RESPONSE TO FEEDBACK ON THE PUBLIC CONSULTATION ON APPROACHES TO MANAGING PERSONAL DATA IN THE DIGITAL ECONOMY

Issued 1 February 2018

TABLE OF CONTENTS

PART I: INTRODUCTION AND BACKGROUND

1.1 The Personal Data Protection Commission (the "PDPC") launched a public consultation on 27 July 2017 on Approaches to Managing Personal Data in the Digital Economy.

1.2 In the public consultation, PDPC sought views on the relevance of other bases for collecting, using and disclosing personal data under the Personal Data Protection Act 2012 ("PDPA"), namely the proposed 'Notification of Purpose' and 'Legal or Business Purpose' approaches. PDPC also proposed a mandatory data breach notification regime for notification of data breaches to PDPC and affected individuals under the PDPA. These proposals are part of the PDPC's review of the PDPA.

1.3 The consultation closed on 5 October 2017 with 68 responses from consumers and organisations (including business associations) representing various sectors. Please refer to the PDPC's website for the full list of respondents and their submissions[1]. The PDPC thanks all respondents for the comments submitted to the public consultation.

1.4 This note summarises the key matters raised by respondents in this public consultation, and provides PDPC's responses and positions on the proposals taking into consideration the comments received.

[1] Available at https://www.pdpc.gov.sg/legislation-and-guidelines/public-consultations/responses-received-on-5-october-2017.

PART II: ENHANCED FRAMEWORK FOR COLLECTION, USE AND DISCLOSURE OF PERSONAL DATA

2 'Notification of Purpose' approach

2.1 In the public consultation, PDPC considered that notifying individuals of the purpose ("**Notification of Purpose**") can be an appropriate basis for an organisation to collect, use and disclose personal data where it is impractical to obtain consent. PDPC consulted on the proposal to provide for 'Notification of Purpose' as a basis for collecting, using and disclosing personal data under the PDPA, subject to the following conditions:

a) it is impractical for the organisation 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.

Feedback received

2.2 While most of the respondents generally supported 'Notification of Purpose' as a basis for collecting, using and disclosing personal data under the PDPA, some raised concerns and/or sought clarifications on the proposed conditions for 'Notification of Purpose' to apply.

2.3 In particular, several respondents raised concerns over the uncertainty of assessing 'impracticality' and the factors to be considered. For instance, respondents asked whether organisations were required to exhaust all avenues of contacting the individual first before it would be considered 'impractical' to obtain consent.

2.4 Respondents raised similar concerns over the uncertainty of assessing whether the collection, use or disclosure is 'not expected to have any adverse impact on the individuals'. Questions were also raised as to whether the collection, use or disclosure of personal data for marketing purposes would be considered to have an 'adverse impact' on the individuals.

PDPC's response

2.5 In consideration of the feedback received, PDPC intends to remove the condition of 'impractical to obtain consent', but to retain (and rephrase to similar effect) the condition of 'not likely to have any adverse impact on the individuals'. The intent is that the use of 'Notification of Purpose' as a basis for collecting, using and disclosing personal data is appropriate in situations where there is no foreseeable adverse impact on the individuals arising from the collection, use and disclosure of their

personal data. PDPC is cognisant of the need for guidance as to what would be considered 'not likely to have any adverse impact' and will issue guidelines to provide further clarity.

3 Appropriate notification to be provided for 'Notification of Purpose'

3.1 In the public consultation, it was proposed that organisations that wish to rely on 'Notification of Purpose' must provide appropriate notification of the purpose of the collection, use or disclosure of the personal data, and information about how individuals may opt out, where applicable. It was proposed that where feasible, organisations must allow individuals to opt out of such collection, use or disclosure.

Feedback received

3.2 Respondents sought clarifications on whether posting a general notification on organisations' website or privacy policy would suffice under the 'Notification of Purpose' approach. There were suggestions for organisations to provide a mechanism and reasonable period for individuals to opt out before collecting, using or disclosing the personal data for the purpose. Respondents also sought clarifications on the thresholds for cost and difficulty that would be considered not 'feasible' to allow individuals to opt out.

PDPC's response

3.3 In line with the current approach for notifications under the PDPA's Notification Obligation, PDPC will not specify how organisations are to notify individuals. There could be certain circumstances (e.g. the organisation has no means of contacting the individuals) where it may be considered appropriate for the organisation to provide a general notification on its website or social media page. The onus would be on the organisations to determine the most appropriate way of doing so based on their specific circumstances, and to ensure they take reasonable steps to inform individuals of the purposes and how they may opt out or withdraw consent from the collection, use or disclosure of personal data for the purposes.

3.4 PDPC recognises the need to cater to circumstances where large volumes of personal data are instantaneously and seamlessly collected (e.g. data collected by sensors), and the inherent challenge in allowing individuals to opt out in such circumstances. PDPC will provide further guidance on this in guidelines.

4 Revised consent framework to incorporate 'Notification of Purpose'

4.1 Presently, the consent framework under the PDPA provides for actual consent and deemed consent[2]. Individuals may at any time withdraw any consent given, or deemed to have been given, under the PDPA in respect of the collection, use or disclosure of their personal data for any purpose.

4.2 PDPC intends to provide for 'Notification of Purpose' as part of the consent framework under the PDPA as outlined below:

a) As per the current actual consent under the PDPA, express consent is obtained through a positive action of the individual to consent to the collection, use and disclosure of his personal data for purposes which the individual has been informed of (henceforth referred to as 'Express Consent').

b) As per the current deemed consent under the PDPA, an individual is deemed to consent to the collection, use and disclosure of his personal data for a purpose if the individual voluntarily provides the personal data to the organisation for that purpose, and it is reasonable that the individual would do so. An organisation is not required to inform an individual of the purposes for the collection, use or disclosure of his personal data (henceforth referred to as 'Deemed Consent by Conduct').

c) In addition, PDPC intends to provide for an opt-out approach where the individual is notified of the purposes of the collection, use or disclosure of his personal data, and provided a reasonable time period to opt out (where opt-out is feasible) but does not opt out within the time period[3] (henceforth referred to as 'Deemed Consent by Notification'). Under this approach, the organisation must conduct a risk and impact assessment, such as a data protection impact assessment ("DPIA"), as an accountability measure to ascertain whether the intended collection, use or disclosure is likely to have any adverse impact on the individual. (See further discussion on accountability measures in section 6 below). Organisations may not rely on Deemed Consent by Notification for purposes that are likely to have any adverse impact or consequences for the individual. Organisations may also not rely on Deemed Consent by Notification for direct marketing purposes. For such purposes, organisations must obtain Express Consent from the individual.

[2] Section 15 of the PDPA.
[3] Where the individual does not opt out within the time period provided, he may still withdraw consent for the collection, use or disclosure of his personal data after the opt-out period.

5 'Legal or Business Purpose' approach

5.1 In the public consultation, PDPC recognised that there are circumstances where organisations need to collect, use or disclose personal data without consent for a legitimate purpose, but the collection, use or disclosure is not authorised under the PDPA or other written laws (e.g. the sharing and use of personal data to detect and prevent fraudulent activities). PDPC hence proposed to provide for the collection, use or disclosure of personal data regardless of consent where it is necessary for a '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.

Feedback received

5.2 Most of the respondents generally supported the proposal to allow for the collection, use or disclosure of personal data for 'Legal or Business Purpose' regardless of consent. However, there were mixed views on the proposed conditions of 'not desirable or appropriate to obtain consent' and 'benefits to the public (or a section thereof) clearly outweigh any adverse impact or risks to the individual'.

5.3 Several respondents sought clarification as to what would be considered 'not desirable or appropriate to obtain consent' and the factors to be considered for such an assessment. Similar clarifications were sought on the assessment of 'benefits to the public (or a section thereof) clearly outweigh any adverse impact or risks to the individual'.

5.4 Some respondents requested for PDPC to clearly define the activities that would be considered for a 'Legal or Business Purpose'. Queries were also raised as to whether organisations could rely on 'Legal or Business Purpose' to market to individuals where there was a benefit to the individuals.

5.5 Respondents also suggested using the term 'Legitimate Interests', and to embody the legitimate interest test adopted in the European Union General Data Protection Regulation ("EU GDPR")[4]. Suggestions were also made for organisations to be required to notify individuals when relying on 'Legal or Business Purpose' to collect, use or disclose personal data.

[4] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC.

PDPC's response

5.6 In view of the comments and feedback, PDPC intends to provide for 'Legitimate Interests' as a basis to collect, use or disclose personal data regardless of consent. As 'Legitimate Interests' is an evolution of the 'Legal or Business Purpose' approach proposed in the public consultation, the PDPC will provide clarification in guidelines on the legal or business purposes that come within its ambit. These may include purposes such as preventing fraud, which are currently within the ambit of the 'Legal or Business Purpose' approach that was proposed, and may extend to other business purposes consistent with the intent of this exception. However, the 'Legitimate Interests' exception is not intended to cover direct marketing purposes.

5.7 The intent is to enable organisations to collect, use or disclose personal data in circumstances where there is a need to protect legitimate interests that will have economic, social, security or other benefits for the public (or a section thereof), and such processing should not be subject to consent since individuals may not provide consent in such circumstances (e.g. to avoid fraud detection).

5.8 PDPC intends to retain (and rephrase to similar effect) the condition that 'benefits to the public (or a section thereof) must outweigh any adverse impact to the individual' as part of the **accountability measures** to be implemented by organisations when relying on this exception. Organisations that wish to collect, use or disclose personal data regardless of consent for 'Legitimate Interests" will need to conduct a risk and impact assessment to determine whether the benefits outweigh any foreseeable adverse impact to the individual. (See further discussion on accountability measures in section 6 below.)

5.9 As an additional safeguard, PDPC intends to provide for an **openness requirement** to the 'Legitimate Interests' exception, similar to the current requirement under the PDPA to inform individuals of the purpose of managing or terminating employment relationship[5]. An organisation that is relying on this exception will be required to:

a) disclose its reliance on 'Legitimate Interests' as a ground for collection, use or disclosure. This could be done through the organisation's data protection policy that is made available to the public; and

b) make available a document justifying the organisation's reliance on 'Legitimate

[5] Section 20(4) of the PDPA provides that, notwithstanding subsection (3), an organisation, on or before collecting, using or disclosing the personal data about an individual for the purpose of managing or terminating an employment relationship between the organisation and that individual, shall inform the individual of (a) that purpose; and (b) on request by the individual, the business contact information of a person who is able to answer the individual's questions about that collection, use or disclosure on behalf of the organisation. PDPC's Advisory Guidelines clarify that it may be sufficient to provide general notification to employees such as through employment contracts, employee handbooks, or notices in the company intranet.

Interests', and the business contact information of the person who is able to answer individuals' questions about such collection, use or disclosure on behalf of the organisation.

6 Accountability measures for 'Notification of Purpose' and 'Legal or Business Purpose'

6.1 In the public consultation, PDPC proposed that organisations must conduct a risk and impact assessment, such as a DPIA, and put in place measures to identify and mitigate the risks when relying on the 'Notification of Purpose' or 'Legal or Business Purpose' approach to collect, use or disclose personal data.

Feedback received

6.2 Clarifications were sought as to whether the risk and impact assessment or DPIA must be documented, and whether it would be subject to PDPC's review or pre-approval. Respondents also queried if individuals could request for a copy of the risk and impact assessment or DPIA. There was a suggestion for organisations to produce a summary rather than provide the full assessment to protect confidential business information.

PDPC's response

6.3 In relying on 'Notification of Purpose' (or 'Deemed Consent by Notification') or 'Legitimate Interests' to collect, use or disclose personal data, the burden of responsibility shifts from the individuals to the organisations to safeguard the interests of individuals. Organisations must thus implement accountability measures when relying on these approaches. This ensures that the overall protection for individuals' personal data is maintained even if individuals' ability to exercise choice and control over their personal data through consent is reduced.

6.4 Organisations must conduct a risk and impact assessment, such as a DPIA, as an **accountability measure** when relying on 'Deemed Consent by Notification' or 'Legitimate Interests'. This accountability measure also places the onus on organisations to put in place measures to identify and mitigate the risks before relying on the aforesaid approaches to collect, use or disclose personal data.

6.5 Organisations should document their risk and impact assessments. However, given the potential commercial sensitivity of such assessments, these assessments will not be considered to be personal data protection policies and they need not be made available to the public or to individuals on request. However, in the event of complaints, PDPC reserves the right to require organisations to disclose these assessments for PDPC's consideration in determining whether there is any contravention of the PDPA.

PART III: MANDATORY DATA BREACH NOTIFICATION

7 General comments

7.1 The public consultation highlighted the impetus for the proposed mandatory data breach [6] notification regime. With mandatory breach notification, affected individuals will have the opportunity to take steps to protect themselves from the risks and impact from the data breach, while affected organisations will be able to receive guidance from PDPC on post-breach remedial actions when they notify PDPC. Overall, this will enable PDPC to better oversee the level of incidences and management of data breaches at the national level.

Feedback received

7.2 Majority of responses were supportive of the proposed mandatory breach notification regime, and agreed with PDPC's approach to strike a reasonable balance between the need for organisations to collect, use and disclose personal data and individuals' right to the protection of their personal data. The alignment with international standards on specific details of the regime were also noted.

7.3 Many respondents reiterated the need for guidelines from the PDPC to guide organisations in complying with the requirements of the data breach notification regime.

PDPC's response

7.4 As stated in the public consultation, advisory guidelines will be issued by the PDPC to provide guidance for organisations in complying with the data breach notification requirements when introduced, including the considerations for assessing whether data breaches meet the criteria for notification, the time frame for notification, and the types of information to be included in the breach notification to affected individuals and to PDPC.

8 Criteria for notification

8.1 In the public consultation, PDPC proposed for notification to affected individuals and the PDPC when there is a breach that poses any risk of impact or harm to the affected individuals. Where the breach does not pose any risk of impact or harm to affected individuals but is of a significant scale (e.g. 500 affected individuals), organisations are only required to notify PDPC of the breach.

[6] A data breach refers to the unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks of personal data in an organisation's possession or under its control.

Feedback received

8.2 Majority of respondents proposed for PDPC to adopt a consistent risk-based approach, and a higher threshold for notification to affected individuals as well as to PDPC. This is to avoid imposing overly onerous regulatory burdens on organisations to report data breaches which are not likely to result in significant harm or impact to affected individuals. In particular, there were suggestions for PDPC to adopt a similar criteria for notification as Australia's notifiable data breaches scheme[7].

8.3 On the proposed scale of breach as a criterion for notification to PDPC, majority of respondents disagreed with the proposed threshold of 500 affected individuals. Several respondents proposed the removal of scale of breach as a criterion, given that PDPC's objectives for the mandatory breach notification regime would still be satisfied.

PDPC's response

8.4 In consideration of the responses provided, PDPC intends to retain and rephrase (to similar effect) the criterion to **'likely to result in significant harm or impact to the individuals to whom the information relates'** for breach notifications to affected individuals as well as to PDPC. This would allow affected individuals to take steps to protect themselves from the risks of harm or impact from the breach, while minimising notification fatigue for individuals and regulatory burden on organisations. Further guidance on assessing whether a data breach is likely to result in significant impact or harm would be provided in guidelines.

8.5 PDPC also intends to retain the criterion of significant scale of breach for notification to PDPC, but will not prescribe a statutory threshold for number of affected individuals (e.g. 500 or more). This is necessary for PDPC to effectively monitor the market for large scale breach incidences. PDPC will provide further guidance on assessing the scale of impact in guidelines.

9 Time frame for notification

9.1 The public consultation sought views on the proposed time frames for data breach notifications to affected individuals and to PDPC.

Feedback received

9.2 Several respondents requested for more time than the proposed cap of 72 hours for

[7] Australia's Privacy Amendment (Notifiable Data Breaches) Act 2017 recently established a Notifiable Data Breaches ("NDB") scheme that requires organisations covered by the Australian Privacy Act 1988 (Privacy Act) to notify any individuals likely to be at risk of serious harm by a data breach. The NDB scheme will commence on 22 February 2018.

affected organisations to notify PDPC of a breach. Most respondents agreed with the proposal for affected individuals to be notified as soon as practicable, in view of the variability of data breach circumstances.

9.3 Several respondents also sought clarifications as to when the 'clock' starts for the 72-hour time frame, with some suggestions for the 'clock' to commence from the time the organisation is able to reasonably determine that a breach is eligible for notification.

PDPC's response

9.4 PDPC intends to retain the proposed time frames for notification to affected individuals (i.e. '**as soon as practicable**') and to PDPC (i.e. '**as soon as practicable, no later than 72 hours**').

9.5 PDPC acknowledges that organisations may require time to determine the veracity of suspected breaches. The time frames for notifying affected individuals and PDPC will thus commence from the time the organisation determines that the breach is eligible for reporting. To ensure the reporting and assessment of breach incidents are expediently handled by organisations, PDPC intends to provide for **an assessment period of up to 30 days** from the day the organisation first becomes aware of a suspected breach, to assess its eligibility for notification. This follows Australia's notifiable data breaches scheme, which allows organisations a 30-day assessment period for a suspected breach. The organisation must document the steps taken in assessing a breach from the time it first becomes aware of it to demonstrate that it has taken all reasonable and expeditious steps to assess the breach. Where an organisation is unable to complete the assessment within 30 days, it should document the reasons for the delay as justification that the time taken for the assessment is reasonable and expeditious in the circumstances[8]. Unreasonable delays in reporting breaches that cannot be justified will be considered a breach of the mandatory data breach notification obligation.

9.6 Following the organisation's assessment, where the organisation determines that the breach is eligible for reporting, then the organisation must notify the relevant parties within the required time frame (i.e. 'as soon as practicable' to affected individuals, and 'as soon as practicable, no later than 72 hours' to PDPC, from the time of determination). Notwithstanding this, organisations may choose to notify PDPC of the suspected breach incident at any time during the assessment period so that they can receive guidance from PDPC where necessary.

9.7 To be clear, the organisation must notify all affected individuals as soon as

[8] The organisation may be required to produce such documentation to the PDPC as part of its notification to the PDPC of an eligible breach, or for any investigation by the PDPC of a suspected breach.

practicable from the time the organisation determines that the breach is eligible for reporting, **regardless of whether it has fully utilised the 30-day assessment period**. The organisation must also notify PDPC as soon as practicable, no later than 72 hours, from the time it determines the breach is eligible for reporting. Prescribing a cap of 72 hours provides clarity for organisations as to the definitive time by which they would have to notify PDPC.

9.8 Where a data breach is discovered by a data intermediary ("DI") that is processing personal data on behalf and for the purposes of another organisation, the 30-day assessment period for that organisation to assess and establish the eligibility of a suspected breach will commence from the time the DI first becomes aware of the breach. The DI will thus be required to notify the organisation that it processes the personal data on behalf and for the purposes of, **without undue delay from the time it first becomes aware of the breach**. This is similar to the requirements under the EU GDPR[9], where data processors are required to notify the data controllers 'without undue delay' after becoming aware of a personal data breach, and the data controllers are to notify the relevant supervisory authority and affected individuals.

10 Exceptions to notify affected individuals

10.1 The public consultation sought views on the proposed exceptions to the requirement to notify affected individuals under the mandatory data breach notification regime.

Feedback received

10.2 Some respondents suggested extending the coverage of the law enforcement exception to cover all forms of investigation and proceedings, including investigations by other government agencies. There was also a suggestion to broaden the technological protection exception beyond encryption to be technology neutral.

10.3 There were suggestions to include other exceptions, notably an exception for organisations which have taken remedial action to reduce the likelihood of harm or impact to the individuals from the breach.

PDPC's response

10.4 In view of the responses, PDPC intends to extend the coverage of the law enforcement exception to include investigations carried out by agencies that are authorised by the law[10]. Organisations will not be required to notify affected individuals of an eligible breach that is the subject of an ongoing or potential

[9] Article 33 of the EU GDPR.
[10] This would include investigations conducted by organisations to discharge obligations under the law.

investigation under the law, if it is assessed that notifying affected individuals will compromise investigations or prejudice enforcement efforts under the law.

10.5 On the technological protection exception, PDPC intends to broaden the exception beyond technological encryption and make it technology neutral. The unauthorised collection, use or disclosure of personal data that has been encrypted may not constitute a data breach unless the data can be decrypted. Organisations that experience a loss of encrypted data that has been encrypted to a reasonable standard may therefore rely on the technological protection exception from the requirement to notify affected individuals[11].

10.6 PDPC also intends to provide an exception for organisations which have taken remedial actions to reduce the potential harm or impact to the affected individuals. The organisation will need to demonstrate that, as a result of the organisation's remedial actions, the breach is not likely to have any significant harm or impact to the affected individuals.

10.7 To be clear, organisations will still be required to notify PDPC of eligible breaches even if an exception to the requirement to notify affected individuals applies. PDPC reserves the right to direct organisations to notify affected individuals of the breach even if an exception to the breach notification requirement may apply. Additionally, to cater to certain exceptional circumstances where notification to affected individuals may not be desirable, PDPC will also have the power to exempt organisations from notifying affected individuals.

10.8 PDPC intends for the exclusions under Section 4 of the PDPA to apply to the data breach notification provisions under the PDPA[12]. For instance, where a data breach is committed by an employee acting in the course of his or her employment with the organisation, the organisation (not the employee) will be liable for the data breach under the PDPA, and the organisation will be responsible for complying with the data breach notification requirements under the PDPA.

11 Concurrent notification to PDPC and other regulators

11.1 The public consultation sought views on the proposed concurrent application of PDPA's mandatory data breach notification requirements with other laws and

[11] This is similar to the EU GDPR. Article 34(3) of the EU GDPR provides that notification to an individual is not required if the organisation has "implemented appropriate technological and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it".

[12] For example, any individual acting a personal or domestic capacity; any employee acting in the course of his or her employment with the organisation; any public agency; any organisation in the course of acting on behalf of a public agency.

sectoral regulations.

Feedback received

11.2 Views on the proposed concurrent application of PDPC's mandatory data breach notification regime with other sectoral breach notification regimes were divided, with some in agreement with the proposed approach, and others proposing that only a single regulator should be notified of a breach. There were also proposals for a harmonised notification platform across government agencies and overseas jurisdictions.

PDPC's response

11.3 Where an organisation is required to notify a sectoral or law enforcement agency of a data breach under other written law, and that data breach meets the criteria for notification under the PDPA, the organisation must notify the other sectoral or law enforcement agency according to the requirements under the other written law, and it must also notify PDPC and affected individuals according to the time frames for data breach notifications under the PDPA. In order to minimise the regulatory burden on organisations, an organisation may adopt the same format of notification required for reporting to the other sectoral regulator or law enforcement agency for its breach notifications to PDPC. For breach notifications to affected individuals, PDPC will issue advisory guidelines to provide guidance on the information to be provided in organisations' communications to ensure clarity and assurance for affected individuals.

11.4 To help further reduce the effort and cost for organisations to comply with the notification requirements under multiple laws and sectoral regulations, PDPC will also explore mechanisms for streamlining notifications to PDPC and the relevant sectoral or law enforcement agencies.

PART IV: CONCLUSION

12.1 This is the first of a series of public consultations that PDPC is conducting for the review of the PDPA. The PDPC will continue to solicit feedback and views on other key areas of review.

12.2 Advisory guidelines and other resources will be provided to assist organisations in complying with the changes or new requirements when they are introduced.

12.3 Once again, PDPC thanks all respondents for their comments and submissions to this public consultation.

END OF DOCUMENT