PUBLIC CONSULTATION
by
Personal Data Protection Commission

APPROACHES TO MANAGING PERSONAL DATA IN THE DIGITAL ECONOMY

COMMENTS

Gn Chiang Soon
PDataCare Consultancy Pte Ltd
PDataCraft Consultancy LLP
CS GN Law Chambers
email: chiangsoon@gmail.com
tel: 96168660

Mimi Oh
Ethos Law Corporation
email: mimi.oh@ethoslaw.com.sg
tel: 97866950

Michael S Chia
MSC Law Corporation
email: michael.s.chia@msclawcorp.com
tel: 98870942

4 September 2017

COMMENTS

NOTIFICATION OF PURPOSE

Proposal

To allow organisations to collect, use and disclose personal data without consent by providing the appropriate notification of purpose where:

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

b) the collection, use or disclosure of the personal data is not expected to have any adverse impact on the individuals.[1]

Questions

1. Should the Act provide for Notification of Purpose as a basis for collecting, using and disclosing personal data without consent?[2]

2. Should the proposed Notification of Purpose approach be subject to conditions? If so, what are your views on the proposed conditions (i.e. where it is impractical to obtain consent and not expected to have any adverse impact on the individual)?

Comments

Overall – In General

1. In principle the writers support the various proposed enhancements to the framework for collecting, using and disclosing personal data under the Act as stated in the Consultation Paper, provided the terms, phrases and words used to describe and represent the enhancements, namely, the exceptions and conditions, are well defined, the scope of their application is clear, and they are easy to apply.

1.1 Hence, the writers' comments will be directed mostly at the wordings used to describe the exceptions and conditions, their clarity, whether and how they would work and fit in harmoniously with other existing provisions of the Act.

---

[1] Para 3.8 of the Consultation Paper:-
'PDPC is thus considering providing for Notification of Purpose as a basis (that is not tied to the consent requirement) 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 (make it clear that it is subjective, case to case according to the individuals concerned) on the individuals.'

[2] These questions are found below para 3.11 of Part II: Enhanced Framework for Collection, Use and Disclosure of Personal Data

Exception

2. As it is the intention of the Commission to maintain and keep consent as the key basis for the collection, use and disclosure of personal data[3], and to allow the collection, use and disclosure of personal data without consent by way of giving notification of purpose where it is **'impractical** to obtain consent' and it is '**not expected to have any adverse impact on the individuals'**, the writers view the current proposal as another exception to the existing regime of consent under the Act

2.1 Hence, perhaps the above two questions can be conflated to read as:

'Should the Act provide '**Notification of Purpose'** as an exception for collecting, using and disclosing personal data without consent where it is impractical to obtain consent and it is not expected to have any adverse impact on the individual?'

3. The writers' view is that the idea of providing Notification of Purpose for the collection, use and disclosure of personal data without consent in the circumstances stated merits consideration, provided the stated conditions of ***'not expected to have any adverse impact on the individual'*** and it is ***'impractical to obtain consent'***[4] are better defined, refined and worded as elaborated below.

Not expected to have any adverse impact

4. Whether the collection, use and disclosure of personal data of an individual is expected to have an adverse impact on that individual, can be a challenging question for an organisation. This is because the effect of an impact when assessed individually and subjectively can vary from person to person.

Is it a subjective or objective test?

4.1 Unless expressly stated, the condition ***'not expected to have any adverse impact on the individual'*** appears to provide a subjective test. The fulfilling requirement is stated as '***not expected to have***' and not '***not <u>reasonably</u> expected to have***'. The latter would indicate that an objective test is to be applied. Using a subjective test, the fulfilment of the said proposed condition will have to be determined from the point of view of that individual. This then raises the question of what if the individual has a peculiar character or personality that makes him particularly sensitive to the impact and which thereby made it adverse, when in normal circumstance it would not be so.

4.2 Hence, it is important for the Commission to make it clear by adopting the appropriate language as to whether the intention is for the impact to be assessed objectively or subjectively.

---

[3] Para 3.2 of the Consultation Paper:-
'PDPC proposes for consent to remain a key basis for collecting, using and disclosing personal data under the PDPA to provide individuals the right to exercise choice and control over their personal data. Organisations should therefore seek to obtain consent for the collection, use or disclosure of personal data where seeking consent is practical, especially where there could be any adverse impact or risks to the individual.'

[4] These conditions are elaborated in para 3.8 of the Consultation Paper.

4.3 The adverse impact can be described as a matter of degree, such as, little, inconsequential, and mild, great, grave and serious. For the purpose of this exception, any organisation would like to know the degree of impact required to constitute an adverse impact in order to gauge whether they can avail themselves of the benefits of this exception.

Impractical for the organisation to obtain consent

5. For the purpose of fulfilling the proposed condition of ***'impractical to obtain the consent of an individual'***, organisations may wish to know whether ***'inconvenience'*** is good enough to constitute an 'impractical' situation for them to obtain consent. It is the writers' view, that inconvenience may not be adequate and that more explanations or illustrations are required. The question then is how difficult must the situation be in order to be considered as 'impractical'?

5.1 It may appear to be a straightforward question for organisations to decide what is impractical, but in practice, in the absence of illustrations and explanations on what constitutes an impractical situation under the Act, organisations may err on the side of caution and may hesitate to conclude that consent is not required for fear that its decision may be challenged by the individuals concerned. To resolve this doubt, perhaps the Act can define and/or give examples and illustrations of what is **'impractical'** for the purpose of this exception. Such illustrations can also further assist to indicate whether organisations can include administrative, financial, technological and technical factors in their assessment besides those emanating from the individuals.

6. It is noted that the condition for the exception of collection, use and disclosure of personal data without consent under the 2nd Schedule, para 1(a), 3rd Schedule, para (1a) and 4th Schedule, para 1(a) of the Act, is that consent cannot be obtained in a ***'timely way'***, instead of ***'impractical'*** to do so[5]. Is there a reason for the condition of this new exception to be worded differently? Is it meant to be a wider or narrower or similar condition?

6.1 If there is no reason to require a differently worded condition, then, for purpose of simplicity and consistency, perhaps a commonly worded condition can be adopted for both the proposed and aforesaid existing conditions.

Forms of Notification of Purpose

7. If it is the decision of the Commission to leave it to the organisations to decide on the form of notification that they deem most appropriate[6], then it should be made clear that

---

[5] 3rd Schedule, para 1(a) –
'An organisation may use personal data about an individual without the consent of the individual in any of the following circumstances:
(a) the use is necessary for any purpose which is clearly in the interests of the individual, if **consent for its use cannot be obtained in a timely way** or the individual would not reasonably be expected to withhold consent;'

[6] Para 3.9 of the Consultation Paper –
'PDPC proposes for organisations that wish to rely on this approach to provide appropriate notification of the purpose of the collection, use or disclosure of the personal data, and where it is feasible for the organisation to allow individuals to opt out of the collection, use or disclosure, information about how individuals may opt out. **PDPC does not intend to prescribe how organisations are to notify individuals, but will leave it to organisations to assess and determine the most appropriate form of notification** to ensure the individuals are made aware of the purpose of the collection, use and disclosure of their personal data.'

the form of notification chosen must not only be appropriate but also effective in bringing the notification to the knowledge of the individuals. This is because what is appropriate may not necessarily be effective.

7.1 For instance, inserting a notification in a 20-sentence page on the organisation's website would have a different degree of effectiveness compared to a notification, say, inserted somewhere in a 20-page website.

7.2 In the writers' opinion, effectiveness of the form of notification is more important than its appropriateness. This is to ensure that the individual will become aware of the fact that his personal data has been or will be collected, used or disclosed without his consent for a certain purpose by a particular organisation, and if indeed there were any adverse impact on him, he would have a timely opportunity to bring it to the attention of the organisation and/or the Commission.

Purpose

8. One issue constantly encountered by the writers in explaining the application of the terms of the Act, is how specific and detailed must purpose be stated when giving notification of the purpose of the intended collection, use and disclosure of personal data? For instance, for the collection of a purchaser's name, home address and telephone number, is it sufficient for the organisation to broadly describe the purpose as ***'for us to communicate with you'***, or must it be more detailed and specific like ***'for us to communicate with you regarding the delivery, maintenance and servicing of the products that you have just purchased from us'*****?**

Commission's Guidelines

8.1 The Commission has issued guidelines on this matter[7] for the existing regime of consent. Are these guidelines sufficient for the purpose of this new exception? It is to be noted that these guidelines were issued to apply to notification of purpose where consent is required to collect, use and disclose an individual's personal data. Whereas the notification of purpose proposed herein, is for situations where the personal data is or will be collected, used or disclosed without consent. Clearly the circumstances for the two situations are quite different.

8.2 In the writers' view, this is a timely occasion to make clear how detailed and specific the purpose in a notification must be, so that it can be consistently applied to both situations where consent is required under the existing regime and where it is dispensed with under the proposed exceptions. In this regard, the writers are of the view that the purpose to be notified for the proposed exception needs to contain detailed information and be as specific and detailed as possible. For instance, **'the purpose of collecting the medical data on your diabetes is to develop a drug to cure it'** would be preferred to the **'purpose of collecting your medical data is for carrying out medical research'.**

[7] A GUIDE TO NOTIFICATION, page 27 - GENERAL PRINCIPLES ON STATING PURPOSES - 'The purpose(s) must be specified in some **reasonable level of detail**. Organisations are not required to list all the activities and processes that are part of the purpose(s). Consider if particular purposes should be highlighted - Purpose(s) that are likely to be of particular concern to the individual (e.g. for marketing or disclosure to third parties); or Unexpected in the context of the notification.'

LEGAL OR BUSINESS PURPOSE

Proposal

To provide for the collection, use and disclosure of personal data without consent and without notification of purpose where it is necessary for a legal or business purpose and:

(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.[8]

Questions

3. Should the Act provide for Legal or Business Purpose as a basis for collecting, using and disclosing personal data without consent and notification?

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)?[9]

Comments

9. It is observed by the writers that the exception of Legal or Business Purpose is intended to have a wider effect on the consent regime than the exception of Notification of Purpose. Under the Legal or Business Purpose exception, organisations are not required to obtain consent or notify individuals of the purpose of the collection, use and disclosure of their personal data. As the effect of this exception is far greater, its description and conditions ought to be more vigorously examined and made as clear and unambiguous as possible.

Benefits to the public (or a sector thereof)

10. It is not difficult to see how the balancing-formula worded condition of ***'the benefits to the public (or a sector thereof) clearly outweigh any adverse impact or risks to the individual'*** applies to the case of ***'organisations sharing information and personal data of customers in order to identify and prevent fraudulent activities'***[10] as the degree of

---

[8] Para 3.15 of the Consultation Paper –

'To cater to such circumstances, PDPC proposes 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"). In addition, PDPC considers 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. PDPC is therefore proposing **not to subject organisations to the requirement to notify individuals of the purposes** when collecting, using or disclosing personal data in these circumstances. The proposed Legal or Business Purpose would be 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.'

[9] These questions are found just after para 3.17 of the Consultation Paper

[10] Para 3.14 of the Consultation Paper –

'PDPC recognises that there may be other 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

benefits therein is clear. Neither is it difficult to see why ***'it is not desirable or appropriate to obtain consent'*** from the individuals concerned for this purpose[11].

10.1 However, unless the degree of benefits required is made certain by the Act, this balancing-formula worded condition may not be easy to apply, as benefits can be a matter of degree such as little, much, a lot, a great deal, significant and substantial.

10.2 For instance, would this exception and its balancing-formula worded condition apply if a group of insurance companies want to disclose the names of drivers, who had been involved in road accidents during a period of time, say, in the last 36 months, in return for the benefits of the driving public having to pay a lower insurance premium?

10.3 Organisations with big plans to gather, use and share personal data to conduct long-term expensive experiments and trials would be greatly aided in their decision to proceed if the Act can further refine the balancing-formula worded condition to indicate the degree of benefits required. In this regard, it may want to consider adding the preceding word **'considerable'** or **'substantial'** to the word, **'benefits'** if the intention is to exclude benefits that are either insignificant or negligible to any sector of the public.

10.4 Further, the balancing-formula worded condition requires every set of benefits to be weighed against each and every adverse impact on the individuals. Thus, this poses the question of who is the deciding body to make that crucial determination. The absence of a central authority to make this determination may cause many interested organisations to hesitate, question their own assessment and wonder whether it will be upheld when challenged. For it to work, the writers strongly advocate the provision of an assessment panel, to serve as a mechanism for organisations to test their assessment by putting forth their plan for determination.

10.5 It is also noted that the term ***'benefits to the public'*** is worded differently from the term ***'in the public interest'*** used in the exception under the 4th Schedule, para 1(g) of the Act[12]. Furthermore, the full term of the proposed condition of ***'benefits to the public (or a sector thereof)'*** raises the question of whether the existing condition of ***'in the public interest'*** would be satisfied if the interest benefited only a sector of the public? For simplicity and consistency perhaps the Commission may want to take this occasion to consider the use of similar wordings and description for both the aforesaid existing and proposed conditions.

---

authorised under the PDPA or other written laws (e.g. the **sharing and use of personal data to detect and prevent fraudulent activities**).'

[11] Para 3.15 of the Consultation Paper –

' The proposed Legal or Business Purpose would be 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.'

[12] 4th Schedule, para 1 –

'An organisation may disclose personal data about an individual without the consent of the individual in any of the following circumstances:

(g) the **disclosure** is to a public agency and such disclosure is necessary **in the public interest**;'

Business Purpose

11 As pointed out in the Consultation Paper[13] the term **'Legal or Business Purpose'** is already set out in s.22[14] and s.24[15] of the Act.

11.1 The writers would also like to add that under the existing consent regime, there are issues with regard to interpretation of the term, ***'business purpose'***. To begin with, what exactly constitutes ***'business purpose'***? For instance, under s. 24 of the Act, can a recruitment organisation continue to retain the personal data of all the applicants who responded to its advertisement for a particular position on the ground that these personal data can be used to fill up similar positions in the future and henceforth, these personal data are necessary for its business purpose?

11.2 Again, can a club or an association refuse to remove from its record the personal data of members, who have terminated their membership as stipulated under s. 24 on the ground that it is necessary for its 'business purpose' to continue to communicate with these former members and to keep them informed and interested in the club's or the association's activities?

11.3 To apply s.24, one can argue that the **'business purpose'** ought to be restricted and tied to its original business purpose for which the personal data was initially collected and that the personal data cannot be kept for any other business purposes which the individuals were not notified of. As regarding the proposed exception, there is no **'original business purpose'** to tie or restrict its application or the meaning of 'business purpose'.

11.4 Apart from that, it is salient to note that s. 24 also requires the organisation to show that the retention of personal data is necessary for its business purpose. Hence, this raises the question of whether it is the intention of the Act not to require organisations, utilising the proposed exception of Legal or Business Purpose, to also show that the collection, use and disclosure of such personal data is necessary for their business purpose?

---

[13] Para 3.13 –
'Presently, the PDPA recognises the need to strike a reasonable balance between the need for organisations to collect, use and disclose personal data with individuals' right to protection of their personal data. The PDPA therefore provides for organisations to collect, use or disclose personal data without consent **for certain legal or business purposes**, such as where it is necessary for any investigation or proceedings, to recover a debt, or for a research purpose. The PDPA also provides for the retention of personal data where necessary **for a business or legal purpose**, and for the transfer of personal data out of Singapore for certain legal and business purposes prescribed in the Personal Data Protection Regulations 2014'

[14] S22**(2) –**
'Unless the organisation is satisfied on reasonable grounds that a correction should not be made, the organisation shall —
(a) correct the personal data as soon as practicable; and
(b) subject to subsection (3), send the corrected personal data to every other organisation to which the personal data was disclosed by the organisation within a year before the date the correction was made, unless that other organisation does not need the corrected personal data **for any legal or business purpose.**'

[15] S24 –
'An organisation shall cease to retain its documents, or remove the means by which the personal data can be associated with particular individuals, as soon as it is reasonable to assume that —
(a) the purpose for which that personal data was collected is no longer being served by retention of the personal data; and
(b) retention is no longer necessary **for legal or business purposes.'**

11.5 It is thus important and useful to define what comes within the term **'business purpose'** under the proposed exception, otherwise the term can be read to include potential future business purpose, any big or small business purpose so long as it can be said to be related in some way to the business of the organisation. Therefore, is it the intention to allow all types of personal data to be collected, used and disclosed under the proposed exception of **'business purpose'**?

Whether to use 'legitimate purpose'?

12. The writers are of therefore of the view that the term **'Legal or Business Purpose'** can be replaced by the term ***'Legitimate Purpose'***. The term ***'Legitimate Purpose'*** is proposed because to come within it, factors other than the business purpose of the organisation can be considered. For a purpose to be legitimate, the organisation needs to show that there is also a reasonable and rightful purpose to do so. For instance, to disclose a customer's purchase price may be within the organisation's business purpose to do so, but the organisation may not have a legitimate purpose if the customer has not given the organisation any good cause to reveal it.

MANDATORY DATA BREACH NOTIFICATION

Proposal

To require organisations to notify affected individuals and the Commission of any data breach involving unauthorised access, collection, use, disclosure, copying, modification, disposal of personal data or similar risks[16], that poses any risk of impact or harm to them[17]; and to notify the Commission even where there is no risk of impact or harm to affected individuals if the number affected is 500 or more[18].

Question

5. What are your views on the proposed criteria for data breach notification to affected individuals and to the Commission? 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 the Commission?[19]

---

[16] Footnote no. 23 –
'A **data breach refers** to the unauthorised access, collection, use, disclosure, copying, modification, disposal of personal data or similar risks.'

[17] Para 6.2(a) of the Consultation Paper -
'The PDPC proposes to adopt the following **criteria for notification** to affected individuals and/or PDPC of a data breach:
a) **Risk of impact or harm** to affected individuals – Organisations must notify affected individuals and PDPC of a data breach that poses any risk of impact or harm to the affected individuals.'

[18] Para 6.2(b) of the Consultation Paper -
'The PDPC proposes to adopt the following criteria for notification to affected individuals and/or PDPC of a data breach:
b) Significant scale of breach – Organisations must notify PDPC where the scale of the data breach is significant, even if the breach does not pose any risk of impact or harm to the affected individuals. PDPC is proposing for a data breach **involving 500** or more affected individuals to be considered of a significant scale that would need to be notified to the PDPC'

[19] This question appears just after para 6.2 of the Consultation Paper.

Comments

Any risk of impact or harm

13. It is noted that the conjunctive word used between the criteria of **'impact'** and **'harm'** is ***'or'*** and not ***'and'*.** In the writers' view this would mean that the notification obligation will apply to almost every data breach. This is because, unless the term **'risk of impact'** is further refined to refer only to '**adverse impact'**, it would encompass risk, impact and harm of any kind and size, including minor and harmless ones.

13.1 Under the criteria of ***'scale of data breach,'*** where notification of the breach is required to be given to the Commission, even if the data breach poses no risk of impact or harm to the individuals[20], notification must be given even when the impact is harmless or negligible. This is because the subject matter of concerns therein, is the personal data protection and security system of the organisations and not the individuals.[21]

13.2 However, in the case of the criteria where the data breach ***'poses … risk of impact or harm'*** to affected individuals, the subject matter of concerns, are the risk, impact and harm to the individuals. Hence, is it the intention to require notification to individuals even when the impact is also harmless and negligible? If a certain degree of adverse impact or harm is the intended requirement, then, the conditions may be stated as 'risk of **adverse** impact or harm' or 'risk of impact **and** harm'.

13.3 Another clarification sought by the writers is whether the type and degree of risk, impact and harm under this proposed exception differ from the impact and harm that ***'threaten the safety or physical or mental health'*** and ***'cause immediate or grave harm to the safety or to the physical or mental health'*** of the individuals, as contained in s. 22(3)[22], or that ***'threatens the life, health or safety'*** of the individuals, as contained in 2nd, 3rd & 4th Schedules, para 1(b) therein ?[23] The present proposed term of ***'any risk of impact or harm'*** appears to have a wider application. Is that the intended effect?

13.4 The next clarification sought is whether the criteria of **'risk of impact or harm'** is confined to the individuals whose personal data is being collected, used and disclosed, or does it

---

[20] Para 6.2(b) –
'Significant scale of breach – Organisations must notify PDPC where the scale of the data breach is significant, even if the breach does not pose any risk of impact or harm to the affected individuals.'

[21] Para 6.2(b) –
'Data breaches of a significant scale could **indicate a systemic issue** within the organisation, which may require PDPC's further investigation and guidance to the organisation on implementing the appropriate remedial actions to address it.'

[22] Section 22 (3) –
(3) An organisation shall not provide an individual with the individual's personal data or other information under subsection (1) if the provision of that personal data or other information, as the case may be, could reasonably be expected to —
(a) threaten the **safety or physical or mental health** of an individual other than the individual who made the request;
(b) cause **immediate or grave harm to the safety or to the physical or mental health** of the individual who made the request;

[23] 2nd Schedule, para 1(b) –
' An organisation may collect personal data about an individual without the consent of the individual or from a source other than the individual in any of the following circumstances:
the collection is necessary to respond to an emergency that **threatens the life, health or safety** of the individual or another individual;'

apply to other individuals? In the existing exception of disclosing personal data without consent under the 4th Schedule, para 1(b) & (c), the risk of impact and harm applies to other individuals as well[24]. In the writers' view, the proposed risk of impact or harm in the proposed exception should thus apply to other individuals as well.

Guidelines

14. In the Consultation Paper it is stated that the Commission will develop and issue guidelines to organisations on the assessment of risk of impact or harm to affected individuals[25]. The writers are of the view that since only illustrations and definitions given in the Act have binding legal effect on the interpretation of the provisions, and guidelines issued outside the Act only have persuasive effect, it may be better to have the exact and intended meaning of the proposed exception and conditions incorporated into the statutory provisions of the Act rather than left to guidelines.

Scale of data breach

15. Though the number of data breaches that would require notifying the Commission should be based on what is indicative of a systemic problem[26] in an organisation, the writers are of the view that the size of a country's population ought to be of some considerations as well. As 700 affected individuals constitute a mere 0.0035% in a country of 20 million people and 500 affected individuals is 0.01% in a country like Singapore where the population is around 5 million people, perhaps, the triggering number for the proposed purpose can be slightly higher than the proposed 500 affected individuals. In the writers' view, it can be in the region between 1,000 to 1,500 affected individuals.

EXCEPTIONS AND EXEMPTIONS FROM BREACH NOTIFICATION

Proposal

All the exclusions under s. 4 of the Act, are to apply to the proposed breach notification provisions under the Act, i.e., any individual acting in 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; and where provisions of other written law are inconsistent with the proposed breach notification provisions under the Act[27].

---

[24] 4th Schedule, para 1 –
'An organisation may disclose personal data about an individual without the consent of the individual in any of the following circumstances:
(b) the disclosure is necessary to respond to an emergency that threatens the **life, health or safety of** the individual **or another individual**;
(c) subject to the conditions in paragraph 2, there are reasonable grounds to believe that **the health or safety of** the individual **or another individual** will be seriously affected and consent for the disclosure of the data cannot be obtained in a timely way;'

[25] Para 6.2(a) and footnote 34 of the Consultation Paper-
'PDPC will **develop and issue guidelines** to provide guidance to organisations on **assessing risk of impact or harm** to affected individuals.'

[26] Para 6.2(b) of the Consultation Paper –
'PDPC is proposing for a data breach **involving 500** or more affected individuals to be considered of a significant scale that would need to be notified to the PDPC. Data breaches of a significant scale could indicate a **systemic issue within the organisation**, which may require PDPC's further investigation and guidance to the organisation on implementing the appropriate remedial actions to address it.'

[27] Para 6.9 of the Consultation Paper

Question

7. What are your views on the proposed exceptions and exemptions from the data breach notification requirements?[28]

Comments

Public agencies

16. As the stated reason to require organisations to notify individuals of the data breach is to enable affected individuals to take remedial steps to protect themselves[29] the writers are of the view that public agencies ought to be required to provide such notification too.

16.1 S. 4[30] of the Act exempts public agencies only with regards the obligations set out in Parts III to VI of the Act. It does not exempt them of the obligations under Part IX of the Act, where the personal data involved are individuals' Singapore telephone numbers.

16.2 In Part IX therein, public agencies are required to comply with the obligations contained therein, such as, sending business messages to individuals' Singapore telephone numbers.[31] If public agencies have leaked the individuals' personal data, the writers can see more benefits than harm to require them to inform the individuals concerned so that the individuals can take steps to manage the risk of the impact and harm.

16.3 However, if, on grounds of national interests and/or national security, public agencies are to be exempted from notifying affected individuals of the data breach, then it is also the writers' view that the public agencies should at least be required to notify the Commission of the data breach.

Organisation in the course of acting on behalf of a public agency

17. Similarly, for the same reasons, if the data breach is caused by organisations acting for public agencies, these organisations also ought to be required to notify the affected individuals. This should be so whether or not the public agencies that they are working for are exempted, unless the public agencies concerned have already provided the notification to the affected individuals.

17.1 The writers noticed that such organisations are also treated differently from the public agencies that they are working for, under Part IX, 8th Schedule, para 1(a) of the Act[32],

---

[28] This question is found just after para 6.11 of the Consultation Paper.

[29] Para 5.3 of the Consultation Paper –
'With mandatory data breach notification, affected individuals who are notified of the data breach will have the opportunity to **take steps to protect themselves** from the risks or 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.'

[30] Section 4 –
'(1) Parts III to VI shall not impose any obligation on —
(c) any public agency or an organisation in the course of acting on behalf of a public agency in relation to the collection, use or disclosure of the personal data;'

[31] 8th Schedule, para 1 -
'For the purposes of Part IX, a specified message shall not include any of the following:
(a) any message sent by a **public agency** under, or to promote, any programme carried out by any public agency which is **not for a commercial purpose**;

[32] 8th Schedule, para 1 -
'For the purposes of Part IX, a **specified message shall not include** any of the following:

wherein such public agencies do enjoy a certain degree of exemptions when sending specified messages, but not the organisations acting for them.

Personal and domestic purpose

18. Under the existing consent regime, it is not spelt out in the Act, whether an individual claiming to collect, use and disclose personal data without consent under the exemption of **'personal and domestic purpose'** can do so only for personal data that are themselves of a personal or domestic nature. For instance, can a nurse disclose the name of her clinic's patients when she talks to her boyfriend after work under the exemption of **'personal and domestic purpose'**?

18.1 Similarly, for the purpose of data breach notification, can a nurse be exempted from this obligation if she has caused the data breach of her clinic patients' medical records while working on her own personal computer at home after work?

18.2 The writers are of the view that it is timely if the Commission can take this occasion to clarify, whether the exemption of **'personal and domestic purpose'** is to apply only wherein the subject personal data itself is of a ***'personal or domestic'*** nature.

CONCLUSION

NOTIFICATION OF PURPOSE

Questions 1[33] **& 2**[34]

We therefore conclude as follows:

1. Yes, the Act can provide for Notification of Purpose as a basis for collecting, using and disclosing personal data without consent and subject the approach to the conditions of **'impractical to obtain consent'** and **'not expected to have any adverse impact on the individual'**, with some clarifications and modifications.[35]

1.1 Need to manage and provide clear illustrations and definition of the terms **'not expected to have any adverse impact'** and **'impractical for the organisation to obtain consent'**. ***Not expected to have any adverse impact***

1.2 Clarify whether an impact is to be assessed subjectively from the individual's point of view or objectively?[36]

(a) any **message sent by a public agency** under, or to promote, any programme carried out by any public agency which is not for a commercial purpose;

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

[34] 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)?

[35] Paras 1 & 3 of the Comments.

[36] Paras 4 & 4.2 of the Comments.

1.3 Propose to use the term '**not reasonably expected to have any adverse impact'** instead of '**not expected to have any adverse impact'**.[37]

1.4 Clarify whether a certain degree or to what degree, an adverse harm, is required for an impact to be considered an **'adverse impact'**.[38]

Impractical for the organisation to obtain consent

2. Define what constitutes an **'impractical situation to obtain consent'**?[39]

2.1 Clarify how is **'impractical to obtain consent'** different from **'consent cannot be obtained in a timely way'**.[40]

2.2 Propose to use and adopt the same term either **'impractical'** or **'not in a timely way'** if no difference is intended.[41]

Form of Notification of Purpose

3. Propose to make it clear that the form of notification used must also be '**effective'.**[42]

Purpose

4. How specific and detailed must the purpose be described in a notification?[43]

4.1 Propose that the purpose in a notification, at least for this new exception, needs to be as specific and detailed as possible.[44]

LEGAL OR BUSINESS PURPOSE

Questions 3[45] **& 4**[46]

We therefore conclude as follows:

5. The exception of Legal or Business Purpose has wider effect on the existing consent regime as it dispenses with two obligations, namely, obligations to obtain consent and to notify purpose of collection, use and disclosure of personal data.[47]

---

[37] Para 4.1 of the Comments.
[38] Para 4.3 of the Comments.
[39] Paras 5 & 5.1 of the Comments.
[40] Para 6 of the Comments.
[41] Para 6.1 of the Comments.
[42] Paras 7 & 7.1 of the Comments.
[43] Paras 8 & 8.1 of the Comments.
[44] Para 8.2 of the Comments.
[45] Should the PDPA provide for Legal or Business Purpose as a basis for collecting, using and disclosing personal data without consent and notification?
[46] 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)?
[47] Para 9 of the Comments.

Benefits to the public (or a sector thereof)

6. Need to manage and provide clear illustrations and definition of the terms **'legal and business purpose'** and **'benefits to the public (or a section thereof)** clearly outweigh any **adverse impact or risks to the individual'**.

6.1. Clarify whether a certain degree or what degree of benefits is required to qualify as **'benefits to the public or a sector thereof'.**[48]

6.2. Propose a mechanism for organisations to apply to an assessment panel formed under the Act, for determination as to whether the potential benefits outweigh the adverse impact and risks to the individuals concerned.[49]

6.3. Is **'benefits to the public (or a sector thereof)'** meant to have the same application as **'in the public interest'** presently used in the Act? [50]

6.4. Propose to use the same wording if no differences are intended.[51]

Business Purpose

7. Clarify what constitutes **'business purpose'**[52]

7.1. Clarify whether organisations need to show that it is **'necessary'** for their business purpose in order to avail themselves of this proposed exception.[53]

7.2. Propose to replace the term **'Legal or Business Purpose'** with **'Legitimate Purpose'**.[54]

DATA BREACH NOTIFICATION

Question 5[55]

We conclude as follows**:**

Any risk of impact or harm

8. Need to manage and provide clear illustrations and definition of the term **'risk of impac**t **or harm to affected individuals'**.

8.1. Is '**risk of impact'** itself sufficient for the condition to be satisfied, similarly for **'harm'**, or must both elements be fulfilled in order for the condition to apply?[56]

---

[48] Paras 10 to 10.3 of the Comments.
[49] Para 10.4 of the Comments.
[50] Para 10.5 of the Comments.
[51] Para 10.5 of the Comments.
[52] Paras 11.1 and 11.2 of the Comments.
[53] Para 11.4 of the Comments.
[54] Para 12 of the Comments.
[55] 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?
[56] Para 13 of the Comments.

8.2. Need to clarify whether the term **'any risk of impact or harm'** means all sorts, types and degrees of risk, impact and harm, whether negligible or minimal?[57]

8.3. Propose for the conditions to be stated as **'risk of adverse impact or harm'** or **'risk of impact and harm'**[58]

8.4. Clarify how the degree and type of impact and harm envisaged here differs from those under the present terms set out in the Act, such as those that **'threaten the safety or physical or mental health'**, **'cause immediate or grave harm to the safety or to the physical or mental health'** and **'threatens the life, health or safety' of individuals.**[59]

8.5. Clarify whether the criteria **'risk of impact or harm'** apply to other individuals as well.[60]

Guidelines

9. Propose to have as many guidelines as possible to be incorporated under the Act as they have legal binding effect on the interpretation of the provisions.[61]

Scale of data breach

10. Propose to increase the triggering number from 500 affected individuals to between 1,000 and 1,500,[62] based on the size of the population in Singapore.

EXCEPTIONS AND EXEMPTIONS FROM BREACH NOTIFICATION

Question 7[63]

We conclude as follows:

Public agencies

11. Propose not to exempt public agencies from the obligation to provide notification of data breach.[64]

Organisation in the course of acting on behalf of a public agency

11.1. Propose not to exempt organisations acting for public agencies from the notification obligation too.[65]

[57] Paras 13 to 13.2 of the Comments.
[58] Para 13.2 of the Comments.
[59] Para 13.3 of the Comments.
[60] Para 13.4 of the Comments.
[61] Para 14 of the Comments.
[62] Para 15 of the Comments.
[63] What are your views on the proposed exceptions and exemptions from the data breach notification requirements?
[64] Paras 16 to 16.2 of the Comments.
[65] Para 17 of the Comments.

Personal and domestic purpose

12. Propose to take the occasion to clarify whether the exemption, **'personal and domestic purpose'** is to apply only wherein the personal data concerned itself is of a personal or domestic nature.[66]

Gn Chiang Soon

Mimi Oh

Michael S Chia

[66] Paras 18 to 18.2 of the Comments.