Singtel

SINGAPORE TELECOMMUNICATIONS LTD

SUBMISSION TO THE PERSONAL DATA PROTECTION COMMISSION

IN RESPONSE TO THE

PUBLIC CONSULTATION FOR APPROACHES TO MANAGING PERSONAL DATA IN THE DIGITAL ECONOMY

DATE OF SUBMISSION: 21 SEPTEMBER 2017

Singtel

SINGAPORE TELECOMMUNICATIONS LTD

SUBMISSION TO THE PERSONAL DATA PROTECTION COMMISSION IN RESPONSE TO THE PUBLIC CONSULTATION FOR APPROACHES TO MANAGING PERSONAL DATA IN THE DIGITAL ECONOMY

1. INTRODUCTION

1.1. Singapore Telecommunications Limited and its related companies (**Singtel**) are licensed to provide info-communications services in Singapore. Singtel is committed to the provision of state-of-the-art info-communications technologies and services in Singapore.

1.2. Singtel has a comprehensive portfolio of products that includes voice and data services over fixed, wireless and Internet platforms. Singtel provides services to both corporate and residential customers and is committed to bringing the best of global info-communications to its customers in the Asia Pacific and beyond.

1.3. Singtel is also a leading Internet service provider ("**ISP**") in Singapore and has been at the forefront of Internet innovation since 1994, being the first ISP to launch broadband services in Singapore. It is licensed to offer IPTV services under a nationwide subscription television licence granted by the Info-communications Media Development Authority of Singapore ("**IMDA**").

1.4. Singtel refers to the Public Consultation Paper for Approaches to Managing Personal Data in the Digital Economy issued by the Personal Data Protection Commission's (**PDPC**) on 27 July 2017 (**Consultation Paper**).

1.5. Singtel welcomes the opportunity to make this submission on the Consultation Paper and would be pleased to clarify any of the views and comments made in this submission, as appropriate.

1.6. This submission is structured as follows:
Section 2 – Executive summary;
Section 3 – Specific comments; and
Section 4 – Conclusion.

Singtel

2. EXECUTIVE SUMMARY

2.1. Through the Consultation Paper, the PDPC has proposed a number of changes to the current personal data protection regime under the Personal Data Protection Act 2012 (the "**PDPA**").

2.2. Singtel recognises that since the introduction of the PDPA in 2012, the technological landscape in Singapore has evolved. As such, Singtel welcomes the PDPC's review of the PDPA, and is generally supportive of the following proposals that have been raised by the PDPC:

- introducing a "Notification of Purpose" basis for collecting, using and disclosing an individual's personal information as a separate basis to the consent obligation in section 13 of the PDPA; and
- introducing a "Legal or Business Purpose" exception to the consent obligation in section 13 of the PDPA.

2.3. In Singtel's view, such proposals represent an update to the current regime which will ensure that it is:

- fit for the current technological landscape;
- is workable and fit for purpose, in light of the circumstances facing organisations in respect of the collection, use and disclosure of personal information; and
- provides adequate protection of individual's personal data.

2.4. As an upfront matter, Singtel notes that it is currently unclear how the PDPC intends to implement the current proposals (i.e. through amendments to the PDPA or through the development of guidelines), and whether it intends to continue to publicly consult on the proposals moving forward.

2.5. Singtel would welcome further guidance being provided by the PDPC in relation to how the PDPC's proposals are intended to be implemented operationally, either through the development of guidelines to assist organisations in complying with their obligations under the new proposals or through further refinement to the proposals themselves. Should there be consequential amendments to the existing regulations and/or the PDPA arising from this Consultation, Singtel submits that the industry should be given an opportunity to further review and comment on those proposed amendments.

Singtel

Shift in the data protection regime

2.6. The current regime under the PDPA for the collection, use and disclosure of an individual's personal information is centred around obtaining an individual's consent. Introducing a parallel "Notification of Purpose" basis for collecting, using or disclosing an individual's data represents a necessary update to the current regime.

2.7. Singtel is supportive of the PDPC's proposal to provide for a separate basis for the collection, use and disclosure of personal information, where obtaining consent is impractical or is not expected to have an adverse impact.

2.8. As such, Singtel would welcome further development of this proposal, including the provision of further detail on the manner in which Notification for Purpose will be practically implemented by the PDPC within the current regime, including whether the following existing sections of the PDPA will apply:

- the current "limitation of purpose and extent" conditions in Division 2 of Part IV
- the enforcement mechanisms under Part VII of the PDPA will apply to the Notification of Purpose basis.

2.9. Singtel supports the broad basis on which the "Notification for Purpose" basis and the "Legal and Business Purpose" exception are set out. Singtel would welcome further development of these bases including the provision of further guidance from the PDPC in respect of how the relevant criteria is intended to be practically applied by organisations.

Introduction of a mandatory data breach notification obligation

2.10. Singtel is of the view that the voluntary system prescribed in the PDPC's Guidelines on Managing Data Breaches[1] has worked well since its introduction, providing organisations with a degree of flexibility to determine how to notify individuals of a data breach, and sufficient scope to undertake any necessary internal investigations and assessment of a suspected data breach. Singtel notes that organisations are, by default, in favour of providing their customers the security of knowing whether their personal data is safe and therefore, will adopt a framework of voluntarily informing them where there are possible breaches.

[1] Personal Data Protection Commission, Guideline on Managing Data Breaches (released 8 May 2015).

2.11. There is merit in allowing the voluntary disclosure framework to continue. For example, organisations may be in the process of co-operating with law enforcement agencies and this places them in a difficult situation where disclosure may interfere with the investigations. Investigations to ascertain the source and full extent of damage also require time.

2.12. As such, Singtel supports the PDPC's initiative to retain some of the flexibility of the voluntary approach, including its proposal to not specify how organisations should notify individuals of a data breach, and setting a threshold in relation to notifying individuals of a data breach "as soon as practicable".

2.13. In light of this, Singtel is of the view that the PDPC should further develop this proposal, including providing operational detail in respect of:

- how the PDPC intends for organisations to discharge their obligations under the proposed mandatory regime; and
- associated penalties applicable.

2.14. While Singtel is broadly supportive of the mandatory data breach notification regime, it is concerned in respect of the PDPC's view of what data breaches are subject to the mandatory data breach notification regime. The PDPC has proposed that notification obligations will apply to data breaches where there is "any risk of harm" to an affected individual. In Singtel's view, this threshold has the capability of applying to all data breaches, and will place a heavy administrative and regulatory burden on organisations. Singtel would welcome further consultation on this issue.

3. SPECIFIC COMMENTS

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

3.1. Singtel supports the principle that there should be a Notification of Purpose basis for collecting, using and disclosing personal data without an individual's consent. The PDPC should continue to develop this proposal including providing further detail in respect of the manner in which the proposal will be implemented within the existing regime.

Singtel

3.2. In particular, Singtel would welcome further detail in respect of:

a) how Notification of Purpose, as a parallel basis for collecting, using and disclosing personal data, will sit within a broader data protection regime which is built on an obligation of obtaining consent (i.e. if it is intended to be an exception to the consent obligations and therefore to be included within Schedules 2, 3 and 4, or to be included as an alternate basis under section 13); and
b) whether any "limitation of purpose and extent" restrictions similar to those set out in section 18(a) of the PDPA will apply to the Notification of Purpose basis.

3.3. Additionally, under the current regime, pursuant to section 18(a) of the PDPA an individual's personal data can only be collected, used or disclosed for a purpose that a reasonable person would consider appropriate in the circumstances. Singtel would welcome further clarification in respect of whether the Notification of Purpose basis will be subject to a similar restriction.

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)?

3.4. Singtel supports the principle that the Notification of Purpose approach should be subject to conditions.

3.5. The proposals set out in the Consultation paper in respect of threshold criteria, notification requirements and risk management obligations should be further developed by the PDPC for consultation.

Threshold criteria

3.6. Singtel supports the conditions proposed by the PDPC to be applicable to the Notification of Purpose approach, i.e. that such an approach can only be taken if it is impractical for the organisation to obtain consent and where the collection, use or disclosure of personal data is not expected to have any adverse impact on the individual.

3.7. However, in Singtel's view, the words "impractical" and "adverse impact" are capable of having a wide interpretation. As such, Singtel would welcome further clarification by the PDPC on the standards and thresholds to be applied in interpreting these conditions and the circumstances in which the PDPC considers would meet these thresholds.

3.8. Such clarification will provide organisations with a sufficient degree of regulatory certainty to rely on the Notification of Purpose basis for collecting, using or disclosing information.

Appropriate manner of notification

3.9. The Consultation Paper states that the PDPC does not intend to prescribe the manner of notification to be made when an organisation relies on the Notification of Purpose approach. The PDPC has proposed to let organisations assess their circumstances and determine the most appropriate form of notification that ensures the individuals are made aware of the purpose of the collection, use and disclosure of their personal data.[2]

3.10. Singtel supports this flexible approach over an approach which requires organisations to use to a single prescribed method. Organisations themselves would be best placed to determine the most appropriate form of notification to the individual such as through signage, digital, written and/or other forms and methods of notification.

3.11. While the PDPC's proposal to allow organisations to determine the most appropriate form of notification provides organisations with a level of flexibility, Singtel would support the development of Guidelines by the PDPC to provide further clarification and guidance on what the PDPC considers to be appropriate notification.

Risk mitigation

3.12. The PDPC proposes that organisations that wish to rely on the Notification of Purpose approach must assess if there are any risks or impacts to individuals from the collection, use or disclosure of personal data, and must put in place appropriate measures to mitigate such risks.[3]

---

[2] Paragraph 3.9, Consultation Paper.
[3] Paragraph 3.10, Consultation Paper.

Singtel

3.13. The risk mitigation aspects of the Notification of Purpose approach have been set out at a high level in the Consultation Paper and Singtel would welcome further clarification from the PDPC on how it intends to implement these aspects operationally, including:

a) how risk assessment should be undertaken;
b) what risk mitigation measures are considered appropriate by the PDPC;
c) whether risk assessment must be documented, and whether assessments are subject to review and or pre-approval by the PDPC before an organisation can rely on the Notification of Purpose approach; and
d) what consequences or penalties follow if an organisation fails to put in place risk mitigation measures, or, if the risk mitigation measures put in place by the organisation are subsequently considered by the PDPC to be inadequate.

3.14. Singtel is of the view that guidelines would be appropriate to provide clarity on the different risk mitigation measures considered to be acceptable to the PDPC. Singtel would also encourage the PDPC to further develop and consult on the more operational aspects of the proposed risk mitigation measures applicable to 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?

3.15. Singtel supports the introduction of a broad Legal or Business Purpose exception to the general obligation to obtain consent from an individual before collecting, using or disclosing their personal data.

3.16. While Singtel supports the flexibility of a broad exception, the exception must be implemented in a manner that provides organisations with a sufficient degree of regulatory certainty. As such, in Singtel's view, the PDPC should clearly define what a "legal" and "business" purpose is.

3.17. The PDPA currently provides a limited number of exceptions to the basic obligation to obtain consent, which relate to a legal or business purpose.[4] These existing legal and

[4] Section 17 of the PDPA currently provides that an organisation may collect, use or disclose an individual's personal data if one of the circumstances in the Second, Third or Fourth Schedule apply. See Schedule 2, sections 1(e) and (j); Schedule 3, sections 1(e) and (h); Schedule 4, sections 1(f) and (j).

business exceptions in the PDPA are prescriptive and set out circumstances relating to specific legal or business purposes (for example, investigations or proceedings, or for the provision of legal services).

3.18. While the PDPC has recognised that there may be legal or business purposes that exist where collection, use or disclosure without consent are not currently authorised under the PDPA,[5] the Legal or Business Purpose exception has been constructed in the Consultation Paper as a broad exception with no limitation as to the type of legal or business purpose it is directed to.

3.19. Singtel would encourage the preparation of Guidelines to clearly set out what additional circumstances not already found in the Second Schedule, the Third Schedule and the Fourth Schedule are intended to be covered under this "Legal or Business purpose" exception.

3.20. It is also unclear how the "Legal or Business purpose" basis is to interact with both the current section 13 of the PDPA, and the proposed "Notification of Purpose" basis, i.e. if it is intended that both the "Legal or Business purpose" and "Notification of Purpose" bases are to be exceptions to the current section 13 and thus included in Schedules 2, 3 and 4; or if only the "Legal or Business purpose" basis is included as an exception in Schedules 2, 3 and 4, and the "Notification of Purpose" basis is to be found in section 13.

3.21. Singtel therefore agrees that "Legal or Business Purpose" should be a basis for the collection, use and disclosure of personal data without consent or notification under the PDPA. However, the manner in which Legal or Business Purpose exception has been proposed by the PDPC requires further development.

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)?

3.22. Singtel is supportive of the criteria proposed by the PDPC to be applicable to the Legal or Business Purpose exception.

[5] Paragraph 3.14, Consultation Paper.

Singtel

3.23. The PDPC has proposed that for the Legal or Business Purpose exception to be available, the following criteria must be met:

a) it is not desirable or appropriate to obtain consent from the individual for the purpose; and
b) the benefit to the public (or a section thereof) clearly outweigh any adverse impact or risks to the individual.

3.24. In Singtel's view, the PDPC should provide further clarity in respect of when the proposed criteria will be met. Singtel would welcome the inclusion of a set of non-exclusive matters which can be used by organisations when assessing whether they meet the criteria proposed by the PDPC. Singtel would also support the provision of such clarification through clear guidelines.

3.25. While the PDPC has provided an example of a situation which would meet the applicable conditions (i.e. sharing information and analysing customers personal data to identify and prevent fraudulent activities),[6] it is currently unclear how the PDPC intends the criteria to be applied in practice. Singtel would welcome further detail from the PDPC in respect of how organisations should weigh the benefit to the public against the adverse impact to the individual, and what factors the PDPC would consider relevant to such an assessment.

3.26. The Legal or Business Purpose exception is currently set out in the Consultation Paper as available for legal or business purposes generally. While Singtel welcomes a broad approach, the PDPC should provide further clarification as to whether the intention is for this exception to be broad and in relation to any legal or business purpose (subject to compliance with the criteria described above) or whether the Legal or Business Purposes exception will have a more limited availability.

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?

[6] Paragraph 3.16, Consultation Paper.

Singtel

Notification to individuals and the PDPC – risk of harm threshold

3.27. The PDPC has proposed that an organisation must notify affected individuals and the PDPC if a data breach occurs which poses **any risk of impact or harm** to the affected individuals.[7]

3.28. Singtel is of the view that a standard based on "any risk of impact or harm" is too broad and has the potential to apply to all data breaches regardless of how minor the risk. Singtel would caution against using such a threshold, as it is likely to result in the PDPC being inundated with notifications, may cause notification fatigue, and may cause unnecessary alarm to affected individuals.

3.29. Instead of a standard based on "any risk" of impact or harm, Singtel would favour an approach similar to that taken in Australia. The *Privacy Amendment (Notifiable Data Breaches) Act 2017* (the "**Act**") will take effect in Australia in January 2018 and introduces mandatory obligations to notify individuals affected by an eligible data breach. Under the Act, the mandatory data breach notification obligation regime is based on the following:

- The duty to notify is triggered if unauthorised access, disclosure or loss of information (where such loss would result in unauthorised access or disclosure) would be **likely to result in serious harm** to any of the individuals to whom the information relates.[8] The likelihood to result in serious harm is to be judged from the standard of a reasonable person.

- A non-exclusive set of relevant matters is provided under the Act to assist organisations in determining if the standard is met, for example, the kind of information, sensitivity of the information, whether security measures were in place, and the nature of the persons who have obtained the information.[9]

3.30. The context to the threshold taken in Australia was that it was not intended that every data breach should be notified.[10] The PDPC appears to have taken a similar stance to

[7] Paragraph 6.2(a), Consultation Paper.
[8] Section 26WE(2), *Privacy Amendment (Notifiable Data Breaches) Act 2017.*
[9] Section 26WG, *Privacy Amendment (Notifiable Data Breaches) Act 2017.*
[10] Explanatory Memorandum to the *Privacy Amendment (Notifiable Data Breaches) Bill 2017*, page 4 – "It is not intended that every data breach be subject to a notification requirement. It would not be appropriate for minor breaches to be notified because of the administrative burden that may place on entities, the risk of

notification of data breaches, stating in the Consultation Paper that it is mindful to not impose overly onerous regulatory burdens on businesses or to create notification fatigue in individuals.[11]

3.31. In Singtel's view, a mandatory notification framework may also mislead individuals and indirectly encourage individuals to make impractical or unfeasible requests of an organisation. As such, it is necessary that any applicable threshold be set at an appropriate level which would avoid creating an overly onerous administrative burden on organisations.

3.32. In this context, Singtel would encourage the PDPC to consider increasing the threshold applicable to the notification of data breaches to a "high risk of harm",[12] or moving to a "serious risk of harm" threshold.

3.33. Singtel would also encourage the PDPC to consider providing clarification of what risks of harm to the individual should be considered by organisations when conducting a risk assessment. In the Australian context, as the risk of harm is judged from a reasonable person, it is expected that a likely risk of harm would include financial, economic or physical harm.[13]

3.34. An additional concern for Singtel is the lack of a distinction drawn between when an organisation has a reasonable suspicion to believe that a data breach has occurred, and when it knows that a breach has occurred. Singtel would encourage the PDPC to consider the effect of such a distinction on the proposed mandatory data breach notification regime.

3.35. In Singtel's view, the mandatory data breach notification obligation should only apply from when an organisation is aware that a data breach has occurred. If an organisation only has reasonable grounds to suspect that a data breach has occurred, organisations should be given a sufficient amount of time to make necessary investigations and inquiries before the data breach notification provisions are applicable.[14]

'notification fatigue' on the part of individuals, and the lack of utility where notification does not facilitate harm mitigation."

[11] Paragraph 6.1, Consultation Paper.

[12] If a "high risk of harm" threshold is used, guidelines should be issued to set out clearly what would constitute a "high risk" of impact or harm to the affected individual, e.g. what scale of breach will constitute "high risk".

[13] Explanatory Memorandum to the *Privacy Amendment (Notifiable Data Breaches) Bill 2017*, page 3.

[14] This is similar to the approach taken in Australia. Under section 26WH of the *Privacy Amendment (Notifiable Data Breaches) Act 2017,* if an organisation has reasonable grounds to suspect that a data breach has occurred, they must undertake an assessment within 30 days of becoming aware of that suspicion.

Notification to the PDPC – significant scale threshold

3.36. The PDPC has proposed that an organisation must notify the PDPC when the scale of a data breach is "significant". The PDPC has proposed that a data breach will be taken to be of a significant scale when at least 500 or more individuals are affected.[15]

3.37. Singtel is of the view that the threshold proposed by the PDPC is currently set too low.

3.38. The PDPC appears to have based the "significant scale" threshold on the position taken in the Californian Civil Code (**Code**).[16] The obligation to notify of data breaches of a significant scale in the Code relates to breaches in respect of sensitive information only i.e. first name and last name in combination with social security number, drivers licence number, account number, medical information, health insurance information, etc.[17]

3.39. In comparison, a data breach as set out in the Consultation Paper appears to be set out in respect of "personal data" generally. Under the PDPA, personal data is defined as "any data, whether true or not, about an individual who can be identified from that data or, from that data and other information to which the organisation has or is likely to have access".[18] In this context, it would not be appropriate to draw on and use a threshold from a regime which is focused on more sensitive forms of information.

3.40. Singtel is of the view that the threshold applicable to data breaches of a significant scale should be raised to 10,000 affected individuals. Such a position is consistent with the position taken under South Korea's *Personal Information Protection Act*.[19] This is especially given that this criterion is for situations where the personal data breach does not pose any risk of impact or harm to the affected individuals.

---

[15] Paragraph 6.2(b), Consultation Paper.
[16] Paragraph 6.2(b), Consultation Paper.
[17] Section 1798.82(3)(h), *California Civil Code*.
[18] Section 2, PDPA.
[19] Article 34(3), *Personal Information Protection Act*, read with Article 39(1), *Enforcement Decree of the Personal Information Protection Act*.

Singtel

General cautions

3.41. The PDPC has stated in its Consultation Paper that notification to affected individuals will enable them to take the necessary steps to protect themselves from the risks or impact from the data breach.[20]

3.42. Singtel cautions the PDPC against taking a view that notification will always provide individuals with the ability to protect themselves. There may be situations where neither the organisation nor an individual will be certain of the full extent of the harm resulting from the data breach. For example, if the information was accidentally published then the organisation cannot be certain who has received the information and how the individual can take steps to protect itself especially if the information is of a kind which cannot be altered (for example, name, gender and NRIC).

3.43. As such, in developing a regime to guide mandatory data breach notification, the PDPC should be aware that it is misleading to assume that a mandatory notification framework will provide the individuals with the ability to protect themselves in all circumstances.

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?

3.44. Singtel supports the PDPC's effort to provide for efficiency but it is not clear whether the proposal is viable and practicable. Singtel would prefer that the proposal in paragraph 6.3 (a) of the Consultation Paper be subject to further discussion.

3.45. To illustrate Singtel's concerns, Singtel notes that the requirements under other sectoral regulations could be based on different thresholds and therefore, aligning the notifications [such that a notification required another law/regulation would indirectly therefore apply under the PDPC framework] would be inappropriate.

3.46. Singtel also notes that the *Cyber Security Bill* was only just recently consulted on and the Bill has not yet been passed.[21] Guidelines for the implementation have not even been set

[20] Paragraph 6.2(a), Consultation Paper.
[21] "Singapore's Cybersecurity Bill delayed to 2018", http://www.channelnewsasia.com/news/singapore/singapore-s-cybersecurity-bill-delayed-to-2018-9225622, 19 September 2017.

out or consulted on. It would not be possible to envisage the nature of the notifications under the Bill as compared to those envisaged by the PDPC.

3.47. Furthermore, even if a comparison were to be made between the provisions proposed by the PDPC and relevant ones in the Bill, the proposed concurrent application of PDPA's data breach notification requirements may in fact be impracticable due to the application of a relevant 'secrecy provision' in the Bill.

3.48. For example, it is proposed that under the *Cyber Security Bill*, the Commissioner of Cybersecurity may designate computers or computer systems designated as critical information infrastructure (**CII**) during times of national emergency. Designation as CII is an 'official secret' under the Official Secrets Act and shall not be divulged to the public.[22] As such, concurrent notifications to the Commissioner of Cybersecurity in respect of a significant cybersecurity incident involving CII and to the PDPC would be impracticable.

3.49. In Australia, the inconsistent operation of mandatory data breach notification requirements and a 'secrecy provision' which prohibits or regulates the use or disclosure of information is recognised. Under the *Privacy Amendment (Notifiable Data Breaches) Act 2017*, it is an exception to the obligation to notify, if compliance with the obligation would be inconsistent with a secrecy provision.

3.50. Consequently, without further discussion or consultation on the possible guidelines on concurrent notification, it would not be advisable to make that a requirement or obligation. Singtel reiterates that even where there is a concurrent application, an exception must be introduced to the PDPC's proposed concurrent application requirement, so that an organisation will not be in breach of such a requirement if compliance with it would be inconsistent with any 'secrecy provision' in any other prevailing legislation that prohibits or regulates the use or disclosure of information.

[22] Public Consultation Paper on the Draft Cybersecurity Bill, issued by the Ministry of Communications and Information and the Cyber Security Agency of Singapore on 10 July 2017, page 8.

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

3.51. Singtel agrees with the principle that an organisation should not be required to notify individuals under mandatory data breach notification obligations if notification is likely to impede enforcement obligations. The PDPC should provide further clarification in respect of how this exception will operate.

3.52. Section 4 (6)(b) of the PDPA currently provides that to the extent that Parts III to VI of the PDPA are inconsistent with the provisions of another written law, the provisions of the other written law will prevail. To cater for a law enforcement exception, section 4 (6)(b) should be amended to extend the exception to include directions made by a law enforcement agency or officer pursuant to such a written law.

3.53. The PDPC should also make it clear that failure to comply with an obligation under Parts III to VI of the PDPA as a result of the operation of section 4 (6)(b) will not attract any consequences or penalties.

3.54. In respect of the technological protection exception proposed by the PDPC, the requirement that encryption be "to a reasonable standard" is unclear. Singtel prefers that an approach be taken similar to that in Article 34(3) of the EU (Regulation (EU) 2016/679 – General Data Protection Regulation.[23] Such an approach provides a sufficient level of clarity and certainty to organisations.

3.55. Singtel also encourages the PDPC to consider adding an exception when an organisation has already undertaken remedial action in respect of the data breach which effectively removes the need to notify affected individuals. A similar exception is taken in Australia.

3.56. In Australia, it is an exception to the mandatory data breach notification obligation if:

- an organisation takes action in relation to a breach before it results in serious harm to any of the individuals to whom the information relates; and

[23] 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.

- a reasonable person would conclude that as a result of that action the breach would not be likely to result in serious harm to any of those individuals.[24]

3.57. In Singtel's view, such an exception will reduce the administrative burden on organisations to notify individuals when a risk of harm is removed, and would reduce the likelihood of creating unnecessary alarm among individuals.

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

Notification time frames – notification to individuals

3.58. The PDPC recommends that the organisation notifies all affected individuals as soon as practicable. Singtel supports the PDPC inclusion of a practicality threshold as this is an important consideration for organisations. The PDPC has proposed to allow organisations to determine what "as soon as practicable" means in light of their own circumstances, however the term can be open to wide interpretation. As such, Singtel welcomes further clarification from the PDPC on how it will assess compliance with this standard.

3.59. This threshold for "as soon as possible" can vary from organization to organization and can even be interpreted by individuals or affected end-users as "almost immediately". Organisations will require a sufficient degree of scope to conduct internal assessments, investigate the data breach, and develop appropriate notifications to affected individuals. In the case of the latter, issues of resource are to be considered, e.g. in some cases, emails and SMSes can be sent but in other cases, letters have to be mailed out. Therefore, the PDPC should provide some guidelines as to the maximum time organisations should be given, e.g. up to one (1) month to notify the end-users or affected individuals, given that time is needed to investigate and establish facts, craft messages etc.

3.60. An additional concern for Singtel is the issue of when the applicable time frame for notification commences. The Consultation Paper states that when a data breach meets the criteria for notifying affected individuals, the organisation must notify all affected

[24] Section 26WF, *Privacy Amendment (Notifiable Data Breaches) Act 2017.*

individuals as soon as practicable.[25] However, as noted in our response to question 5, there may be circumstances when an organisation only has a reasonable suspicion that a data breach has occurred. In such circumstances, Singtel would suggest that the applicable timeframe should only commence once an organisation has undertaken necessary assessments and has confirmed that a breach has in fact occurred.

Notification timeframes – notification to PDPC

3.61. The PDPC has proposed a 72 hour timeframe for notification of data breaches to the PDPC itself, commencing from as soon as the organisation is aware of the data breach.

3.62. In Singtel's view, 72 hours is too short a timeframe. It will take time for an organisation to determine or have a fair idea of the scale and extent of the breach, and to consider if and how individuals will be affected.

3.63. An organisation will also require time to determine how it should address the breach. Therefore, it is unclear when an organisation will be considered to have been "aware of the data breach". Similar to the position in paragraph 3.60, the timeframe applicable for notifying the PDPC of a data breach should only commence once an organisation has sufficient time and information to determine whether or not there is a data breach and to assess the severity of the breach.

3.64. Organisations should be given up to seven (7) working days to notify the PDPC of a data breach.

4. CONCLUSION

4.1. Singtel appreciates the opportunity to contribute to the consultation process on this important area of public policy.

4.2. Singtel welcomes the proposals set out in the Consultation Paper as a necessary update to the current data protection regime under the PDPA. Singtel supports the major proposals made by the PDPC and would encourage it to further develop the proposals and provide further detail to organisations in respect of how the proposals will be practically implemented.

[25] Paragraph 6.12, Consultation Paper.

4.3. We look forward to engaging further with the PDPC on this important matter.