LYN BOXALL LLC

The Personal Data Protection Commission
460 Alexandra Road
#10-02 PSA Building
Singapore 119963

29 September 2017

corporate@pdpc.gov.sg

Dear Sir/Madam,

PDPA' Public Consultation on
Approaches to Managing Personal Data in the Digital Economy

The Data-Driven Marketing Association of Singapore (**DMAS**) thanks the Personal Data Protection Commission for the opportunity to provide comments in its public consultation on Approaches to Managing Personal Data in the Digital Economy.

DMAS is a non-profit trade organisation established in 1983 as the Direct Marketing Association of Singapore. Its mission is to enable its members to keep abreast of industry trends and best practices in Singapore and the region. It champions and promotes the interests of its members. It helps to enhance knowledge by facilitating the sharing of information and ideas on data-driven marketing. Key areas include social media, search, direct mail, email, and mobile marketing. DMAS' activities offer the opportunity for members to network and build relationships to profitably grow their businesses. DMAS also safeguards members' interests by constantly seeking to raise the stature and standards of data-driven marketing and building consumer confidence with adherence to high ethical standards of practice.

We attach a submission to the above consultation by DMAS. It sought feedback on this consultation from its membership base and community of data-driven marketers of which 45 percent are SMEs and the balance are MNCs.

Contact details for DMAS are:

Ms Lisa Watson, Chairman, and Mr Azhar Azib, DPO
Data-Driven Marketing Association of Singapore
113A Telok Ayer Street, Singapore 068582
Tel: +65 6227 8055 - E-mail: info@dmas.org - Website: www.dmas.org

Yours faithfully

Lyn Boxall
Director, Lyn Boxall LLC

50 Raffles Place
#37-00 Singapore Land Tower
Singapore 048623
+65 6829 7031
lyn@lynboxall.com

Registration No 201506074M

In summary, while the Data-Driven Marketing Association of Singapore (**DMAS**) has some comments on the details of the Commission's proposals about managing personal data in the digital economy (as set out below) and urges an element of caution, DMAS welcomes the proposed changes to the Personal Data Protection Act. Crafted carefully, they should help its members and organisations generally to both meet the challenges they face and the opportunities open to them successfully in the digital economy.

Enhanced Framework for Collection, Use and Disclosure of Personal Data

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)?

Notification of Purpose and Conditions for Notification of Purpose – Summary

DMAS sees the addition of an option for an organisation to collect personal data without consent, after the organisation has notified individuals of the purpose for which the personal data will be used and/or disclosed, as a good move. Used wisely, this option should support innovation in Singapore by giving organisations the ability to use and disclose personal data when they might not otherwise be able to do so.

However, collecting personal data without consent after notification of purpose should not be seen as, or become, the course of least resistance. It should be structured in such a way that it does not become the default collection mode. Consent is still preferred and encouraged, where possible.

In practice, DMAS considers that consent should continue to be preferred, although DMAS is not advocating that such preference should be stated explicitly in the Act. Instead, the controls over its use should be such that organisations would likely choose it only in extraordinary circumstances.

Two circumstances to be considered

The proposal is framed in the context of an organisation being able to notify the purposes for which it collects personal data at the outset – namely, before the organisation collects the personal data. DMAS sees two circumstances in which the digital economy brings both challenges and opportunity to organisations in Singapore.

First, there are circumstances where it is simply not practicable to obtain the consent of individuals to the collection of personal data about them in a way that is economic from a business perspective and/or that is acceptable from the perspective of the individual. (Here

'acceptable' means, for example, where individuals simply run out of patience – they get consent fatigue – as a result of repetitious requests for consent.)

Second, there are circumstances where the purposes are simply not known or knowable by the organisation at the time personal data is collected. Most notably, organisations may collect personal data for a defined purpose, such as participation in a retailer's loyalty programme. Later, the organisation may want to use or even disclose that personal data in carrying out data analytics, such as seeking correlations and designing algorithms to pursue opportunities for the organisation and benefits for the individuals arising from the analysis. While it may often be possible to carry out such analytics on anonymised data, comparing such data with separate known data sets can result in re-identification of the personal data.

DMAS suggests that the enhanced framework for the collection, use and disclosure of personal data should take both these circumstances into account.

Data protection impact assessment

The 'cost' of collecting personal data without consent, but with notification of the purposes for which the personal data will be used and/or disclosed is the performance of a data protection impact assessment (**DPIA**). DMAS supports the idea of organisations needing to do a DPIA for this purpose.

However, DMAS is concerned that where an organisation decides to apply this basis for most, or a significant part, of its collection of personal data carrying out DPIAs will be burdensome. This may play out in one of several ways.

For example, the data protection officer might find themselves spending a disproportionate amount of time doing DPIAs with the consequence that other important aspects of their role as data protection officer receive insufficient attention. One might say that organisations should hire additional staff. But in reality qualified and appropriately experienced data protection officers are in short supply in Singapore and many organisations will, in any event, balk at the expense of hiring an additional staff.

Busy data protection officers may decide to have their business line colleagues carry out the DPIAs. These individuals will face an obvious conflict of interest due to their virtually inevitable desire to reach a conclusion that enables their proposed programme to go forward. In other words, they are unlikely to be able to assess objectively the risks or impact to the individuals from the proposed collection, use or disclosure of personal data and/or to propose ways of mitigating such risks if those ways might reduce the effectiveness of the proposed programme from a business perspective.

In any event, DMAS considers that it will be necessary for the Commission to provide resources to organisations to assist them to conduct effective DPIAs and to implement appropriate risk mitigation measures. In addition, there should be a clear set of criteria laid down as to how the Commission will assess the adequacy of the DPIA in any particular case. Organisations will otherwise be unsure about what needs to be done and the

standards expected by the Commission. Organisations need visibility on how the Commission will assess DPIAs if the Commission investigates an organisation or reviews any specific DPIA.

On 4 April 2017, the Article 29 Working Party adopted guidelines on DPIAs and their sufficiency. DMAS does not express a view one way or the other as to the adequacy or suitability of the criteria for an acceptable DPIA that are included in Annex 2 to those guidelines. However, DMAS does suggest that the Commission publish an equivalent set of criteria appropriate to satisfy any requirements for a DPIA in Singapore.

Such a set of criteria published by the Commission should be directed at achieving a robust, framework for DPIAs that is risk-based. However, the framework should also be flexible because risk thresholds, for example, and potentially other thresholds become very specific to organisations and their risk appetite. The volatility (or lack of volatility) in any particular situation should also be taken into account.

Conditions for Notification of Purpose

The conditions proposed in the Consultation document are very general. DMAS considers that it would be helpful if examples – use cases – are made available. Descriptive language (such as 'material adverse impact') might be useful, although DMAS well recognises that it has the potential to be a double-edged sword. Of course, the DPIA must be risk-based and accommodate each organisation's risk appetite and tolerance.

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)?

Legal or Business Purpose - Summary

DMAS generally supports the addition of an exception to consent to collect, use and disclose personal data when it is necessary for a legal or business purpose. On the one hand, however, the Commission seems to be suggesting adding this exception to the Second, Third and Fourth Schedules to the Act. On the other hand, it is proposing that an organisation would need to carry out a DPIA prior to making use of the new exception, notwithstanding that an organisation is not required to conduct a DPIA before relying on any other exception to consent in the Second, Third or Fourth Schedules to the Act.

DMAS considers that, consistent with the existing exceptions in the Second, Third and Fourth Schedules to the Act, the proposed new exception is narrowly defined and does not require a DPIA.

Need for a 'legal or business purposes' exception

DMAS assumes that the enforcement decision against Jump Rope (Singapore) that was published in December 2016 involves the type of circumstances where the Commission has in mind that a 'legal or business purposes' exception from consent would likely be applicable.

If so, DMAS does not have any objection generally to the addition of an exception to consent to collect, use or disclose personal data for legal or business purposes. However, DMAS considers that the exception should be clearly defined and not serve potentially as a default position, again in the sense of becoming the course of least resistance.

'Legal and business purposes' generally

DMAS of course acknowledges the retention limitation obligation and the requirement for an organisation to delete documents containing personal data when no longer required for a legal or business purpose. However, in practice, it observes that 'business purpose' in the context of retention of personal data is interpreted in a very wide range of different ways.

Again, DMAS considers that any exception to consent for legal and business purposes should be clearly defined so that it cannot become a default position that erodes the importance of consent.

Notification of purpose

DMAS agrees that an organisation should not be compelled to notify an individual when the organisation has used or disclosed personal data about the individual under an exception to the need for consent in the context of legal or business purposes.

Right to access personal data and information about use and disclosure

If an exception to consent for collection, use and disclosure of personal data for legal or business purposes is introduced, section 21 of the Act should be taken into account. Specifically, an organisation should not be required to provide information about the use or disclosure of personal data about an individual for a legal purpose without consent:

- at all (unless it chooses to do so voluntarily) or
- at least where providing such information would or might tend to defeat the purpose of the collection, use or disclosure of personal data for legal purposes without consent – for example, where it would alert the individual that the organisation had disclosed personal data about the individual to identify and prevent potential fraudulent activities

Weighing benefits to the public or a section thereof

It seems to DMAS that this is a very amorphous condition. It needs more definition. Examples may assist or may unintentionally limit the intended scope of the exception.

For example, if organisation A discloses personal data to organisation B for the purpose of organisation B determining whether its customer is engaging in fraudulent activities, does organisation B constitute a section of the public? Does it make a difference if 'the public' more broadly than organisation B may never become aware of the suspected fraudulent activities because, for example, the sharing of personal data resolved the situation? Is organisation A exposed to potential liability under the Act if the suspected fraudulent activity is found not to exist? To what extent should organisation A have sought evidence from organisation B of the need for organisation A to disclose personal data?

Does the benefit to organisation B clearly outweigh the adverse impact or risks to the individual, namely the individual being identified as being engaged in fraudulent activity with the consequence (depending on the circumstances) of their employment being terminated or a police report being made about their conduct or some other consequence that, though appropriate in the circumstances, has an adverse impact on the individual?

Requirement for a DPIA – legal purpose exception

It does not seem to DMAS to be logical to require an organisation to do a DPIA where it proposed to collect, use or disclose personal data without consent for a legal or business purpose where a DPIA is not required where an organisation proceeds under any of the other exceptions to consent in the Second, Third or Fourth Schedule. (Nor should DMAS be understood to be suggesting that the requirement for a DPIA should extend to any other exceptions from consent.)

In addition, a legal purpose may arise unexpectedly and where there is insufficient time to carry out a DPIA.

Our comments above about a DPIA apply equally in this context if the Commission determinates ultimately that an organisation should carry out a DPIA before collecting, using or disclosing personal data without consent for a legal purpose.

Extension of existing exception

It seems to DMAS that its objective revealed by the Consultation document could be achieved by amending the existing exceptions for investigations or proceedings, as indicated below:

> 'the collection is necessary for any investigation or proceedings, if it is reasonable to expect that seeking the consent of the individual would compromise the availability or the accuracy of the personal data or the collection is necessary for another legal purpose or a business purpose intended to protect the reasonable interests of either or both of the disclosing organisation and the collecting organisation and the

organisation does not reasonably expect that the individual would consent to such disclosure'

'the use is necessary for any investigation or proceedings or for another legal purpose or a business purpose intended to protect the reasonable interests of the organisation and the organisation does not reasonably expect that the individual would consent to such use'

'the disclosure is necessary for any investigation or proceedings or for another legal purpose or a business purpose intended to protect the reasonable interests of either or both of the disclosing organisation and the collecting organisation and the disclosing organisation does not reasonably expect that the individual would consent to such disclosure'

Mandatory Breach Notifications

In summary, DMAS considers that voluntary notification is preferable to mandatory notification of data breaches. The Commission could allow mitigation factors to an organisation that voluntarily notifies the Commission about a known or suspected data breach.

However, DMAS recognises that the current global trend is to require mandatory notification of data breaches and the following comments recognise that it is likely unacceptable for Singapore to take a different approach to this issue.

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?

DMAS considers that specifying any number, whether 500 or not, is very prescriptive and unnecessarily rigid. DMAS recommends using a more holistic set of attributes to assess scale and harm of the data breach. Any number may be too low a threshold for some types of breach and too high for other types of breach.

While less objective criteria may be criticised in many contexts, in the case of data breaches DMAS considers them to be the preferable approach. In addition, use of a specific number is inconsistent with the approach taken generally in the Act including, in particular, the emphasis in the Act on reasonableness.

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?

DMAS considers that concurrent application of data breach notification requirements is a sensible approach because it does not create incremental work or other administrative effort for an organisation.

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

DMAS supports the extension of the exclusions under section 4 of the Act to the proposed breach notification provisions, not least because organisations are familiar with them typically. DMAS also supports the two additional exceptions noted in the Consultation document.

It is unclear whether the proposal is for the Minister to approve organisations to be exempted from the breach notification requirements:

- on the basis of an exemption application or similar request after a data breach has occurred or
- prior to a data breach occurring and to apply, of course, only if and when a data breach occurs within that organisation and on the basis of anticipated exceptional circumstances

Either way, the proposal seems to DMAS to be misconceived – impractical to seek an exemption and for it to be approved within 72 hours of a data breach occurring and equally impractical for an organisation to envisage with any particularity exceptional circumstances that may arise in the future.

In the latter case, if the availability of such an exemption is retained, all exemptions should be published so that they are generally available to the public so that individuals may consider the exemption before deciding to provide their personal data to an organisation.

Perhaps it would be better for a third exception to be included at the outset, namely an exception to the requirement to notify affected individuals where it is in the national interest not to notify affected individuals of a data breach.

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

DMAS is concerned that a limited time frame for notification can result in notifications being made before an organisation has been able to properly assess a suspected or actual data breach, both in terms of the individuals affected and the personal data of each individual is compromised. Flexibility is preferable and DMAS considers that a two-stage notification process may be preferable:

- first, to notify the Commission (perhaps within a specified period) of a known data breach or the existence of a suspected data breach to the extent that the organisation has relevant details and

- second, to notify the affected individuals within a reasonable period and when the organisation has been able to assess a suspected or actual data breach to the extent necessary to provide a meaningful notification to affected individuals (versus alarming them unnecessarily albeit quickly after a suspect data breach) and to develop appropriate and effective messaging

DMAS supports requiring data intermediaries to immediately notify the relevant organisation(s) so that the latter have the maximum amount of time to assess and execute relevant notification requirements.

29 September 2017