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

Issued 27 July 2017

TABLE OF CONTENTS

PART I: INTRODUCTION

1.1 The Personal Data Protection Act 2012 (the "PDPA") governs the collection, use and disclosure of individuals' personal data by organisations. The PDPA's data protection obligations are set out in Parts III to VI of the PDPA (the "Data Protection Provisions"). The functions of the Personal Data Protection Commission (the "PDPC") include, amongst others, promoting awareness of data protection in Singapore and administering and enforcing the PDPA.

1.2 Enacted in 2012 and taking effect from 1 July 2014[1], the PDPA was developed based on principles drawn from international frameworks, namely the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data [2] ("OECD Guidelines") and the APEC Privacy Framework[3], and benchmarked against the data protection regimes of key jurisdictions such as the EU, UK, Hong Kong, Canada, Australia and New Zealand.

1.3 The PDPA primarily provides for consent as the basis for collecting, using and disclosing personal data. The PDPC also adopts a voluntary approach for organisations to notify the PDPC and affected individuals of any data breaches that might cause public concern or risk of harm to affected individuals.

1.4 In view of technological advances and global developments, PDPC is reviewing the relevance of other bases for collecting, using and disclosing personal data under the PDPA, as well as considering the need for mandatory data breach notifications to PDPC and affected individuals under the PDPA.

[1] The Do Not Call Provisions took effect from 1 January 2014, and the full PDPA took effect from 1 July 2014.
[2] Published by the Organisation for Economic Co-operation and Development in 1980. A revised edition was published in 2013.
[3] Published by the Asia-Pacific Economic Co-operation forum in 2005.

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

2 Challenges for Consent

2.1 The fast emerging Digital Economy is presenting challenges for consent-based approaches to personal data protection. Ubiquitous computing has changed the nature of data collection from active interaction to a passive one where devices seamlessly collect and transmit personal data across communications networks. The growth of Internet of Things ("IoT") devices, machine learning and artificial intelligence has given rise to the ability to collate and analyse large amounts of data, opening up new possibilities to derive insights that can yield enormous benefits for individuals and society.

2.2 Increasingly, it may not always be possible to anticipate the purposes for using and disclosing personal data at the outset. Furthermore, where huge volumes of personal data involving large numbers of individuals are collected at high velocities and from a variety of sources, it may not be practical for organisations to seek individuals' consent in every instance of data collection, or to attempt to identify the individuals in order to seek their consent for every new purpose. In some cases, organisations do not have a means of contacting the individuals to seek their consent. Facilitating withdrawals of consent in some of these situations may also pose a challenge.

2.3 Relying only on consent for the collection, use and disclosure of personal data may have deleterious effects. A common phenomenon these days is for organisations to resort to obtaining consent based on lengthy or broadly worded notices that may not allow the individual to reasonably ascertain the purposes of the collection, use or disclosure of his or her personal data in order to provide meaningful consent. The frequent taking of consent and proliferation of verbose consent clauses may unduly burden individuals and cause consent fatigue. An approach that calibrates the balance of responsibilities by holding organisations accountable to act responsibly and adopt pre-emptive preventive measures can meaningfully address consent fatigue.

2.4 The consent approach also assumes that individuals, in exercising "informed" choice over their personal data, will weigh the cost to themselves and the benefits to the wider public. Individual consent decisions, however, may not always yield the most desirable collective outcomes for society. There may be circumstances where consent is not desirable or appropriate, such as for detection of fraud and security threats. A recalibration of the balance between individual autonomy and corporate responsibility may be necessary, particularly in situations where the use or disclosure

is appropriate, is expected to have broader systemic benefits or is unlikely to have any adverse impact on the individuals.

2.5 PDPC recognises the importance of data for innovation and growth. When harnessed optimally and responsibly, data analytics and machine learning can bring about positive transformations to both traditional and emerging industries. PDPC is therefore reviewing the PDPA to ensure the regulatory environment keeps pace with evolving technology in enabling innovation, while providing for effective protection for individuals' personal data in the changing landscape.

3 Review of Current Regime

3.1 The PDPA currently provides for the right of individuals to exercise choice and control over their personal data through consent, while also providing for other bases for organisations to collect, use and disclose personal data for legitimate purposes. In particular, section 13(b) of the PDPA provides that an organisation may collect, use or disclose personal data without consent where required or authorised under the PDPA or any other written law. The PDPA also authorises[4] the collection, use or disclosure of personal data without actual consent in certain circumstances, for example where consent is deemed[5], or where it is necessary in the interests of the individual, for any investigation or proceedings, or for a research purpose[6].

3.2 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.

3.3 Notwithstanding this, PDPC recognises the need to strengthen provisions for parallel bases for collecting, using and disclosing personal data under the PDPA, to cater to circumstances where consent is not feasible or desirable, and where the collection, use or disclosure would benefit the public (or sections thereof). In relying on parallel bases for collecting, using and disclosing personal data under the PDPA, greater responsibility would be placed on organisations to demonstrate accountability in ensuring the protection of personal data and safeguarding the interests of individuals.

[4] To avoid doubt, these authorisations under the PDPA do not affect any obligation or limitation under other laws (see PDPA Section 4(6)).
[5] See PDPA Section 15.
[6] See PDPA Section 17, as well as the Second Schedule, Third Schedule and Fourth Schedule to the PDPA. In particular, the specific exceptions (and the conditions to be met, if any) for the circumstances highlighted are set out in the Second Schedule, paragraphs 1(a), 1(b) and 1(e), Third Schedule, paragraphs 1(a), 1(b), 1(e), and 1(i) and 2, and Fourth Schedule, paragraphs 1(a), 1(b), 1(f), and 1(q) and 4.

3.4 The following sections outline PDPC's considerations and proposed enhancements to the framework for collecting, using and disclosing personal data under the PDPA.

Notification of Purpose

3.5 The requirement for consent has typically been coupled with the requirement to notify, as there cannot be informed consent without notifying the individual of the purpose for the collection, use or disclosure of personal data for which consent is sought. Nonetheless, notification can still be appropriate in the absence of consent-taking.

3.6 Several jurisdictions permit the collection of personal data with notification of purpose in the absence of consent, as a way of ensuring individuals retain some measure of control. For instance, Australia's Privacy Act 1988 is primarily a notification based regime, and consent is required in limited circumstances. Generally, the organisation must notify the individual of the purposes of collecting his personal information and the consequences if the information is not collected, amongst other things[7]. Under British Columbia's Personal Information Protection Act, organisations may collect, use or disclose personal information where reasonable having regard to the sensitivity of the personal information in the circumstances, if they notify the individual of the purposes of the intended collection, use or disclosure with reasonable opportunity for the individual to decline[8]. Similarly, New Zealand's Privacy Act 1993 permits collection of personal data with notification and does not specifically require that consent be obtained from the individual. The individual must similarly be notified of the purpose for which the information is being collected and the consequences for the individual if the information is not collected, amongst others[9].

3.7 Another example is Japan's Act on the Protection of Personal Information, which provides that having acquired personal information, a business is to notify individuals, or publicly announce, the purposes for using the personal information ("Purpose of Use"); consent is required in limited circumstances, such as where the personal information is to be used beyond the scope necessary to achieve the Purpose of Use, where the personal information is to be disclosed to third parties or in respect of sensitive information[10].

[7] See Australia's Privacy Act 1988, Schedule 1, Part 2. The Australia Privacy Act 1988 also appears to generally require organisations to collect personal information directly from the individual concerned.
[8] See British Columbia's Personal Information Protection Act, Section 8(3). Organisations must provide individuals reasonable time to decline and may collect, use or disclose the personal information if the individuals do not decline.
[9] See New Zealand's Privacy Act 1993, Principles 2 and 3. The New Zealand Privacy Act 1993 also appears to generally require organisations to collect personal information directly from the individual concerned.
[10] See Japan's Act on the Protection of Personal Information, Article 18.

3.8 PDPC considers 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. Notification provides a way of ensuring individuals retain some measure of control over their personal data in such circumstances. 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 on the individuals**. This includes ensuring the personal data will not be used to make a decision about the individual that may have an adverse impact on the individual, or to circumvent a prior withdrawal of consent (e.g. target the individual for direct marketing after he had opted out of receiving marketing communications).

3.9 PDPC proposes for organisations that wish to rely on this approach to provide **appropriate notification**[11] 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.

3.10 PDPC also proposes that organisations must assess if there are any risks or impact to the individuals from the collection, use or disclosure of personal data. Organisations will therefore be required to conduct a **risk and impact assessment**, such as a data protection impact assessment ("DPIA"), and put in place measures to mitigate the risks when relying on Notification of Purpose to collect, use or disclose personal data.

3.11 An example of a situation where the proposed Notification of Purpose approach could be appropriate is where an organisation does not have the contact information of its customers but wishes to use its customers' personal data for a new purpose of conducting analytics to develop new products and services. Another example is where organisations wish to deploy recording devices or drones in high traffic situations that are likely to capture personal data. The proposed approach will allow organisations to provide appropriate notification of the purposes without obtaining

[11] Notification could be one-to-one from the organisation to the individual, or one-to-many from the organisation to a group of individuals (e.g. signage at the location where personal data is collected).

consent from the individuals, while ensuring greater protection for individuals by requiring that organisations must assess the risks and impact to the individuals, and implement the necessary measures to mitigate such risks when doing so.

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

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)?

Legal or Business Purpose

3.12 The EU Directive[12], as well as the new EU General Data Protection Regulation ("GDPR")[13], provide for a "legitimate interests" basis for processing personal data. The "legitimate interests" condition weighs the individual's fundamental rights to personal data protection against possible legitimate interests of the organisation, including enforcing a legal claim, preventing fraud, monitoring employees for safety or management purposes, and conducting scientific research[14]. Republic of Korea's Personal Information Protection Act also permits the collection and use of personal data where it is necessary to realise the legitimate interests of the organisation and it obviously takes precedence over the rights of the individual[15].

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[16]. 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[17], to recover a debt[18], or for a research purpose[19]. The PDPA also

[12] Directive 95/46/EC of the European Parliament and the Council of 24 October 1995.
[13] 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.
[14] Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC (Article 29 Data Protection Working Party, 9 April 2014) at Annex 2.
[15] See Republic of Korea's Personal Information Protection Act, Article 15(1)(6). Retrieved from http://law.go.kr/engLsSc.do?menuId=0&subMenu=5&query=%EA%B0%9C%EC%9D%B8%EC%A0%95%EB%B3%B4%EB%B3%B4%ED%98%B8%EB%B2%95#AJAX.
[16] See PDPA Section 3.
[17] See PDPA Second Schedule paragraph 1(e), Third Schedule paragraph 1(e) and Fourth Schedule paragraph 1(f).
[18] See PDPA Second Schedule paragraph 1(i), Third Schedule paragraph 1(g) and Fourth Schedule paragraph 1(i).
[19] See PDPA Third Schedule paragraphs 1(i) and 2, and Fourth Schedule paragraphs 1(q) and 4.

provides for the retention of personal data where necessary for a business or legal purpose[20], and for the transfer of personal data out of Singapore for certain legal and business purposes prescribed in the Personal Data Protection Regulations 2014[21].

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

3.15 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**.

3.16 An example of a situation where collection, use or disclosure of personal data without consent and notification for a Legal or Business Purpose could be allowed is where a group of organisations in a particular sector needs to share information and analyse personal data of customers in order to identify and prevent potential fraudulent activities.

3.17 As a safeguard for individuals, PDPC proposes for organisations that wish to collect, use or disclose personal data without consent and notification for a Legal or Business Purpose, to undertake measures to identify and minimise the risks to the individual from the collection, use or disclosure of personal data. In this regard, a **risk and impact assessment**, such as a DPIA, will need to be conducted to assess the risks and impact of the intended collection, use or disclosure of personal data to the individual.

[20] See PDPA Section 25.
[21] See Personal Data Protection Regulations 2014, Regulations 9 and 10.

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?

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)?

PART III: MANDATORY DATA BREACH NOTIFICATION

4 Overview of Current Regime

4.1 The PDPA requires that organisations make reasonable security arrangements to protect personal data in their possession or under their control[22]. However, there is no mandatory requirement to notify any party when a data breach[23] has occurred. Organisations are encouraged to notify the PDPC as soon as possible of any data breaches that might cause public concern or where there is a risk of harm to a group of affected individuals[24].

4.2 The current voluntary approach to notification has resulted in uneven notification practices across organisations. Some organisations may decide to notify the affected individuals and the PDPC, while others may decide not to notify any party in a similar data breach incident. In some situations, organisations deciding not to notify affected individuals of a data breach may leave them vulnerable to the risk of harm when they remain unaware that their personal data has been compromised and do not take steps to protect themselves.

4.3 Internationally, jurisdictions that have or are looking to introduce mandatory data breach notification in legislation include Australia[25], Canada[26], New Zealand[27], the EU[28], the UK[29] and the US[30].

4.4 While the specific features of mandatory data breach notification models vary across jurisdictions (e.g. the trigger for notification, content of notification, exceptions and exemptions), the need to notify individuals at risk as soon as possible is evident in all. For example, Australia recently passed legislation that will require organisations to

---

[22] See PDPA Section 24.

[23] A data breach refers to the unauthorised access, collection, use, disclosure, copying, modification, disposal of personal data or similar risks.

[24] Please refer to PDPC's Guide to Managing Data Breaches.

[25] The Privacy Amendment (Notifiable Data Breaches) Act 2017 was passed by the Australian Senate in February 2017 and will by and large take effect one year after the bill receives Royal Assent.

[26] Canada passed the Digital Privacy Act in June 2015 that includes provisions on breach reporting (these provisions are to come into force on a day to be fixed by order of the Governor in Council). Currently, Alberta is the only province to have mandatory data breach reporting for all private sector organisations as provided for under the Personal Information Protection Act ("PIPA"). Retrieved from http://www.qp.alberta.ca/1266.cfm?page=P06P5.cfm&leg_type=Acts&isbncln=9780779762507.

[27] In 2011, the New Zealand Law Commission recommended mandatory reporting in its privacy law review, and a Cabinet Paper released in 2014 largely agreed with that recommendation. Retrieved from http://www.lawcom.govt.nz/our-projects/privacy?id=907.

[28] See EU GDPR, Articles 33 and 34.

[29] See UK's Privacy and Electronic Communications (EC Directive) Regulations 2003.

[30] Majority of US states have had legislative data breach reporting requirements. At the federal level, the most recent proposal for a nationwide mandatory breach notification is the proposed Personal Data Notification and Protection Act (H.R. 1704). Retrieved from https://iapp.org/resources/proposed-personal-data-notification-and-protection-act/ and https://www.congress.gov/bill/114th-congress/house-bill/1704.

notify individuals as soon as practicable when there are sufficient grounds to believe that the data breach is likely to result in serious harm to the individual. Under the forthcoming EU GDPR, Article 33 requires organisations to inform the supervisory authority without undue delay and, where feasible, not later than 72 hours after becoming aware of the breach, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Further, in the event of a personal data breach where the breach is likely to result in a high risk to the rights and freedoms of individuals, Article 34 of the EU GDPR requires the organisation to communicate the breach to the individual without undue delay.

4.5 Under the UK's Privacy and Electronic Communications (EC Directive) Regulations 2003 ("PECR"), service providers are required to notify the Information Commissioner's Office ("ICO") if a personal data breach occurs within 24 hours of detection. In cases where it is not feasible to provide the ICO with the full details within 24 hours, the initial notification must still be given within 24 hours, and a second notification is then to be sent within three days of the initial notification to provide further information[31]. Further, if the breach is likely to adversely affect the personal data of the service provider's subscribers or users, it is mandatory for service providers to notify the affected individual without undue delay.

5 Need for Mandatory Data Breach Notification

5.1 With Singapore's Smart Nation initiative and push towards a Digital Economy, personal data will increasingly be capitalised to deliver more innovative services and improve lives. This, however, brings with it heightened risks and impact of data breaches for individuals. Gemalto, a digital security organisation, reported that compared to 2015, 2016 saw a 86% increase in data records lost or stolen worldwide[32]. Identity theft was the leading type of data breach since Gemalto started tracking breach incidents in 2013.

5.2 To strengthen protection for individuals and build confidence in organisations' management and protection of personal data, PDPC is proposing to introduce a mandatory data breach notification regime under the PDPA.

5.3 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

[31] ICO's guidance on Notification of PECR security breaches (19 March 2015) ("ICO's PECR guidance"), retrieved from https://ico.org.uk/media/for-organisations/documents/1583/notification-of-pecr-security-breaches.pdf.

[32] The Gemalto Breach Level Index reported that there were almost 1.4 billion compromised data records in 2016. In comparison, there were 740 million compromised data records in 2015. According to Statista, in the US alone there is a general upward trend of data breaches from 2005 – 2016. Retrieved from http://www.breachlevelindex.com/assets/Breach-Level-Index-Report-2016-Gemalto.pdf and https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/.

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.

6 Proposed Data Breach Notification Framework

6.1 PDPC is mindful not to impose overly onerous regulatory burdens on businesses in Singapore, or to create notification fatigue for individuals. The proposed data breach notification framework also takes into consideration the data breach notification models adopted in overseas jurisdictions and existing local sectoral legislation[33]. Advisory guidelines will be issued to provide further guidance for organisations on complying with the data breach notification requirements.

Criteria for Breach Notification

6.2 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[34]. For instance, a data breach that involves personal data such as NRIC number, health information, financial information or passwords would be considered to pose a risk of impact or harm to the affected individuals. Notifying affected individuals will enable them to take the necessary steps to protect themselves from the risks or impact from the 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[35]. Data breaches of a significant scale could indicate a systemic issue within the organisation, which

[33] Organisations may be subject to other sector-specific rules under laws that require them to complement or further protect personal data. In this regard, Section 4(6) of the PDPA states that unless otherwise provided in the PDPA, the provisions of other written law shall prevail to the extent that any provision of Parts III to VI is inconsistent with the provisions of that other written law.

[34] PDPC will develop and issue guidelines to provide guidance to organisations on assessing risk of impact or harm to affected individuals.

[35] Under California's Civil Code Section 1798.82, an organisation that is required to issue a security breach notification (pursuant to that section) to more than 500 California residents as a result of a single breach of the security system must electronically submit a single sample copy of that security breach notification to the Attorney-General.

may require PDPC's further investigation and guidance to the organisation on implementing the appropriate remedial actions to address it.

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?

Concurrent Application with Other Laws and Sectoral Breach Notification Regimes

6.3 PDPC proposes for the data breach notification requirements under the PDPA to apply concurrently with other notification requirements under other laws and sectoral regulations (e.g. Monetary Authority of Singapore ("MAS") Notices 127 and 644 on Technology Risk Management[36]) in the following manner:

a) where the 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 notifying the PDPC, it is proposed that the organisation shall **notify PDPC concurrently with the sectoral regulator or law enforcement agency in accordance with the notification requirements under the other written law**. In such cases, the organisation may submit to the PDPC the same notification or copy the PDPC in its notification to the sectoral or law enforcement agency. This is to minimise the effort and cost involved to comply with notification requirements for the same data breach, while allowing PDPC to continue to be kept informed of data breaches of potential concern; and

b) where the organisation is required to notify affected individuals under other written law, and that data breach meets the criteria for notifying affected individuals under the PDPA, PDPC proposes that the organisation be considered to have fulfilled its breach notification obligations under the PDPA if it notifies the affected individuals according to the requirements under the other written law. The organisation in such a situation must also notify the PDPC of that data breach.

6.4 Where the organisation is not required to notify the sectoral or law enforcement agency and/or affected individuals under other written law, and that data breach meets the criteria for notifying the PDPC and/or affected individuals under the PDPA,

[36] Notice 127, issued pursuant to Section 64(2) of the Insurance Act, applies to all licenced insurers, other than captive insurers and marine mutual insurers. Notice 644, issued pursuant to Section 55 of the Banking Act, applies to all banks in Singapore.

the organisation must notify the PDPC and/or affected individuals according to the breach notification requirements under the PDPA.

6.5 For example, banks are required to notify MAS of relevant incidents as defined in MAS Notice 644. In the event that a bank experiences a data breach which meets the definition in MAS Notice 644 and also meets the criteria for notifying the PDPC and affected individuals under the PDPA, the bank would have to notify MAS and the PDPC, and to notify the affected individuals according to the breach notification requirements under the PDPA.

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?

Obligations of Data Intermediary

6.6 Where the organisation's data intermediary ("DI")[37] experiences a data breach, PDPC proposes that **the DI be required to immediately inform the organisation** that it processes the personal data on behalf and for the purposes of, regardless of the risk of harm or scale of impact of the data breach. The organisation will be responsible[38] for complying with the breach notification requirements under the PDPA.

6.7 The proposed requirement for the DI to immediately inform the organisation is necessary for the organisation to undertake expedient assessments to determine whether the data breach meets the criteria for breach notifications under the PDPA and any other law, as well as to take timely remedial actions to mitigate any risks of harm arising from the data breach.

6.8 PDPC highlights that organisations may also need to comply with requirements under other laws to notify third parties (e.g. banks) of the data breach. Where it is not required under other laws, the organisation would need to consider any relevant sectoral restrictions[39] as well as the PDPA obligations and exceptions[40], if it wishes to disclose personal data to these parties.

[37] "Data intermediary" means an organisation which processes personal data on behalf of another organisation but does not include an employee of that other organisation.
[38] This position is similar to that under the EU GDPR. Under Article 33 of the EU GDPR, processors are to notify the data controllers "without undue delay" after becoming aware of a personal data breach, and controllers are to notify the supervisory authority.
[39] Such as confidentiality obligations.
[40] Disclosure of personal data without consent under the Fourth Schedule to the PDPA.

Exceptions and Exemptions from Breach Notification

6.9 PDPC proposes for the exclusions under Section 4 of the PDPA to apply to the proposed breach notification provisions under the PDPA, 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 PDPA. For instance, where other written law prohibit notification, the provisions of other written law shall prevail to the extent that the breach notification provisions are inconsistent with the provisions of other written law.

6.10 In addition, it is proposed that the following exceptions to the requirement **to notify affected individuals** be provided:

a) law-enforcement exception, where notification to affected individuals is likely to impede law enforcement investigations[41]; and

b) technological protection exception[42], where the breached personal data is encrypted to a reasonable standard.

6.11 The Commissioner, with the approval of the Minister, may also exempt organisations from the breach notification requirements to cater to exceptional circumstances where notification to affected individuals may not be desirable and the PDPA or other laws do not provide for.

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

Time Frame for Breach Notification

6.12 Where a data breach meets the criteria for notifying affected individuals under the PDPA, PDPC proposes to require that the organisation **notifies all affected individuals as soon as practicable**, unless an exception or exemption applies. The proposed notification time frame of 'as soon as practicable' is intended to allow affected individuals the opportunity to take timely remedial actions to mitigate

[41] Under this exception, the law enforcement agency may direct the organisation not to notify affected individuals because it may impede investigations.

[42] The EU GDPR has a similar exception. Article 34(3) of the EU GDPR provides that notification to an individual is not required where 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".

potential risk of harm or loss arising from the data breach. In view of the variability of data breach circumstances, PDPC proposes not to impose a time cap for breach notifications to all affected individuals, and organisations are to determine what is 'as soon as practicable' in the given circumstances. The organisation in such a situation must also ensure it notifies the PDPC of that data breach within the time frame discussed in the following paragraph.

6.13 Where a data breach meets the criteria for notifying PDPC under the PDPA, PDPC proposes to require that the organisation **notifies the PDPC as soon as practicable, no later than 72 hours from the time it is aware of the data breach**. For breach notifications to PDPC, prescribing a cap of 72 hours [43] provides clarity for organisations as to the definitive time by which they would have to notify PDPC, and they may provide the PDPC with relevant information that is available to the organisation at the time of notification. In addition, if that data breach also meets the criteria for notifying affected individuals under the PDPA, the organisation must ensure it notifies the affected individuals as soon as practicable.

6.14 The proposed time frames for breach notifications to affected individuals and to PDPC are similar to what are prescribed under the forthcoming EU GDPR, and comparable with UK's PECR for service providers, as highlighted in paragraph 4.5.

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

Mode of Breach Notification

6.15 PDPC does not intend to prescribe the mode of notification to PDPC and affected individuals. PDPC recognises that there are many different modes of notification that could evolve with technology, and organisations should be allowed to determine the most efficient and expedient [44] mode of notification to comply with the breach notification requirement to inform affected individuals as soon as practicable so that they may take actions to mitigate the potential risk of harm or loss from the breach[45].

6.16 PDPC will issue advisory guidelines to provide guidance for organisations on complying with the data breach notification requirements when introduced,

[43] In certain cases, an organisation may require more than 72 hours to confirm the breach and obtain the necessary details of the incident. In such a scenario, the organisation should still notify PDPC with as much information as possible within the 72 hours and provide PDPC with the remaining information as soon as possible.
[44] For example, an online notification posted on the organisation's website.
[45] The EU GDPR provides that organisations may communicate the personal data breach to the affected individual via public communications if it would involve disproportionate effort to do so otherwise. In adhering to UK's PECR, ICO's PECR guidance states that the means of communication should be a specific message about the data breach and not be combined with communications on another topic.

including the considerations for assessing whether data breaches meet the criteria for notification, the time frames and the types of information to be included in breach notifications to affected individuals and to PDPC.

PART IV: SUBMISSION OF COMMENTS

7.1 Parties that wish to submit comments on this public consultation paper should organise their submissions as follows:

a) cover page (including particulars of the organisation and contact person);

b) comments, with reference to specific sections or paragraphs if appropriate; and

c) conclusion.

7.2 Supporting material may be placed in an annex. All submissions should be clearly and concisely written, and should provide a reasoned explanation for any comments. Where feasible, parties should identify the specific section on which they are commenting and explain the basis for their proposals.

7.3 All submissions should reach PDPC by **5 October 2017**. Comments should be submitted:

a) in soft copy (in Microsoft Word format);

b) to the following e-mail address: corporate@pdpc.gov.sg; and

c) with the email header: "PDPC's Public Consultation on Approaches to Managing Personal Data in the Digital Economy".

7.4 The PDPC reserves the right to make public all or parts of any written submission and to disclose the identity of the source. Commenting parties may request confidential treatment for any part of the submission that the commenting party believes to be proprietary, confidential or commercially sensitive. Any such information should be clearly marked and placed in a separate annex. If the PDPC grants confidential treatment it will consider, but will not publicly disclose, the information. If the PDPC rejects the request for confidential treatment, it will return the information to the party that submitted it and will not consider this information as part of its review. As far as possible, parties should limit any request for confidential treatment of information submitted. The PDPC will not accept any submission that requests confidential treatment of all, or a substantial part, of the submission.

END OF DOCUMENT