Consultation Paper on the Proposed Approaches to Managing Personal Data in the Digital Economy

Feedback on the proposed amendments to the PDPA as issued by the PDPC

KPMG Services Pte Ltd

21 September 2017

Contents

1 Executive Summary 2

2 Answer to the Enhanced Framework for Collection, Use and Disclosure of Personal Data 3

2.1 Consent and the purpose of the PDPA 3

2.2 Challenges for Consent 4

2.2.1 Internet of Things and Artificial Intelligence 5

2.2.2 Fraud and security threats 6

2.2.3 Drones and recording devices 7

2.2.4 Other data protection regulations 8

2.3 Notification of Purpose 9

2.3.1 Not practical to obtain consent 10

2.3.2 No adverse impact on individuals 11

2.3.3 The right to information and consent 11

2.3.4 No specification for notification 11

2.4 Legal or Business Purpose without consent, nor notification 12

3 Answer to the Mandatory Data Breach Notification 13

3.1 Data Breach Notification to the PDPC 13

3.1.1 Criteria to notify the PDPC 13

3.1.2 Platform to notify the PDPC 14

3.1.3 Exception to the notification 14

3.1.4 Timeline to notify the PDPC 15

3.1.5 Content of the notification 16

3.1.6 Notification in breach with other regulations 17

1 Executive Summary

KPMG Singapore ("KPMG") is pleased to provide feedback on the proposed amendments to the Personal Data Protection Act (PDPA) as issued by the Personal Data Protection Commission (PDPC). Our review and feedback is based on KPMG's experience of conducting PDPA engagements in Singapore and with similar legislation and regulation in other jurisdictions, where KPMG provides privacy and data protection related services. This document provides our observations based on our review of the proposed changes and specific questions raised in the public consultation paper.

The primary change proposed is that the PDPC indicates a less stringent approach for the consent mechanism by introducing Notification of Purpose and Legal or Business Purpose, as a legitimate basis for the processing of personal data, without the need to obtain explicit consent from the individual.

In our various consultations, we have noted a number of concerns around specific implementations of the provisions of the proposed amendments that are not explicitly addressed in the consultation paper. The key concerns are in the areas of respect for the right to privacy of individuals. Also, we found that the proposed "opt-out" approach differs from the current "spirit of the law", the best practices and trends perceived in other national privacy, and data protection legislations which advocate stringent consent regimes.

KPMG fully supports the PDPC's proposal to introduce a mandatory data breach notification scheme. This requirement is found in many progressive privacy and data protection regulations, and will raise awareness regarding data breaches thereby enabling organisations to enhance their practices based on hard lessons learned.

2 Answer to the Enhanced Framework for Collection, Use and Disclosure of Personal Data

2.1 Consent and the purpose of the PDPA

Privacy, and implicitly the protection of personal data, is recognised as a fundamental human right.[1] Activities that restrict the right to privacy, can only be justified when they are prescribed by law, necessary to achieve a legitimate aim, and proportionate to the aim pursued.[2] The PDPA recognises this fundamental right as its dual purpose is "to govern the collection, use and disclosure of personal data by organisations in a manner that recognises both the right of individuals to protect their personal data and the need of organisations to collect, use or disclose personal data for [appropriate] purposes […]."[3]

Consent is perceived as a key element in the protection of privacy and data protection, in both jurisprudence and legal instruments[4]: Consent enables the individual to allow or restrict the processing of personal data to conform their own values and preferences. Under the current PDPA, we see that consent has a prominent position, indicating that the PDPC is focussed on addressing the concerns of individuals and maintaining individuals' trust in organisations that manage their data.

The PDPA does not specifically confer any property or ownership rights on personal data *per se* to individuals or organisations. This also does not affect existing property

[1] Article 12, Universal Declaration of Human Rights.
[2] Article 29, Universal Declaration of Human Rights; General Comment No. 27, Adopted by The Human Rights Committee Under Article 40, Paragraph 4, Of The International Covenant On Civil And Political Rights, CCPR/C/21/Rev.1/Add.9, November 2, 1999.
[3] Article 3, Personal Data Protection Act 2012.
[4]Article 8 in the Charter of Fundamental Rights of the European Union defines the right of Protection of personal data as: "everyone has the right to the protection of personal data concerning him or her. Such data must be processed […] on the basis of the consent of the person concerned […]."

rights in items in which personal data may be captured or stored.[5] However, the concept of consent can be defined in terms of ownership. Where a regulatory law such as PDPA prioritises the rights of individuals, the ownership of personal data is intrinsic. This should translate to a stringent consent regime, where the individual has to "opt-in" before organisations can process their personal data. This is now the case in EU.[6] However, if the PDPA focuses instead on facilitating the processing of personal data by organisations, the ownership of personal data becomes extrinsic, resulting in a relaxed consent regime; i.e. organisations will not need to obtain consent before processing personal data. In this circumstance the onus is on the individual to opt-out. This makes the potentially erroneous assumption that all citizens are aware and vigilant in defending their liberties.

Consideration should be given to the precarious balance between the interests of private individuals and organisations. With the proposed changes to the PDPA, it would seem that the focus of the PDPC has shifted to the facilitation of data processing by organisations. Consequently, the protection of individuals' right to data protection can deteriorate significantly due to the loss of control on how and for which purposes their personal data will be processed. It is important to recognise that a change in the consent regime can derogate from the initial spirit of the law, and can detract from Singapore's determination to respect the Human Right to Privacy.

2.2 Challenges for Consent

The PDPC highlights multiple challenges for the consent obligation. These examples are used to justify less stringent consent requirements in contrast to the more stringent consent requirements currently set in the PDPA. In the next sections, KPMG provides observation on how these challenges can be addressed without changing the current "opt-in" consent regime defined in the current version of the PDPA.

[5] Section 5.28, Advisory Guidelines on Key Concepts in the Personal Data Protection Act, Issued By The Personal Data Protection Commission, Issued 23 September 2013, as revised on 16 May 2014.
[6] The European General Data Protection Regulation (GDPR) prioritises the rights and freedoms of individuals to the interests of organisations: every act of processing that is not based on consent, have to be weighed against the fundamental rights of individuals.

2.2.1 Internet of Things and Artificial Intelligence

The PDPC states that it might not be possible to anticipate the purposes for using and disclosing personal data at the outset when this is related to Internet of Things (IoT) and Artificial Intelligence (AI). For this reason, the PDPC suggests that the conditions for consent should be less stringent. IoT is the inter-networking of an item with the embedded electronics, software, sensors, actuators, and network connectivity which enable these objects to collect and exchange data. The PDPA only has pertinence in relationship to IoT if the IoT device is used to process personal data of the individual. In case the use of IoT has an aspect related to the processing of personal data, then applying the consent principle will not be different from other data protection processing activities without the use of IoT.

Artificial Intelligence (AI), also called "machine learning", is the use of algorithms to self-improve other processes with minimised human intervention. AI is used to analyse big data[7] in a manner that does not differ significantly from standard methods of data analysis. Traditionally, the analysis of a dataset involves constructing a query to find the subject of the analysis, by identifying the relevant data. Big data analytics through AI, on the other hand, typically does not start with a predefined query to test a particular hypothesis; it often involves a 'discovery phase' of running algorithms against the data to find correlations. The entry and exit of personal information, processed through the use of AI, can still be subject to consent, as the purpose is defined upon the retrieval of the personal data of the data subject. In the intrinsic interpretation of the PDPA, the rights of individuals have a central position. An "opt-in" consent regime, will ensure that the individual still has the power to determine whether, how and for what purpose its personal data is processed through the use of AI. Based on specific categorisation of the personal data, personal data can be restricted from being processed in a way that deviates from the specific consent.

[7] "[…] high-volume, high-velocity and high-variety information assets that demand cost-effective, innovative forms of information processing for enhanced insight and decision making", Gartner IT glossary Big data. http://www.gartner.com/it-glossary/big-data, Accessed 20 September 2017.

Industry and academic based initiatives are addressing ethics and data protection in Artificial Intelligence. One example of this is the paper of the UK's Information Commissioner's Office (ICO) on big data and data protection.[8] The ICO argues that gaining explicit consent is not impossible in big data analytics. The guide lists examples of where organisations have used novel and innovative approaches to help gain, manage and withdraw consent. Graduated consent, i.e. consent for different uses of their data throughout their relationship with a service provider, is listed as one possible solution to the common issue in big data analytics of experimenting on, and thereby repurposing, data. In sum, data storage and processing, control on the entry of data and on the purpose of data processing through AI is still achievable.

2.2.2 Fraud and security threats

The PDPC mentions circumstances such as fraud detection and security threats as a reason for a less stringent consent mechanism. Consideration should be given that these circumstances already form an exception to the strict interpretation of the PDPA. This is when "the use is necessary in the national interest"; and when "the use is necessary for any investigation or proceedings."[9] In other national privacy legislations, processing of personal data in the context of fraud or security threats is an exception to the consent requirement. One example is the Data Protection Act in the UK. This Act has a number of sections which allow exemptions for certain reasons, such as the prevention and detection of crime and for matters of national security. This allows agencies to access personal data upon the provision of individual authority. Another example can be found in the GDPR, where investigations related to fraud and security threats are allowed on the basis of public interest and therefore, excluded from the consent requirement. Also, the PDPA may be overruled in specific instances by Singapore's future Cybersecurity Act, particularly when cybersecurity threats are investigated.[10]

[8] ICO, 2017, "ICO Big data, artificial intelligence, machine learning and data protection", https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf .
[9] Third Schedule, (d) and (e), PDPA.
[10] This is indicated by Section 20(5) of the proposed Cybersecurity Bill which protects a person who "[…] in good faith, discloses any information to an investigating officer […]." This person "[…] is not

2.2.3 Drones and recording devices

The PDPC gives the example of recording devices or drones to demonstrate the necessity of a less stringent consent regime. It is true that it is not always practical for an organisation to obtain consent. However, there are circumstances where the filming and publishing of the footage without consent may be lawful. Examples may include when the filming from afar so that no one is identifiable. It may also be when the person has consented, such as at a sporting event as part of the ticketing conditions. It may be if there is a public interest in disclosure, for example, filming a terrorist shooting and using the footage for law enforcement or legitimate media reporting purposes. Under European law, the use of a drone will always require a legitimate ground for processing. This legitimate ground can be, amongst others, the unambiguous consent of the individual or the necessity of the processing for the execution of a contract or for compliance with a legal obligation.

In case there is no legitimate ground, drone manufacturers have built in privacy friendly tools, in order to be compliant with the legislation ("Privacy by Design"). At the earliest stages of development of the drone, manufacturers are required to analyse how their device might interfere with the privacy of individuals. Based on these analyses, they will have to implement technologies that counter the processing of personal data. Best practice examples are technologies providing automatic masking of private areas and automatic detection and the pixilation of faces that are (accidentally) gathered in images and videos. Manufacturers also set up data retention by design, that is to say, the possibility to schedule the automatic and regular deletion of the data processed.

Based on these examples and practices, the PDPC might reconsider the necessity of "notification of purpose without consent" as it is redundant. This may give the perception to organisations that the PDPC takes a less stringent view on the fundamental right of individuals to privacy.

---

treated as being in breach of any restriction upon the disclosure of information imposed by law, contract or rules of professional conduct."

2.2.4 Other data protection regulations

In the consultation paper, the PDPC refers to privacy legislation from Australia, New Zealand, Columbia and Japan to show the "opt-out" regime is in vogue in the neighbouring countries. The current PDPA requires the consent for processing of personal data, however this is not as stringent as other legislations (such as the GDPR) because of the extensive exemptions listed in the PDPA, as well as the notion of deemed consent found in Section 15 of the PDPA. Introducing an explicit "opt-out" regime, would make the difference between the PDPA and GDPR legislations even more significant.

Regarding the data protection regulations in neighbouring countries, the following should be considered:

— Canada's Anti-Spam legislation defines a clear "opt-in" regime and exceptions to this rule are limited.

— Australia's regulation requires email marketers to collect permission from the owner of an email address before sending any communication. In addition, the law require email marketers to keep records of the permissions they gain from subscribers. In case of disputes, this information can be used in court, where the burden of proving permission always lies with the sender.

— China, Japan and New Zealand also require explicit consent for the processing of personal data.

Overall, the most recent data protection legislations follow the trend of more stringent "opt-in" consent regimes. However, the proposed amendments to the PDPC are not in line with this trend. For this reason, KPMG advises to reconsider the introduction of a less stringent consent regime.

2.3 Notification of Purpose

The PDPC proposes amendments to the consent regime as formulated in the current PDPA. The first amendment regards "Notification of Purpose". Here, the PDPC proposes that organisations should solely notify individuals, in case they will process their data and where it is impractical to obtain consent.

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

KPMG's Observations: *The PDPC identified multiple challenges for consent to w a less stringent consent regime, such as "Notification in Purpose". KPMG provides observations related to these challenges, that suggest the need to reconsider a less stringent "Notification of Purpose":*

- *Internet of Things and Artificial Intelligence do not justify a less stringent consent regime, as control on the entry of data and purpose of data processing is still achievable.*
- *The processing of personal data in case of fraud and security threats should be treated as an exception, and therefore does not justify a less stringent consent regime.*
- *The difficulties related to consent that are faced by manufacturers of drones and recording devices can be mitigated, and therefore these challenges do not justify an overall less stringent consent regime.*
- *National privacy and data protection regulations world follow the trend of more stringent consent regimes. This trend that is expected to continue.*

Consequently, KPMG recommends to retain the "opt-in" consent regime, as there is no reason for the PDPA to 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)?

KPMG's Observations: *Question 2 will be answered in point 2.3.1 – 2.3.4 of this paper. In short, KPMG advises to keep the "opt-in" regime as the standard, as a less stringent regime might violate the fundamental rights of individuals. In case the PDPC implements the less stringent regime, KPMG encourages greater clarify for the definition and context of cases where it is "impractical" to obtain consent. We agree that a risk and impact assessment should be conducted regarding the absence of an adverse impact as a condition to rely on Notification of Purpose. KPMG recommends a need to provide guidelines for organisations on how and what to notify individuals.*

2.3.1 Not practical to obtain consent

One condition to rely on the Notification of Purpose is the impracticality for the organisation to obtain consent.

KPMG's Observations: *KPMG suggests that the definition and requirements of 'impractical' should be more clearly defined. Also, KPMG recommends that the introduction of an obligation for controllers to document the decision on the situations in which it is impractical to obtain consent should be considerable. This may be also improved by placing the burden of proof on the data controller.*

2.3.2 No adverse impact on individuals

Another condition to rely on Notification of Purpose is the absence of adverse impact on individuals. Organisations must assess the possible risks and impacts on the individual.

KPMG's Observations: *KPMG agrees that organisations must assess the possible risks or impacts on the individual from the processing of personal data. This also requires measures to mitigate these risks. We would like to highlight that an "adverse impact" is subjective and can differ per individual. KPMG recommends to introduce a clearer guideline for this assessment.*

2.3.3 The right to information and consent

The PDPC proposes a regime where the organisation should communicate with the individual about the processing in case when it is impractical to obtain consent.

KPMG's Observations: *This can be perceived as a contradiction: where an organisation can communicate a notification, it might also be possible to communicate to obtain consent.*

2.3.4 No specification for notification

The PDPC does not intend to prescribe how organisations must notify the individuals and what the content is of the notification.

KPMG's Observations: *KPMG is concerned that by not specifying the content of the notification this may disadvantage the impacted individuals. A fundamental principle is the need to inform individuals about their right to object against the processing, in cases where they did not give their consent. This is required in order to provide transparency, and ultimately, ensure the protection of the individual's rights.*

2.4 Legal or Business Purpose without consent, nor notification

Question 3: Should the PDPA provide for legal or Business Purpose as 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)?

The PDPC proposes for organisations to be able to process personal data without individuals' consent nor notification. This is in case where it is not desirable or appropriate to obtain consent and when the benefits to the public outweigh the adverse impact or risk to the individual.

KPMG's Observations: *The wording "not desirable and appropriate" is not sufficiently clear. It creates too much liberty for data processors to interpret this for their own convenience.*

More importantly, consideration should be given for the circumstances, where it is not "desirable or appropriate to obtain consent", already form an exception to the strict interpretation of the PDPA. The privacy and data protection act is overruled by other legislations and regulations in case of threats, identification of fraud and non-compliance with other regulations. Consequently, this amendment may be redundant. See also section 2.2.2 of this paper.

3 Answer to the Mandatory Data Breach Notification

3.1 Data Breach Notification to the PDPC

3.1.1 Criteria to notify the PDPC

The PDPC proposes that the PDPC should be notified when (1) a data breach poses any risk of impact or harm to the affected individuals; or (2) when 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.

Consideration should be given to the need for organisations to have a register of processing activities. Based on this register, an organisation might be better placed to notify the PDPC within 72 hours about a data breach that affects 500+ individuals. This register enables organisations to see which data breach leads to the exposure of which data, and consequently the population affected.

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?

KPMG's Observations: *KPMG supports the proposed criteria for data breach notification to the affected individuals and to the PDPC. Moreover, KPMG recommends consideration to also implement a requirement to notify a data breach where a specific threshold volume of personal data is breached.*

3.1.2 Platform to notify the PDPC

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?

It is the goal of the PDPC to not impose a regulatory burden or to create a notification fatigue. However, the PDPC also explicitly proposes a concurrent data breach notification process, in addition to existing notification requirements. As a result, in case of a breach, an organisation has to notify different regulators, such as MAS, the Commissioner of Cybersecurity (Cybersecurity Bill) and the PDPC.

KPMG's Observations: *Consideration should be given to potential challenges when organisations are required to notify a single incident to multiple regulators (e.g. cybersecurity incidents, that might include data loss, also have to be notified to the Cybersecurity Commissioner as per the Cybersecurity Bill). KPMG recommends consideration of a framework that would provide a single point of notification of relevant incidents or breaches.*

3.1.3 Exception to the notification

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

The PDPC proposes for the exclusions under Section 4 of the PDPA to apply to the proposed breach notification provisions under the PDPA. This implies that the notification requirement does not apply to (a) any individual acting in a personal or domestic capacity; (b) any employee acting in the course of his employment with an organisation; (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; or (d) any other organisations or personal data, or classes of organisations or personal data, prescribed for the purposes of the PDPA.

KPMG's Observations: *KPMG recommends to reconsider the exception for public agencies or private organisations acting on behalf of a public agency as a data breach of government/public agencies might have equal, if not more severe, consequences for individuals.*

The PDPC proposes two additional scenarios in which the data controller does not need to notify the PDPC in case of a data breach: where notification would impede law enforcement investigations and where breached personal data is encrypted to a reasonable standard.

KPMG's Observations: The exception for encrypted information might be problematic: companies do not need to report a data breach in case it is encrypted, regardless of the context and details surrounding the breach, e.g. the encryption key can be stolen along with the personal data.[11]

Also, it is not clear what is meant with "encrypted to a reasonable standard".[12] What constitutes acceptable encryption should be defined more explicitly.

3.1.4 Timeline to notify the PDPC

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

KPMG's Observations: *Consideration should be given to the case in which the organisation relies on a third party for the processing of personal data, and the third party faces a data breach. KPMG recommends that under such scenario a clause should be incorporated, defining that the third party should notify the organisation without undue delay. Consideration should be given to the MAS Technology Risk Management and MAS Outsourcing regulations, which define the obligation for third*

[11] For this reason, California's AB 2828 (Data Breach Notification Law) was updated in 2017. Now it includes the data breach notification for breaches of encrypted personal information of California residents under the following conditions: (1) encrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person; (2) the encryption key (confidential key or process designed to render the data readable) or security credential was, or is reasonably believed to have been, acquired by an unauthorized person, and; (3) there is a reasonable belief that the encryption key or security credential could render that personal information readable or useable.
[12] Hashing might be seen as encryption, depending on how "encryption" is defined.

parties to notify the Financial Institution such that the FI can subsequently notify the regulator within one hour of data breach or a significant security incident.

3.1.5 Content of the notification

The PDPC does not intend to prescribe the mode of notification to PDPC and affected individuals. In other countries, we see that a predefined set of information must be reported to the Authorities.[13]

KPMG's Observations: *Consideration should be given to the need for clarity for organisations in a crisis situation. KPMG recommends the need to regulate organisations with clear guidelines on what information should be included in the notification. The PDPC could align this with the requirements of other regulators, in order to minimise the regulatory burden on organisations.*

The PDPC has stated that the notification to affected individuals will enable these individuals to take necessary steps to protect themselves from the risks or impact from data breach. However, the PDPC does not define to which extent and what information about the breach must be notified to the individuals.

KPMG's Observations: *We recommend consideration of the obligation for organisations to notify impacted individuals about the identity and contact details of the organisations, as well as a description of the data breach and the kind or information concerned. A crucial part of the notification are the recommendations about the specific actions that affected individuals should take in response to the data breach. This is needed to encourage individuals to take sufficient steps to protect themselves from the impact of a data breach.*

[13] Refer to Appendix 1, Ref. nr. 5.a.

3.1.6 Notification in breach with other regulations

The 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 as well as the PDPA obligations and exceptions, if it wishes to disclose personal data to these parties.

KPMG's Observations: Consideration should be given to the fact that the notification of a data breach does not entail the additional disclosure of the breached datasets or information itself.