Lawful Processing" Obligation more in line with the Article 6 EU GDPR which provides for multiple bases for processing.

Further, where there is an overlap between one of the existing exceptions to consent and the new Notification of Purpose basis, can the organisation select the option which has less onerous conditions?

For example, if an organisation has a choice between the business asset transaction exception and the Notification of Purpose basis, can it choose to make an "appropriate" notification after having performed a DPIA rather than complying with the conditions in the Fourth Schedule para 3 (which limit the data being disclosed to only what is necessary for the prospective party to determine whether to proceed with the business asset transaction)?

(b) The scope of this exception

(i) How an organization can determine whether there will be and what the extent of any "adverse impact" will there be on an individual.

For example, could an organisation safely conclude that there would be no adverse impact in a business asset transaction if the new owners confirmed that they would apply the same privacy policy immediately after closing (knowing that they could simply change it later by notice)?

(ii) Whether this applies to any type of personal data collected (e.g. including sensitive personal data).

Presumably the sensitivity of the data be catered for by the DPIA since the organisation will have to implement the necessary measures to mitigate any increased risks when using the Notification of Purpose basis, however we note that in many jurisdictions with a notification regime, explicit consent is still required for sensitive data;

(iii) Whether this applies to personal data collected from a third party source - we presume that this is not intended to circumvent situations where an organization should verify with the individual (or obtain relevant representations or warranties from the third party source) in respect of personal data collected from a third party source;

(c) The implementation of this exception

(i) Whether it would be typically implemented where it would be considered "impractical" for an organization to obtain consent in an "after the fact" situation.

What happens for example if an organization has instead deliberately collected personal data without obtaining the contact information of the individuals - could it still rely on the Notification of Purpose basis? This would allow it to use such personal data for new purposes as long as such use does not result in an adverse impact to the individual and it makes the "appropriate" notifications.

(ii) The means by which notification may be given

The proposal to allow notification instead of consent as described seems to assume there is an ability to contact the impacted individuals to provide notification (but not an ability to obtain consent). Further examples of the contemplated scenarios in each case would be needed to enable businesses to understand the boundaries of permitted activities via notification. For example, does notification have to be sent to the individual or can a practice of updating a privacy policy posted on the business' website be sufficient notice? Might the answer vary depending on circumstances such as how the business usually interacts with its customers and other individuals? For example, an online business might post a notice prominently on its website that could be seen by all customers before they interact with the website - would that be sufficient for notification?

2. 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)?

2.1 Whilst we are of the view that the Notification of Purpose basis should be subject to some conditions, further clarity is needed in respect of the proposed conditions.

2.2 We note that the example provided by the PDPC at paragraph 3.8(b) provides that this Notification of Purpose should not be to "circumvent a prior withdrawal of consent (e.g. target the individual for direct marketing after he had opted out of receiving marketing communications)". We are of the view that this example sets a high threshold of when the exception should not be used and that a clearer example should be provided. In other words, where the individual has opted out, clearly the Notification of Purpose basis should not be used. However, if the individual had not opted in to receive marketing communications in the first place by leaving a check box unticked, could the Notification of Purpose basis still be used? Would the receipt of marketing communications be considered an "adverse impact" on the individual?

2.3 We are of the view that a more forward looking example may be appropriate. Several examples can also be provided to give clear guidance on the intent of the Notification of Purpose approach. For example, in the world of the internet of things, there may be collection of sensor data in an enclosed

area (e.g. a 'shoppers' club' type supermarket may not be able to rely on the publicly available exception) to allow the supermarket to determine a more efficient shelving system by analyzing customer movement through the store. Other data analytic tools or different uses of data to assist the business to use for the purpose of improve its operations and efficiencies would be expected to become available to the business at a later time but may not be covered in the prior consents. We are of the view that the Notification of Purpose would be more applicable to the collection, use and disclosure of personal data in such a context.

2.4 Appropriate conditions, if any, would also be dependent on the scope of the permitted notification. Please see our comments on Question 1 on matters to clarify on scoping the notification.

3. 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?

3.1 At paragraph 3.15, the PDPC has proposed to provide for the collection, use or disclosure of personal data without consent where it is necessary for a legal or business purpose ("**Legal or Business Purpose**") subject to the following conditions:

(a) it is not desirable or appropriate to obtain consent from the individual for the purpose; and

(b) the benefits to the public (or a section thereof) clearly outweigh any adverse impact or risks to the individual.

3.2 Prior to the PDPA providing the Legal or Business Purpose as a basis for collecting, using and disclosing personal data without consent and notification, we are of the view that PDPC should clarify:

(a) The intent of this exception

(i) Whether the Legal or Business Purpose basis is intended to be an overriding exception of the general consent and notification requirement. In particular we note that even notification would not be required under this Legal or Business Purpose, i.e. it overrides both the Consent Obligation and the Notification Obligation.

(ii) If the intent is to broaden the scope of the existing exemptions that the PDPA has (e.g. disclosure necessary for any investigation or proceedings), or to provide a completely new category of exemption? For example, is the intent to include any potential investigations, or investigations or proceedings related to foreign laws or foreign offences?

We note that EU GDPR allows as an alternate basis to consent, processing which is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, <u>except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.</u>

We note that the Australian Privacy Act 1988 (Cth) allows under Australian Privacy Principle (APP) 3 collection of sensitive information without consent in "permitted general situations". The permitted general situations are listed in 7 Items in a table in section 16A of the Privacy Act. More broadly, APP 6.2 allows use or disclosure of personal information without consent where a permitted general situation exists. Other APPs set rules for personal information treatment in permitted general situations. There is also a similar mechanism in the Privacy Act relating to listed "permitted health situations" in section 16B. The permitted general situations overlap with some matters contemplated in the examples given for considering including notification in the PDPA. As an example, the condition for permitted general situation Item 4 is "The collection, use or disclosure is reasonably necessary for the establishment, exercise or defence of a legal or equitable claim".

We note that the Indian Supreme Court has recently held that privacy is a constitutionally protected right which emerges primarily from the guarantee of life and personal liberty in Article 21 of the Indian Constitution (which is very similar to Article 9(1) of Singapore's Constitution). Can the Legal or Business Purpose basis be used where an organisation is faced with a foreign order from a jurisdiction which does not provide the same checks and balances as Singapore's ?

(b) The scope of this exception

(i) How an organization can determine whether it is "desirable" to obtain consent, or specifically, in which situations (apart from the sharing of information to prevent fraudulent activities) that it would not be "desirable" to obtain consent.

4. 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)?

4.1 Whilst we are of the view that the Legal or Business Purpose approach should be subject to some conditions, further clarity is needed in respect of the proposed conditions.

4.2 At paragraph 3.15, we note that the PDPC has indicated that *"it may not be meaningful to notify individuals of the collection, use or disclosure for a Legal or Business Purpose since the individual may not withdraw consent"*. We would like to clarify if the intent is to enable an organisation to ignore an individual's express withdrawal of consent (assuming it was collected with their consent in the first place and the organisation would not have been able to collect the personal data otherwise) and allow it to continue to use and disclose the personal data if there were clear public benefits?

4.3 It would also be helpful if the PDPC could clarify if the Legal or Business Purpose basis can trump the research exemption or how this would work with the research exemption (e.g. whether it is possible for general research to rely on the Legal or Business approach, rather than the research exemption which is much narrower).

For example, an individual may have consented to the collection of his blood on the express understanding that he could change his mind later and withdraw consent for its further use. Could the organisation use it subsequently against the individual's wishes if the blood was found to be very useful for research but did not want to comply with the conditions of the current research exemption in paragraph 4 of the Fourth Schedule?

4.4 Generally, we are of the view that the Legal or Business Purpose may be more appropriate for big data collection and analytics. For example, the putting of cookies in an individual's computer - such collection and use may potentially yield benefits without any adverse impact or risks to the individual. It would be helpful if the PDPC could provide more specific examples of when the Legal or Business Purpose may be appropriately relied upon by an organization.

5. 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?

5.1 We are of the view that further clarity is needed on the thresholds required for notification. We note that the definition of a "data breach" refers to "unauthorized access, collection, use, disclosure, copying, modification, disposal of personal data or similar risks". In particular, we are of the view that mere access may be too low a threshold for purposes of a data breach. If so, any unauthorized access (without any collection or exfiltration for example) of personal data would need to be notified and this may lead to notification fatigue.

5.2 Further, we are of the view that clarity is needed to determine when the "clock starts to run" in respect of the time frame for breach notification. For example, if a breach (e.g. access into the network) has been discovered, but it is not clear if any personal data has been lost, would the clock start to run? If there has been access but no copying or removal or retrieval, would notification need to be provided (see comment in para 1 above).

5.3 Setting a number of affected individuals threshold for disclosure of any data breach no matter how high raises challenges for a business to manage. If the objective of the notification requirement is to provide the PDPC with information to assist with identifying sectors who could benefit from additional PDPC support or similar, an initial question is whether there are other mechanisms available to achieve this objective that are less burdensome on business.

6. 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?

6.1 We have no comments in respect of the proposal.

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

7.1 We have no comments in respect of the proposal further to those made above.

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

8.1 We are of the view that clarity is needed to determine when the "clock starts to run" in respect of the time frame for breach notification. For example, if a breach (e.g. access into the network) has been discovered, but it is not clear if any personal data has been accessed, when would the clock start to run? If there has been access but no copying or removal or retrieval, would notification need to be provided (see comment in Q5 para 1 above)?

8.2 Further given that a data breach may not mean necessarily that the organisation has breached the Protection Obligation (because it had taken all reasonable measures to protect the personal data), would mandatory early reporting of an unauthorized access (given that any risk of impact cannot yet be ruled out) lead to unnecessary bad publicity for the organisation?

Conclusion

We welcome the PDPC's efforts to update the PDPA to deal with the new challenges posed by Singapore's efforts to create a Smart Nation. While we fully support the creation of alternate bases for processing to consent, the PDPA should be kept business friendly, and more clarity on how the new bases can be applied would be welcome.

We trust you find our comments useful. We would be pleased to discuss our submission further with the PDPC.

Thank you again for the opportunity to provide feedback.

Baker & McKenzie.Wong & Leow

A member of Baker & McKenzie International, a Swiss Verein
Reg. No. 200010145R
8 Marina Boulevard
#05-01 Marina Bay Financial Centre Tower 1
Singapore 018981
Main: +65 6338 1888
Fax: +65 6337 5100