Pinsent Masons MPillay

RESPONSE TO PUBLIC CONSULTATION ISSUED BY MINISTRY OF INFORMATION, COMMUNICATIONS AND THE ARTS

PROPOSED PERSONAL DATA PROTECTION BILL

30 APRIL 2012

Pinsent Masons MPillay LLP
16 Collyer Quay #22-02 Singapore 049318
T +65 6305 0929 **F** +65 6534 3412 www.pinsentmasons.com

RESPONSE TO PUBLIC CONSULTATION ISSUED BY MINISTRY OF INFORMATION, COMMUNICATIONS AND THE ARTS

PROPOSED PERSONAL DATA PROTECTION BILL

INTRODUCTION

We welcome the opportunity to participate in this consultation on the Proposed Personal Data Protection Bill ("**PDPA**").

We have reviewed the PDPA and take the view that it is a robust start to introduce pragmatic and effective data protection laws in Singapore. We believe that it is important that Singapore's proposed data protection law strike a balance between facilitating technology developments and business interests while providing individuals a legislative framework which provides adequate protection for the privacy and security of their data. In this regard, the positions adopted in the PDPA are appropriate in finding this balance between promoting individual privacy and fostering business interests and innovation in Singapore.

The PDPA is presented as a framework law to provide certainty and clarity on the applicable data protection obligations and requirements of organisations in Singapore, regardless of business sector. In this respect, the PDPA takes a less prescriptive and granular approach towards organisations entrusted with the handling of personal information, and provides a level of flexibility for organisations to adapt their practices and policies while still ensuring organisations' compliance with their data protection obligations.

A key challenge in this current technological environment lies in providing data protection laws which are future-proofed and able to keep up with today's rapid pace of technological change. As the PDPA adopts technology and media neutrality (e.g. the PDPA does not indicate preferences for solutions and mechanisms for obtaining consent and does not make the distinction between electronic and non-electronic data), we believe that the PDPA is well-positioned in this regard. We take the view that it is in the best interests of all relevant participants (individuals, organisations and data intermediaries) to retain the ability to flexibly apply the law so that it can be built into existing business processes

Further, we note that the Data Protection Commission is granted strong powers to administer the PDPA (including the power to issue guidelines and directions to remedy non-compliance, to review complaints and initiate investigations). We believe that the DPC, as an active regulatory enforcement body, would play an important part in bringing a level of certainty in how the new data protection laws are to be interpreted and applied.

We have indicated some areas in the PDPA where it may be possible to clarify the positions taken.

We hope that our input will assist MICA in the development of Singapore's new data protection framework.

1. PERSONAL DATA WITH SINGAPORE LINK: SECTION 5

1.1 The PDPA covers personal data with a 'Singapore link' including personal data that is collected, used or disclosed within Singapore (Section 5, PDPA). This could extend to organisations with no physical presence in Singapore engaging in data collection, use or disclosure activities in Singapore, and could have the following implications:

1.1.1 organisations outside of Singapore that collect personal data will be subject to the PDPA so long as the individual was in Singapore when the personal data was collected (Section 5(2)(a)(i)) – this could include organisations which collect personal data from individuals in Singapore through online channels or portals to a server or database located outside Singapore);

1.1.2 Singapore organisations engaging in certain types of data processing activities on behalf of organisations outside of Singapore might be subject to the PDPA as well since such data processing activities may be construed as "*use*" (Section 5(2)(b) covers organisations which "*use*" the personal data in Singapore).

1.2 We recommend that this provision be reconsidered and reframed to avoid unintended extra-territorial application. In the scenario described in paragraph 1.1.1 above, the PDPA is to apply to the collection of personal data with respect to individuals who are physically present in Singapore at the time of collection (Section 5(2)(a)(i), PDPA). Given the increasingly global nature of data flows, focussing on the physical location of the data subject and the data (as Section 5(2)(a)(ii) does) gives rise to the highlighted scenario. Considering the scenario described in paragraph 1.1.2 above, Section 5(2)(b) and the terminology "*use of personal data*" could be clarified such that the Singapore organisation could be regarded as a data intermediary and therefore face reduced data protection obligations under the PDPA.

1.3 Further we suggest that Section 5(2)(b) wording be clarified to ensure that where a Singapore organisation exports personal data to a data intermediary outside Singapore, that Singapore legal requirements flow with personal data and continues to apply and protect such personal data abroad.

2. DISTINCTION BETWEEN DATA CONTROLLER AND DATA INTERMEDIARY

2.1 We note that "*data intermediary*" means "*an organisation which processes personal data on behalf of another organisation but does not include an employee of that other organisation*" (Section 2, PDPA).

2.2 Further clarity on the definition of "*data intermediary*" would be helpful to more clearly draw the distinction between an organisation as data controller and a data intermediary. A defining feature of an organisation as a data controller is its effective control of personal data. We note that the PDPA provides that "*[a]n organisation is responsible for personal data in its custody or under its control*" (Section 13(2), PDPA). We suggest that the definition of "*data intermediary*" and/or Section 13(2) wording be supplemented with language which clarifies that an organisation is data controller (having control and custody) only with respect of the personal data it is processing for its own purposes and that an entity is "*data intermediary*" only to the extent it is

processing personal data on behalf of a data controller (and upon its instructions) and does not have effective control over such personal data.

3. ACCOUNTABILITY: SECTION 13

3.1 We support the PDPA's emphasis on accountability. The PDPA requires an organisation to be responsible for personal data in its custody or under its control (Section 13(2), PDPA) and requires each organisation to implement accountability measures such as appointing a designated data protection officer to ensure the organisation's compliance with the PDPA (Section 13(3), PDPA).

3.2 Individual organisations are thus made responsible for determining how best to meet those standards in practices and to consider and assess what is appropriate in meeting their responsibilities under the PDPA. This permits organisations to adopt methods, practices and processes to comply with the PDPA in a way best suited to their business models and practices. This is important in light of the fact that the PDPA applies to different organisations regardless of business sector, which handle different types and volumes of data and that the PDPA does not seek to impose a "one-size-fits all" model.

3.3 To assist in organisations' compliance, MICA should consider providing guidelines on the roles and responsibilities of the designated individual(s) / data protection officers responsible for compliance with the PDPA.

4. CONSENT: SECTION 15 – SECTION 17

4.1 We note that the PDPA establishes a framework for organisations' data collection, use and disclosure with data subjects' consent, but at the same time, provides organisations with sufficient latitude to determine the appropriate method and mode of obtaining consent from data subjects (Section 13 and Section 14, PDPA).

4.2 The PDPA allows organisation to collect, use or disclosure personal data only if the data subject gives or is deemed to give consent to such collection, use or disclosure (Section 15(a), PDPA), and consent can be deemed only in a very specific instance (where the data subject voluntarily provides the personal data to the organisation and it is reasonable that the data subject would voluntarily provide the data: Section 17, PDPA). While intended to restrict organisations' misuse of personal data, these provisions may have the effect of introducing an "opt-in approach", which could be restrictive and impracticable for organisations in many scenarios.

4.3 We take the view that consent provided by data subjects should be free, unambiguous, specific and informed consent. However, for the purposes of compliance with the PDPA, organisations may require individuals to consent to everything (notwithstanding the Section 20(a) requirement that the purposes of collection, use or disclosure of personal data must be reasonable and appropriate) and individuals may agree without consideration for what organisations intend to do with their personal data, thereby rendering the protection under the PDPA less effective and/or requiring more policing by the regulator. We believe that it is important for the PDPA to allow for a range of grounds to legitimise organisations' use of personal data, consent being one of them.

5. NOTIFICATION OF EMPLOYEES: SECTION 22(4)

5.1 We note that the consent requirement is waived if an organisation's collection of employee personal data is reasonable for the purposes of managing or terminating an employment relationship between an organisation and the individual (Section 19(1) and Third Schedule, 1(r)). However, the organisation is required to *notify* its employees of the collection, use or disclosure of their personal data for purposes of managing or terminating the employment relationship/s (Section 22(4), PDPA).

5.2 We agree that the waiver of the consent requirement is useful in the employer-employee context and recognise that the notification requirement affords a level of protection to individual employees by requiring employers to inform their employees of their data collection and usage practices. For expediency, we suggest that a one-time notification to employees (e.g. at the time of on-boarding, upon receipt of Employee Handbook, company intranet update) by an organisation should suffice for the purpose of satisfying the notification requirement under Section 22(4), PDPA (instead of the organisation providing notification each and every time it collects or uses its employee personal data). This will provide organisations with flexibility in how they can choose to notify their employees while minimising the administrative burden of having to provide notifications repeatedly.

6. ACCESS OF PERSONAL DATA: SECTION 23

6.1 Under the PDPA, individuals will have the right of access to their personal data and information about the ways organisations are using their personal data (Section 23, PDPA). We support giving individuals the ability to access data about themselves and finding out how organisations are using their personal data as access is an essential aspect of an individual's control over his or her own data.

6.2 Exclusions to such right of access are set out in Section 23(2) and Section 23(3) (such as when disclosure could threaten the safety or health of another individual or cause immediate or grave harm to the safety of health of the requesting individual or would reveal personal data about another individual). However if the organisation is able to remove the information referred to in the exclusions, then the organisation shall provide the individual with access to the personal data after all such information is removed (Section 23(4), PDPA).

6.3 We venture to add that an organisation's obligation to provide access should be flexible and reasonable in scope, and also reflect technical and practical realities. There are some technical and practical limitations on the right of access, and organisations should be allowed further flexibility to comply as far as possible, such access requirement should apply to personal data that is reasonably accessible in the ordinary course of business (say, as opposed to data that is in an aggregate, de-identified format or in a format which makes it infeasible to locate or retrieve the data). We recognise that the Sixth Schedule, 1(k) already provides specific exceptions from the Section 23 access requirement (such as any request that would unreasonably interfere with an organisation's operations because of the repetitious or systematic nature of the requests; if the burden or expense of providing access would be unreasonable to the organisation; any request for information that is trivial or otherwise frivolous or vexatious), but we propose that the further flexibility be

permitted by applying the access requirement to personal data that is reasonably accessible in the ordinary course of business.

7. PROTECTION OF PERSONAL DATA - SECURITY ARRANGEMENTS: SECTION 26

7.1 The PDPA provides that an organisation "*shall protect personal data in its custody or under its control by making reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification or disposal or similar risks*" (Section 26, PDPA).

7.2 We agree that the requirement to make reasonable security arrangements are necessary and agree with the proposed approach. These safeguards set out in Section 26 obligate organisations to protect data against improper disclosure or use, but at the same time provide organisations with the flexibility to implement and maintain the appropriate safeguards and controls. We suggest that additional clarification be made to highlight that these security arrangements include the appropriate organisational, administrative, technical and/or physical measures as required in the context and given the nature and amount of personal data being used and processed. In addition, we suggest that Section 26 wording to be extended to include "accidental" and "unlawful" access, use and disclosure, to provide for a more robust framework to be adopted by organisations.

7.3 In relation to data intermediaries (which are also required to have appropriate security arrangements in place under Section 26), we highlight that the organisation/data controller manages the relationship with individuals and the data intermediary does not have a direct relationship with the data subject. For example, in the cloud computing scenario, cloud service provides host, store and deliver large amounts of data and services on behalf of other organisations – cloud providers, as data intermediaries may have little or no knowledge of the personal data which they are handling on behalf of their customers.

7.4 An important part of regulating the data intermediary's data processing activities is thus contractual. It is important to recognise that the data intermediaries' security obligations will depend on the organisation's own obligations and whether the organisation has advised the data intermediary of any special requirements for handling that particular data. Appropriate contractual clauses relating to security measures and an organisation's audit and monitoring rights will help to provide the organisation/data controller with the means to ensure its own PDPA compliance, and at the same time protecting the personal data of individuals. We suggest that guidance on contractual aspects, security measures and audit/monitoring rights be provided to both organisations and data intermediaries to facilitate compliance.

8. RETENTION OF PERSONAL DATA: SECTION 27

8.1 We note that the PDPA requires an organisation to destroy or anonymise personal data as soon as it is reasonable to assume that (a) the purpose for which that personal data was collected is no longer served by such retention; and (b) retention is no longer necessary for legal or business purposes (Section 27(1)).

8.2 As some organisations may already have existing standard data records and retention policies in place, we suggest that retention of personal data in accordance with such organisational policies be considered retention for "business purposes", provided that the relevant organisation (and its policies) comply with, and do not contravene the other requirements under the PDPA. In this way, the individual's rights under the PDPA remain protected whilst not imposing additional compliance costs and efforts to destroy or anonymise personal data on organisations which already have sound data retention policies in place.

9. RIGHT OF PRIVATE ACTION: SECTION 36

9.1 We note that individuals who suffer loss or damage as a result of data protection violations can institute civil proceedings against organisations and remedies which may be sought include injunctions, declarations and damages (Section 36, PDPA).

9.2 Whilst there is a need to ensure that organisations remain accountable in their handing of personal information, the inclusion of a general private right of action may be of less benefit for individuals' privacy as individuals are less likely or less inclined to institute civil proceedings. Instead further protection could be afforded to individual data subjects by introducing and outlining a process whereby individuals may submit complaints directly to the Data Protection Commission (which is already imbued with powers of investigation upon receiving complaints or of its own motion, under Section 33).

10. DO-NOT-CALL REGISTRY: PART IX

10.1 We support the Do-Not-Call Registry ("DNC Registry") in providing individuals a simple and effective means to "opt-out" of receiving marketing messages by registering their telephone numbers with the DNC Registry. The PDPA provides that any sender of a marketing message will be required to check if the Singapore telephone number is registered on the DNC Registry within 30 days before sending the message (Section 47(1), PDPA).

10.2 We believe a distinction should be drawn between telephone numbers which are not personal data (i.e. telephone numbers alone) and telephone numbers which are personal data (i.e. telephone numbers which are held together other information which can identify an individual, such telephone numbers accompanied with name, address, etc.). The DNC Registry will be more useful, and have practical implications only in relation to telephone numbers which are not personal data. Where telephone numbers are personal data, the organisation should not send marketing messages to such telephone numbers in any case since this will be a contravention of the PDPA requirements (unless the individual has consented to use of personal data to receive marketing messages). If the organisation has obtained the relevant consent, then the organisation should be able to send marketing messages to the telephone number since such consent has been obtained (regardless of whether the individual has registered his/her telephone in the DNC Registry or not), unless the individual's registration in the DNC Registry constitutes withdrawal of consent.

10.3 We note that additional clarification can be made to highlight the distinction between telephone numbers constituting personal data and telephone numbers not constituting personal data, i.e. the Section 47 requirement to

check with the DNC Registry should only apply in cases where Singapore telephone numbers do not constitute personal data. Further, it would be helpful to have further guidance on the interplay between the PDPA consent requirement and the DNC Registry requirements.

11. LOCATION-BASED SERVICES ("LBS") AND GEO-LOCATION DATA

11.1 We note from the Consultation Paper that providers of LBS are expected to comply with the PDPA with respect to any personal data (including geo-location data where applicable) under their control or custody. We agree that location and geo-location data should be covered as proposed. Providers of LBS should be governed by the PDPA obligations as such personal data can be used or disclosed to other recipients. Such information gathered may not be able to qualify as personal data when read on its own but could identify individuals when combined with information from other sources. This means that LBS providers and operators should alert mobile users when the technology is in use, because some of the information gathered could later become personal data, depending on the processing of it.

12. DATA BREACH NOTIFICATIONS

12.1 We note that the PDPA does not provide for notification of data breaches, as MICA recognises that notification of every potential data breach may be administratively burdensome for organisations and be of limited usefulness to individuals (paragraph 2.112, Consultation Paper). The PDPA therefore does not make it mandatory for organisations to issue data breach notifications but in the future, the DPC may consider an organisation's issuance of a data breach notification as a mitigating factor in future enforcement actions.

12.2 While data breach notifications are not mandatory, we suggest the issuance of recommendations and best practices to guide organisations when data breaches do occur. For instance, it would be crucial for organisations to undertake data breach notification when there is a significant risk of serious harm to the data subject (as opposed to where the personal information is anonymised, encrypted or in unreadable-format). In the case of data breaches by data intermediaries, organisations can consider building in contractual provisions for the data intermediaries to notify where there is a data breach which could result in the personal data being lost, destroyed, disclosed or misused.

13. ELECTRONIC MARKETING

13.1 In relation to electronic marketing practices, both the Spam Control Act ("SCA") and the PDPA will impact on an organisation's ability to conduct electronic marketing. While the SCA specifically regulates the conduct of electronic marketing, the PDPA will (once enacted) have the broader function of regulating the collection, use, disclosure, transfer and security of personal data. Accordingly, the PDPA does not necessarily adopt the same approach as the SCA, and inconsistencies and overlaps arise between the two laws.

13.2 Under the SCA, there is no requirement for an organisation to obtain an individual's consent to send marketing messages. However, where consent is not given, the SCA imposes certain conditions (such as an unsubscribe facility with details of how to unsubscribe in the message it self; subject lines of messages must be labelled with "ADV".).

13.3 Under the PDPA, an organisation will usually require an individual's consent to use their personal data (Section 15(a), PDPA), which includes email addresses and other contact details. In the context of electronic marketing, this could be by way of an "opt-in" tick-box e.g. "I consent to you sending me marketing information about your products by e-mail from time to time. Please tick box". To gain valid consent, the organisation will need to notify the individuals how their details will be used (i.e. to market to them) (Section 22, PDPA), and an individual can withdraw consent at any time on notice (Section 18, PDPA).

13.4 Prior to the PDPA, an organisation could send marketing messages to an individual without obtaining their consent. However, the PDPA now requires organisations to obtain consent prior to marketing. Accordingly, it now appears the practice permitted under the SCA to market without consent (subject to the conditions in Second Schedule) will not usually be possible. We note that additional clarification could help to clarify and ensure certainty and greater compliance in relation to marketing practices.

CONCLUSION

Businesses increasingly operate on an international basis both internally within global group structures and externally with networks of customers and suppliers. This is facilitated by the internet which allows the quick and easy transmission of data across national boundaries and technologies that allow the increasingly complex and cheap collection, storage, use and disclosure of data. The combination of these factors means that personal information about individuals in Singapore may often be processed overseas, frequently without the explicit knowledge or consent of those individuals. This raises issues such as the security of such data, who may have access to it and for what purposes and what rights the individual may have to object.

We support the PDPA, as a data protection regime which permits and facilitates data flows across international borders based on organisations remaining accountable for the protection of data regardless of geographic location. This permits organisations in Singapore to enjoy the cost and speed efficiencies in today's networked world. At the same time, clarifying and bolstering the data intermediaries' responsibilities and obligations under the PDPA, will also encourage more businesses to run data processing and data management operations out of the country and create a conducive environment for the fast growing global data processing and management industries, like cloud computing.

For any questions concerning our feedback, please contact our Rosemary Lee, Counsel at +65 6305 0912 (email: rosemary.lee@pinsentmasons.com)

Pinsent Masons MPillay LLP

30 April 2012