Baker & McKenzie.Wong & Leow
(Reg. No. 200010145R)

8 Marina Boulevard
#05-01 Marina Bay Financial Centre Tower 1
Singapore 018981

Tel: +65 6338 1888
Fax: +65 6337 5100
www.bakermckenzie.com

Thursday, May 28, 2020

Ministry of Communications and Information and the
Personal Data Protection Commission

Dear Sirs

Public Consultation for the PDP (Amendment) Bill

We refer to the public consultation paper on the Draft Personal Data Protection (Amendment) Bill, Including Related Amendments to the Spam Control Act issued by the Ministry of Communications and Information and the Personal Data Protection Commission on 14 May 2020.

We have been keenly following the previous public consultations, and we are pleased to set out under cover of this letter our comments on the proposed Personal Data Protection (Amendment) Bill.

We thank you for giving us the opportunity to provide feedback on the proposed bill, and we hope that our input would prove useful.

Please do not hesitate to contact the undersigned should any clarification be required

Yours faithfully

Ken Chia
Partner
+65 6434 2558
Ken.Chia@bakermckenzie.com

1. Summary of major points

We welcome the long anticipated refresh of the Personal Data Protection Act which will help propel Singapore to become a Trusted Data Hub and utilise the benefits of new technologies like 5G, IoT, AI and data analytics, whilst ensuring that organisations remain properly accountable for their use of personal data.

We would like to highlight the following areas for MCI/PDPC's further consideration:

Data Portability Right: Whilst it is useful to distinguish between user provided data, user activity data and derived personal data, organisations should not be required to port across data in a structure which reveals the organisation's creative organisation or combination of such data, but only the raw data.

Individuals acting in their personal or domestic capacity: Greater clarity on the scope of this exclusion would be useful and timely given the rise of the gig economy and more people working from home on a casual basis during the COVID-19 pandemic.

Organisations acting on behalf of public agencies: Whilst it is useful to re-demarcate the boundaries between the Government and the private sector, if the sole concern is to ensure proper protection of government data, the enhanced offenses in Part VIIIA should suffice. Otherwise there could remain concerns as to the sharing of personal data between such private sector organisations and the Government (for example if disclosure to a public agency would be in the public interest)

Access requests. Reducing the scope of prohibitions to access in relation to user provided and user activity data could in certain circumstances adversely affect third parties and their interests should be taken into account in a balancing test.

Loss of any storage medium or device. Breach of the Protection Obligation should only occur where personal data is stored in circumstances where unauthorised access, collection, use, disclosure, copying, modification or disposal of the personal data is likely to occur.

Amount of financial penalty. It should be clarified whether the annual turnover is the annual gross turnover of the organisation in Singapore, and whether the turnover of non-involved subsidiaries whose turnover may have been consolidated can be excluded.

Voluntary Undertakings. Greater clarity on whether and when Voluntary Undertakings will be published would help encourage organisations to consider giving voluntary undertakings.

Public benefit exemption. Requiring an organisation to take reasonable steps to inform the affected individuals rather than requiring actual notice would help with the use of the exemption.

Investigations and Business asset transaction exemptions. Modifications to the current exemptions would help address practical issues surrounding the use of such exceptions.

2. Statement of interest

Baker McKenzie Wong & Leow, as a full service legal service provider and advisor, frequently advises clients, both local and multinational from various industries, on their privacy and data protection needs at every stage, including issues that arise during a transaction, their daily operations or a crisis, and help organisations prepare for new legislation. Our IPTech practice which consists of a mix of locally-qualified and internationally-experienced lawyers, takes a proactive approach in anticipating and fully understanding how new legislation will affect our clients in Singapore and the region.

We have thus been following the development of this draft amendment bill very closely, as well as previous public consultations, as we foresee our clients will be impacted by the amendments proposed in the draft bill. We also foresee that the proposed amendments will affect our clients' operational guidelines in relation to their key stakeholders (which includes private individuals, other business entities, and government agencies), as well as in their continued engagement with the Ministry of Communications and Information and the Personal Data Protection Commission.

3. Comments

3.1 Definition of "derived personal data" in s2(1)

Will the "prescribed means or method" cover more than just "data derived by the organisation using simple sorting [or] common mathematical functions like averaging and summation"? MCI/PDPC may wish to borrow copyright concepts like derivative works and compilations, to set a requirement of originality and/or creativity for such derived personal data to avoid expanding (or narrowing) the scope of the data portability right. The data portability right should still require the 'raw' user activity data with for example any additional publicly available data which it may have been simply combined with to be ported across, but the organisation would not have to port across the derived personal data in a structure which reveals the organisation's creative organisation or combination of such data.

3.2 Exclusion of individuals acting in a personal or domestic capacity in s4(1)(a)

Although this provision was not changed, given the rise of the gig economy and more people working from home on a casual basis (e.g. home bakeries), whether an individual can be said to be “acting in a personal or domestic capacity" is becoming increasingly blurred. Perhaps it is time to relook at this exclusion and amend it to "an individual acting other than in the course of a business or for any monetary consideration”.

3.3 Removal of exclusion for organisations acting on behalf of public agencies in s4(1)

While this is useful to ensure the accountability of third-parties handling Government data, if such third parties as data intermediaries of the Government, their only obligations under the PDPA are to comply with the Protection Obligation and the Retention Limitation Obligation, which may still leave a legislative gap. If the intention is to simply protect Government data would not the penalties under the new Part VIIIA be sufficient?

Where such third parties are organisations rather than data intermediaries and need to disclose personal data to the Government, and it is not clear whether "the disclosure is necessary in the public interest", will this mean that such organisations will need to obtain the requisite consents from the individuals and commitments from the Government for example to use the personal data only for the purposes for which the organisation obtained consent, and to cease using such data if consent is withdrawn?

3.4 Access to user activity data about, or any user-provided data from, the individual who made the request despite such data containing personal data about another individual in new section 21(3A)

We note that paragraph 74 of the Consultation Paper states that "To ensure alignment with the Data Portability Obligation and for the reasons provided above in paragraph 46, MCI/PDPC will amend section 21 of the PDPA to reduce the scope of prohibitions to access in relation to user provided and user activity data.

Paragraph 46 of the Consultation Paper states that "Further, the third party's interests are unlikely to be adversely affected as the requesting individual's porting request is restricted to his/her personal or domestic capacity."

However this will mean that CCTV footage which records "user activity data" containing the personal data about another individual (eg a mistress) need not be redacted going forward.

Also, if a record of wrongdoing (eg an internal email between a superior and an employee) is submitted by the employee whistleblower as part of his complaint would that be "user activity data", because it is "created in the course or as a result of the individual's use of any product or service provided by the organisation"? If so, the email would have to be produced in response to an access request, and potentially jeopardise the whistleblower's job.

In such cases the third party's interests are likely to be adversely affected. Should there be a similar balancing test applied to such scenarios i.e. redaction will still be required unless the third party's interests are unlikely to be adversely affected?

3.5 Protection from loss of any storage medium or device on which personal data is stored in s24(b)

Previously the loss of a storage medium or device could be mitigated by encryption or the ability to remotely wipe the device since there would arguably not be any "unauthorised access" in such situations. Will this amendment require e.g. organisations to mandate the use of Kensington locks on their laptops now as a "reasonable security arrangement"?

We note that s26A(b) only requires the notification of "the loss of any storage medium or device on which personal data is stored in circumstances where the unauthorised access, collection, use, disclosure, copying, modification or disposal of the personal data is likely to occur". A similar change to s24(b) would help reduce the practical burden of complying with the change.

3.6 Amount of financial penalty in Section 29(2)(d)

Although the Consultation Paper states that "the amendments will increase the maximum financial penalty to (i) up to 10% of an organisation's annual gross turnover in Singapore; or (ii) S$1 million, whichever is higher", the revised s29(2)(d) does not make it clear that the relevant turnover is annual gross turnover in Singapore. Further if it is the group parent that is found to be the "organisation" responsible (i.e. the data controller), will its consolidated group accounts be used, even though it could include the turnover of subsidiaries which are not involved in the breach at all?

3.7 **Voluntary Undertakings in Section 31A**

The Guide on Active Enforcement states:

"*The PDPC will **not** accept an undertaking request when:*

...

the organisation does not agree for the undertaking to be published."

This seems to suggest that an undertaking agreed with the PDPC will be published.

However, the new Section 31A(5) states:

"*In addition, where an organisation or a person fails to comply with an undertaking mentioned in subsection (2)(c), the Commission **may publicise** the voluntary undertaking in accordance with the undertaking...*"

This suggests that an undertaking is not, in the usual course of things, published unless there is failure to comply with its terms.

Whether an undertaking is publicised or not, is likely to be a material consideration for many companies. Clarification from the PDPC in this matter, in the FAQs or the Guide on Active Enforcement, may be helpful. If undertakings might not be published in the usual course of things, this may incentivize companies to place more emphasis on this route and put in place breach management plans.

3.8 Deletion of First Schedule.

The current First Schedule deals with the Constitution and Proceedings of the Personal Data Protection Commission and is still referred to in Sections 2 and 5(2) of the Act. Will the First Schedule be retained or will the references in Sections 2 and 5(2) of the Act be deleted ?

3.9 Public Benefit exemption in Part 3 First Schedule para 1

The conditions in sub-paragraph 2(b) suggests that **actual** notice (provided in a reasonable form) to the individual may be required. However, there may be situations where the organisation does not have a direct relationship that enables it to provide such actual notification.

If the intention is to require the organisation to disclose its reliance on the legitimate interest exception, it may be clearer to phrase this requirement as: "*take reasonable steps to inform the individual that the organisation is collecting, using or disclosing personal*

data (as the case may be) in accordance with sub-paragraph (1)". This would bring the notification requirement in-line with a similar obligation under Deemed Consent by Notification at Section 15A(3)(b) to "*take reasonable steps to bring…the information to the attention of the individual*".

There shouldn't be a reason for the legitimate interest exemption to be subject to a higher standard of notification, compared to deemed consent by notification, especially since the legitimate interest exemption additionally requires a public benefit or interest to be established.

Conceptually, this would be cleaner as it maintains the distinction between actual notice and requirement to take reasonable steps to inform. By analogy, the difference would be similar conceptually to the difference between requiring actual and substituted service.

3.10 Investigations exemption in Part 3 First Schedule para 3

While this exemption remains unchanged, there is some uncertainty if information related to an investigation (including personal data) can be disclosed under this exemption to other entities within a group or 3rd parties service providers (e.g. data forensics) in course of an investigation.

The condition to the exemption (i.e. "*if it is reasonable to expect that seeking the consent of the individual would compromise the availability or accuracy of the personal data*") seems to contemplate a situation where the gathering of evidence could be compromised by obtaining consent from the individual. However, it is less clear if that condition is satisfied after evidence and information related to an investigation has been collected, and further use or disclosure of that information to other parties is made in the course of an investigation.

For example, obtaining consent to retrieve electronic evidence in devices and local email servers may compromise the availability/accuracy of the information. However, if that information needs to be disclosed to another entity for forensics, seeking consent may not compromise the availability / accuracy of the information already secured (though arguably seeking consent before the close of investigations might compromise further investigations/information gathering).

This issue is particularly acute in organisations where internal investigation functions are centralised, for example, at the headquarters, or where 3rd party service providers are involved in forensic investigations.

The MCI/PDPC may wish to consider expanding the present exemption to include further collection, use and disclosure of information gathered under the present exemption, for the purposes of the investigation.

3.11 Business asset transaction exemption in Part 3 First Schedule para 11

As certain transactions may involve the personal data of individuals such as sole proprietors who may not be a contractor or customer, PDPC may wish to consider the following amendment to para 11(2)(a):

be about an employee, a business partner, a contractor, a customer, a director, an officer or a shareholder of *Y*

To cover the period between signing and completion of a business asset transaction, PDPC may wish to consider the following amendment to para 11(3)(a):

> *X* must collect, and *Y* must disclose, only personal data that is necessary for *X* to determine whether to proceed with the business asset transaction, or (ii) if the determination is made to proceed with the transaction, to complete it.

Many parties may not be able to comply with para 11(4)(c) as the employees, customers, directors, officers and shareholders whose personal data is disclosed may not be able to be notified that the business asset transaction has taken place (i.e. completed). While it could be argued that this could still be fulfilled by notifying the employees etc. that the agreement has been signed, in some circumstances even that is not possible for confidentiality reasons. Accordingly PDPC may wish to consider this amended definition:

> (c) the employees, contractors, customers, directors, officers and shareholders whose personal data is disclosed must be notified within a reasonable time after completion that …

We note that the definition of "Business asset transaction" in para 11(6) remains unchanged i.e. "means the purchase, sale, lease, merger or amalgamation or any other acquisition, disposal or financing of an organisation or a portion of an organisation or of any of the business or assets of an organisation other than the personal data mentioned in sub-paragraph (1)".

As there has been some uncertainty in the market as to whether this exception only applies to asset sales and not share sales, PDPC may wish to consider this amended definition:

> "the purchase, sale, lease, merger or amalgamation or any other acquisition, disposal or financing of an organisation or a portion of an organisation or of any of the [voting] shares, units, equity interests, business or assets of an organisation other than the personal data to be disclosed under paragraph (1)".

4. Conclusion

The proposed Bill provides valuable improvements to Singapore's privacy regime. We would support further changes to the PDPA however in particular in respect of the Transfer Limitation Obligation and how this is implemented in the PDP Regulations.