RESPONSE TO THE PERSONAL DATA PROTECTION COMMISSION'S CONSULTATION PAPER FOR APPROACHES TO MANAGING PERSONAL DATA IN THE DIGITAL ECONOMY

Contact Partner: Lam Chung Nian
d: +65 6416 8271
e: chungnian.lam@wongpartnership.com
WongPartnership LLP
12 Marina Boulevard Level 28
Marina Bay Financial Centre Tower 3
Singapore 018982
www.wongpartnership.com

1. INTRODUCTION

1.1 We wish to thank the Personal Data Protection Commission ("**PDPC**") for the opportunity to comment on the Public Consultation ("**Public Consultation**") for Approaches to Managing Personal Data in the Digital Economy ("**Proposed Approaches**").

1.2 As one of Singapore's largest and leading law firms, with many clients in the public infrastructure, financial services, essential services and technology sectors, we are keen to share our thoughts and concerns in relation to the Public Consultation, as it represents an enhanced framework for collecting, using and disclosing personal data under the Personal Data Protection Act (No. 26 of 2012 of Singapore) ("**PDPA**") in Singapore having an impact on many of our clients.

1.3 In preparing our responses herein, we have had discussions with our clients to understand their concerns and to also validate our thoughts and comments. We are fully supportive of the PDPC's efforts to engage in stakeholder discussions, and would be happy to further discuss or elaborate on any of the points submitted upon.

2. GENERAL COMMENTS

2.1 We agree that in light of the emerging digital economy, 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.

2.2 As such, the introduction of the Proposed Approaches will allow the regulatory environment to keep pace with evolving technology, while providing for effective protection for individuals' personal data in the changing landscape.

2.3 At the same time, following a review of the Proposed Approaches and the questions in the Public Consultation, we would highlight a number of general concerns which merit further deliberation and consideration:

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

Yes, providing for a Notification of Purpose approach as a basis is a move in the right direction in light of the emerging digital economy. This will facilitate innovation and provide companies with flexibility to engage in data analytics and machine learning.

However, the present proposals do not go far enough in giving companies latitude in mining their data.

For instance, we note the PDPC's Guide to Data Sharing (published 27 July 2017) ("**Guide to Data Sharing**") recognises the sharing of anonymised data to be legitimate, but anonymised data may not be sufficient to obtain accurate insights into consumer behaviour. Greater ability to harness customer data is required to allow for organisations to gain deeper insights into relevant products/services.

Very often, a large sample size is required for data analytics, and there may be difficulties with obtaining and maintaining consent from such a large group of individuals in an efficient manner.

While we recognise the importance of data protection, this should be balanced against the fact that having an overly prescriptive or restrictive data protection framework can potentially stand in the way of making headway in a global market.

(b) 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)?

Based on the current proposal, organisations must, amongst other things, satisfy the relevant conditions and conduct a risk and impact assessment (e.g. data protection impact assessment ("**DPIA**")).

The concern is that it may be too onerous for organisations to fulfil the conditions and carry out the DPIA, to the extent that the amount of work involved is comparable to that of obtaining consents from the data subjects, thereby undermining the intent to introduce the proposed Notification of Purpose approach as an alternative to the consent approach in certain specified circumstances. For example, if an organisation has already carried out a DPIA, then the organisation should be allowed to rely on the proposed Notification of Purpose approach without the need for further conditions.

Even if the proposed Notification of Purpose approach is to be subject to, amongst other things, conditions and the requirement for DPIA, there should be further clarity on the scope and application of such conditions and requirement, as further discussed below.

(i) When it is "impractical" to obtain consent is unclear. In paragraph 3.11 of the Public Consultation, the PDPC cites the example of a situation 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.

In relation to when obtaining consent is impractical, we note that the PDPC provided the following example in its Guide to Data Sharing: organisation does not have individuals' contact information or accurate contact information; or burden or cost of seeking consent is unreasonable to the organisation or disproportionate to the individual's interest. Will the example in the Guide to Data Sharing apply in determining when it is "impractical" to obtain consent for the proposed Notification of Purpose approach?

It is submitted that there should be greater clarity as to when it is "impractical" to obtain consent.

There is also considerable overlap with the existing research exception under e.g. Paragraph 2 of the Third Schedule of the PDPA. Under that exception, it must be shown that:

(A) the research purpose cannot reasonably be accomplished unless the personal data is provided in an individually identifiable form;

(B) it is impracticable for the organisation to seek the consent of the individual for the use;

(C) the personal data will not be used to contact persons to ask them to participate in the research; and

(D) linkage of the personal data to other information is not harmful to the individuals identified by the personal data and the benefits to be derived from the linkage are clearly in the public interest.

This exception has proven difficult to apply in practice, given the various conditions to be met.

The present proposal seems to re-introduce many of the same requirements, which may then also render the exception difficult to apply in practice. Against this, therefore, the new proposal does not appear to go far enough in addressing the existing difficulties posed by this research exception, and the conditions for the proposed Notification of Purpose approach should be relaxed (as further discussed below).

(ii) What will constitute "adverse impact" to an individual is unclear. We note that in the Public Consultation, the PDPC provides the example of targeting the individual for direct marketing after he had opted out of receiving marketing communications. This appears to be a narrow example which makes it difficult to understand the sort of "adverse impact" the PDPC has in mind.

It would be helpful if there is greater clarity as to what constitutes "adverse impact to an individual" and the factors to be taken into account when making such an assessment. For example, does "adverse impact" necessarily involve reasonably foreseeable harm or loss to the individual?

(iii) In paragraph 3.9 of the Public Consultation, the PDPC proposes that organisations wishing to rely on the proposed Notification of Purpose approach shall provide appropriate notification of the purpose of the collection, use or disclosure of the personal data.

What will constitute "appropriate notification" is unclear. It is noted that the Public Consultation states that the 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.

In particular, it is very likely that organisations may not have the contact information of the data subjects when seeking to rely on the proposed Notification of Purpose Approach. In the circumstances, while there is no need for PDPC to prescribe how organisations are to notify individuals, it would be helpful for PDPC to provide guidance on the means of notification that it regards to be acceptable.

(iv) In paragraph 3.10 of the Public Consultation, the PDPC proposes that organisations must conduct a risk and impact assessment, such as a DPIA, and put in place measures to mitigate the risk when relying on the proposed Notification of Purpose approach.

Given that the protection for individuals are ensured by requiring that organisations conduct a DPIA and implement risk mitigation measures, we are of the view that the proposed Notification of Purpose approach should not be subject to further conditions -- i.e., organisations should be allowed to self-assess, following the conduct of the DPIA, that there will not be an adverse impact on the individual, and this can then obviate the need for the impracticality assessment.

(v) As an alternative to subjecting the proposed Notification of Purpose approach to conditions, we propose that the PDPC lists circumstances in which an organisation may rely on the proposed Notification of Purpose approach. This

would be similar to the Second Schedule, Third Schedule and Fourth Schedule of the PDPA, which list the circumstances in which an organisation may collect, use or disclose personal data about an individual, without the consent of the individual.

By having prescribed circumstances, organisations will not need to consider if they have met the proposed conditions (i.e., impractical to obtain consent and not expected to have any adverse impact on the individual), and will be able to easily ascertain if they are able to rely on the proposed Notification of Purpose approach. It would then be left to organisations to prove that they have met the prescribed circumstances when they are challenged by an individual.

(vi) The PDPC did not define what the DPIA must contain. The EU General Data Protection Regulation ("**GDPR**") provides for a DPIA concept, in particular, Article 35(7) lists the minimum requirements of a DPIA. The assessment must contain at least:

(A) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;

(B) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;

(C) an assessment of the risks to the rights and freedoms of data subjects; and

(D) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with the GDPR taking into account the rights and legitimate interests of data subjects and other persons concerned.

Further, the EU Article 29 Data Protection Working Party ("**Art 29 Working Party**") proposes various detailed criteria which data controllers can use to assess whether or not a DPIA, or a methodology to carry out a DPIA, is sufficiently comprehensive to comply with the GDPR.

In practice, this results in a DPIA document which runs into many pages and will be costly to carry out, with the effect that the proposal will then be seldom invoked or underutilised.

We would be grateful if the PDPC could define what the DPIA must contain, and also identify a set of common criteria (which is not excessive in its requirements) that organisations can use to show that their DPIA meets the standards required by the PDPC.

(c) 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?

In paragraph 3.15 of the Public Consultation, the 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. What is "necessary" for a business or legal purpose may require further clarification.

We propose that there be greater clarity on what is regarded to be "necessary" for a "business or legal purpose", as well as guidance on the scope of such "business or legal purpose". Further and/or alternatively, the PDPC can consider listing circumstances or specified purposes corresponding to the "business or legal purpose" under which organisations may rely on the proposed Legal or Business Purpose approach, similar to the current approach for statutory exceptions.

(d) 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 general concern is that it may be too onerous for organisations to fulfil the conditions and carry out the DPIA, in order to rely on this approach. For example, if an organisation has already carried out the DPIA, then the organisation should be allowed to rely on the proposed Legal or Business Purpose approach without the need for further conditions.

Even if it is to be subject to conditions, our comments on the conditions are discussed below.

(i) The threshold for desirability or appropriateness to obtain consent from the individual for the proposed Legal or Business Purpose approach is unclear. We note that in the bicycle sharing app example cited by the PDPC in the Guide to Data Sharing, obtaining consent from customers for the purpose of sharing personal data of identified customers with a track record of misusing, damaging or irresponsibly parking the bicycles was determined to be undesirable and inappropriate. Will the bicycle sharing app example apply in determining when it is "not desirable or appropriate" for the proposed Legal or Business Purpose approach?

We would be grateful that the PDPC provides more clarity on what the threshold for desirability or appropriateness is.

(ii) What sort of "benefits" to the public (or a section thereof) which will "clearly" outweigh any "adverse impact or risks" to the individual is unclear. We note that in paragraph 3.16 of the Public Consultation, the PDPC provided the example of a group of organisations in a particular sector needing to share information and analyse personal data of customers in order to identify and prevent potential fraudulent activities. This appears to be a narrow example which makes it difficult to understand the sort of "benefits" which will "clearly" outweigh any "adverse impact or risks" to the individual.

We would be grateful that the PDPC provides more clarity on the sort of "benefits" which will "clearly" outweigh any "adverse impact or risks" to the individual.

(iii) Similar to our comment in paragraph (b)(v) above, as an alternative to subjecting the proposed Legal or Business Purpose approach to conditions, we propose that the PDPC lists the circumstances in which an organisation may rely on the proposed Legal or Business Purpose approach.

By having prescribed circumstances, organisations will then have a clear set of criteria and will be able to easily ascertain if they are able to rely on the proposed Legal or Business Purpose approach. It would then be left to

organisations to prove that they have met the prescribed circumstances when they are challenged by an individual.

(iv) We note that in paragraph 3.17 of the Public Consultation, the PDPC proposes for organisations that wish to collect, use or disclose personal data without consent and notification for a Legal or Business Purpose to conduct a DPIA.

We are concerned that this requirement will impose an onerous burden on organisations. In fact, we note that this requirement exceeds the threshold under the GDPR. In the GDPR, the requirement for data impact assessments is limited to high risk processing, i.e. where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (Article 35(1) of the GDPR). As such, DPIAs are required in the following cases:

(A) if the processing is being carried out using new technologies;

(B) if the processing prevents data subjects from exercising a right or using a contract or service;

(C) if the processing is carried out systematically on a large scale, for example, where there is a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;

(D) if there is processing on a large scale of sensitive data;

(E) if there is processing on a large scale of criminal offences data; or

(F) if there is a systematic monitoring of a publicly accessible area on a large scale.

We are of the view that organisations should not be required to conduct a DPIA when relying on the proposed Legal or Business Purpose approach. Further, a Legal or Business Purpose is arguably a legitimate purpose and organisations should not need to conduct a DPIA in such circumstances.

(e) <u>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?</u>

(i) We agree that the mandatory data breach notification can safeguard the interests of individuals and allow for them to be aware of data breach incidents. However, litigation risk from customers may increase as a result of the mandatory data breach notification requirement and can have a negative effect on transaction costs.

(ii) We note that one of the proposed criteria is that organisations must notify affected individuals and the PDPC of a data breach that poses any risk of impact or harm to affected individuals. We are of the view that "any risk" is too low a threshold, which may cause undue alarm. As such, a real or reasonable

risk of harm to the affected data subjects, having regard to the particular combination of data that has been disclosed and the circumstances of the case, is a more meaningful standard.

(iii) We are of the view that the concept of reporting only for certain categories of personal data (e.g. "sensitive data") should be introduced. This will aid in providing a meaningful standard as to the types of data breaches that warrants a mandatory data breach notification. This will balance the need to safeguard the interests of individuals and the risk of causing undue alarm to individuals.

(iv) In relation to the proposed number of affected individuals (i.e., 500 or more), we are of the view that the number of affected individuals can be viewed as a factor to be taken into account when assessing the need for breach reporting, but the number of affected individuals alone is not a determining factor, as there remains the need to consider the other circumstances of the case, including the potential risk and the nature of the data.

(f) 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?

We are concerned that it will be onerous for organisations to be subject to multiple reporting threshold and requirements. For organisations that are already subject to an existing regulatory regime with reporting obligations, it would be preferable that they are not subjected to further reporting obligations.

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

We propose adding the exception where in the event organisations assess the level of "risk of impact or harm" to individuals to be low, organisations will be exempted from the data breach notification requirements.

Further, the GDPR provides for the following exceptions to the notification requirements in the following circumstances, amongst other things:

(i) the controller takes actions subsequent to the personal data breach to "ensure that the high risk for the rights and freedoms of data subjects" is unlikely to materialise; or

(ii) when notification to each data subject would "involve disproportionate effort", in which case alternative communication measures may be used.

We are of the view that the PDPC should consider a position similar to the GDPR exceptions.

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

The proposed time frames of 72 hours may not provide organisations sufficient time to investigate a suspected breach, liaise with the relevant stakeholders (who may be based in or outside Singapore) and/or to ascertain the actuality and impact of such breach.

Further, if a breach occurs after business hours or on non-business days, the organisation may require more time to carry out its investigations.

We propose a time frame of at least 5 business days. Further, the Commissioner should be given the authority to extend the time frame for organisations who require a longer time frame to investigate and ascertain suspected breaches.

(i) Classification of data intermediary

We note that the Public Consultation provides for the obligations of data intermediary ("**DI**"). We would be grateful that the PDPC provides clearer guidelines as to what constitutes a DI.

In practice, it can difficult to determine whether a party in fact acts as a DI. For example, when a travel booking portal is hacked, does the travel booking portal act as a DI for the various hotels and airlines that list rooms or seats on its site or is the travel booking acting on its own account?

With the increase in technological solutions, the problem with determining whether a party acts as a DI will heighten. Generally, such service providers will retain sole and absolute control over their systems and technology, whilst being able to characterise themselves as a DI in the event of a data breach.

It has been recognised by the UK's Information Commissioner's Office and Art 29 Working Party that the classification of data processors can raise difficult issues. Both have issued guidelines acknowledging the difficulties associated with such classification in some cases, but have nonetheless provided some clarity on guidelines for assessment.

4. CONCLUSION

4.1 In conclusion, whilst we understand and support the need to protect individuals, the imposition of these new requirements will translate into significant business costs and resource allocation for organisations. Accordingly, there will need to be more clarity and guidance from the PDPC in connection with the Proposed Approaches.

4.2 We humbly request that the PDPC takes these issues above into consideration and make the relevant enhancements to the framework for collecting, using and disclosing personal data under the PDPA in view of the issues raised.

WONGPARTNERSHIP LLP
5 October 2017