BAKER & MCKENZIE.WONG & LEOW

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

Monday, April 1, 2013

Personal Data Protection Commission

By email
pdpc_consultation@pdpc.gov.sg

Dear Sirs

Public Consultation on Proposed Regulations on Data Protection in Singapore

We refer to the public consultation paper on the Proposed Regulations on Data Protection in Singapore ("**Proposed Regulations**") issued by the Personal Data Protection Commission ("**PDPC**") on 5 February 2013.

We have been keenly following the development of the *Personal Data Protection Act* ("**PDPA**") and we are pleased to set out under cover of this letter our comments on the Proposed Regulations.

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

This submission is made on behalf of Baker & McKenzie.Wong & Leow. If you require any clarification, please do not hesitate to contact the undersigned.

Yours faithfully

See Khiang Koh
Senior Associate
+65 6434 2651
SeeKhiang.Koh@bakermckenzie.com

TABLE OF CONTENTS

1. SUMMARY OF MAJOR POINTS

1.1 In the next section, we have set out our response to the questions posed in the public consultation paper for the Proposed Regulations. Our comments are summarised below for ease of reference:

Question in relation to the administration of requests for access to and correction of personal data

Question: Do you have any views/ comments on the proposed manner in which an individual may make an access or correction request or the proposed positions relating to how organisations are to respond to such requests?

(a) We are generally supportive of the positions set out in the Proposed Regulations in this regard. However, we would suggest that the Proposed Regulations should impose additional safeguards to prevent organisations from charging an exorbitant fee or taking an inordinate amount of time in responding to an access request. In particular, we would propose that a duty should be imposed on organisations to inform individuals regarding their right to refer the matter to the PDPC for review in the event of a dispute.

Questions in relation to the transfer of personal data outside Singapore

Question 1: Do you have any views/ comments on other means of ensuring the protection of personal data transferred out of Singapore?

(b) We are of the view that there should be other ways of complying with the prescribed requirements for cross-border transfers of personal data in situations where it is impracticable to impose legally binding commitments on the recipient. One option that the PDPC may wish to consider is allowing recipients who are certified under the APEC Cross-Border Privacy Rules ("**CBPR**") system the benefit of a presumption that personal data transferred to such recipients would be afforded a comparable standard of protection.

(c) Clarity should also be provided as to how organisations may qualify for an exemption from the prescribed requirements for cross-border transfers of personal data. In particular, the PDPC should clarify if an exemption may be granted where the individual has been duly notified regarding the transfer of personal data outside of Singapore, and consents to such transfer.

(d) One additional comment that we would raise is that the PDPC should consider whether data intermediaries should also be under similar obligations where they are the party transferring personal data overseas.

Question 2: Do you have any views/ comments on the proposed requirements for contractual clauses and binding corporate rules to protect personal data transferred out of Singapore?

(e) We do not have specific comments on the proposed requirements imposed on contractual clauses or binding corporate rules used to ensure that personal data transferred outside of Singapore will be afforded a comparable standard of protection. However, we would recommend that the PDPC either (i) provide further guidance to organisations by promulgating standard contractual provisions which would satisfy those requirements, or (ii) confirm that the use of EU Model Clauses would suffice.

(f) Further, we would recommend that the PDPC provides a facility allowing organisations to submit their proposed contractual provisions or binding corporate rules for review, in order to ensure that the criteria set out in the Proposed Regulations have been satisfied.

This would be akin to the process for organisations relying on binding corporate rules in the EEA to seek authorisation from the designated lead data protection authority.

Questions in relation to individuals who may act for others under the PDPA

Question 1: Do you have any views/ comments on the areas for which individuals may act for other individuals under the PDPA that should be prescribed?

(g) No.

Question 2: Do you have any views/ comments on the extent to which minors should be able to exercise rights and powers conferred on them under the PDPA?

(h) While we agree that minors should under certain instances be allowed to exercise the rights and powers conferred on them under the PDPA, we are of the view that it is unnecessary to specify an intermediate age range whereby minors are allowed to exercise such rights and powers, provided that they understand the nature of such rights and powers and the consequences of exercising such rights and powers.

Question 3: In particular, do you have any views on the minimum age below which individuals should not exercise their own rights and powers under the PDPA?

(i) As a corollary to our previous point, we would propose that the minimum age should either be specified as 18 or 13, but not 14.

Question 4: Do you have any views/ comments on the proposed priority list in relation to individuals that may act for deceased individuals?

(j) We are of the view that the first order of priority proposed is unduly complex. We prefer the second scheme where categories of relatives are aggregated, but would propose minor amendments to the list.

Question 5: In particular, do you have any views on the appropriate priority list and/or whether priority should be given equally to all relatives (or to relatives within certain categories such as spouse and children, parents and siblings, etc) for the purposes of the PDPA?

(k) As above.

2. COMMENTS

Question in relation to the administration of requests for access to and correction of personal data

Question: Do you have any views/ comments on the proposed manner in which an individual may make an access or correction request or the proposed positions relating to how organisations are to respond to such requests?

2.1 We are generally supportive of the proposed positions relating to how organisations are to respond to access requests from individuals described in the Proposed Regulations, but would suggest minor tweaks to ensure a more equitable outcome. For example, while we agree that organisations should be allowed to charge a minimal fee for access requests on an incremental, cost recovery basis, and should provide the individual with an estimate upfront, we would recommend that organisations should also be under an obligation to provide a breakdown for each line item making up the fee that it wishes to charge. Likewise, we understand the PDPC's concerns in relation to the setting of a quantitative cap on the amount of fees chargeable for access requests, but would suggest that the PDPC provides further guidance in terms of the types of cost that would normally be recoverable and, for each of these, a maximum amount or an indicative range that would likely be considered reasonable (e.g. costs associated with printing or photocopying should not exceed 20 cents per page/ range between 5 to 10 cents per page).

2.2 In terms of the timeframe within which organisations should respond to access requests, we agree with the proposed position requiring organisations to either respond within 30 days, or to inform the individual within this timeframe as to the soonest possible time the organisation will be able to respond. However, given that the Proposed Regulations state that organisations are not obliged to provide access until the individual agrees to pay the fees, or (if required by the organisation) pays the deposit, we would propose that this 30-day period should commence from the date the individual either agrees to pay the fees or actually pays the deposit, rather than the date of the request.

2.3 Finally, we note that it would be difficult for an individual to contest the amount of fees that an organisation wishes to impose. It is even more difficult for an individual to verify whether the organisation is indeed using all reasonable efforts to respond within the shortest amount of time possible. Under section 28 of the PDPA, the PDPC has the power to review both of these matters, and this is a very important safeguard in ensuring that organisations act reasonably in responding to access requests. However, we suspect that the efficacy of such protection will be diluted in practice given that the aggrieved individual may not be aware of his/her right to make an application to the PDPC for such a review to be undertaken. As such, we propose that all organisations should be under an obligation to notify individuals making access requests regarding the existence of such a right, and the manner in which such an application may be made.

Questions in relation to the transfer of personal data outside Singapore

Question 1: Do you have any views/ comments on other means of ensuring the protection of personal data transferred out of Singapore?

2.4 We understand the need for organisations transferring personal data outside of Singapore to ensure that a comparable standard of protection is conferred on the personal data so transferred, as well as the need for organisations to have some flexibility in determining the appropriate means by which such comparable standard of protection is guaranteed. Where such transfers take place between two entities within the same corporate group, it is likely that the two entities

would be able to agree to a binding contract or a set of binding corporate rules governing the use of the personal data transferred. However, as between two independent corporate entities, it may not always be practicable for the organisation transferring the personal data to impose contractual limitations on the recipient. For example, if the transferring organisation is an SME in Singapore while the recipient is an MNC based in another country providing cloud services on its standard terms and conditions, it is likely to prove an uphill task for the local SME to persuade the foreign MNC to change its standard terms and conditions to take into account the requirements prescribed by the PDPC, unless the foreign MNC has a sufficient base of Singapore customers to make such customisation worthwhile.

2.5 We would therefore suggest that alternative methods of satisfying the prescribed requirements should be provided. For example, the PDPC may wish to consider if it would be prepared to set up a framework for organisations receiving personal data from Singapore to voluntarily self-certify compliance with a set of guidelines ensuring that such personal data would be protected to the degree required under the PDPA. Alternatively, the PDPC may wish to rely on certification under the APEC CBPR system, which involve evaluation by an APEC-recognised Accountability Agent and enforcement by an appropriate regulatory authority, as proof that the recipient provides a comparable standard of protection.[1] Likewise, transfers to recipients that have signed up to the EU-US Safe Harbour framework may take place without the need for binding contractual provisions to be put in place. This could be operationalised in the form of a presumption in the Proposed Regulations that such "certified" organisations would provide a comparable standard of protection.

2.6 Another important element of flexibility lies in the power of the PDPC to grant organisations exemptions from the prescribed requirements under section 26(2) of the PDPA. It is not clear if the PDPC intends to set out the conditions that organisations have to satisfy in order to qualify for such exemptions in the Proposed Regulations or in separate regulations to be prescribed in the future, but it is clear that further guidance is required. In particular, we note that similar requirements in the data privacy legislation of a number of jurisdictions (including countries in the EEA and Australia) do not apply where the individual consents to the transfer of his/her personal data outside of the home country. However, the drafting of the PDPA appears to suggest that the prescribed requirements for cross-border transfers of personal data apply regardless whether the individual has consented to the transfer. In fact, given that such transfers would likely also constitute a disclosure of personal data, consent may be required before such transfers can even take place. In the circumstances, granting exemptions based on consent from the individual may potentially render the prescribed requirements nugatory.

2.7 Notwithstanding the foregoing, we would recommend informed consent from the individual should provide a way for organisations to proceed with a transfer of personal data overseas, particularly where it is impracticable for the transferring organisation to impose contractual limitations on the recipient. In order to avoid the difficulties mentioned above, the consent required in such an instance could be of the higher "clear and unambiguous" standard, as required in relation to the do-not-call registry.[2] If it wishes, the PDPC could also be involved in assessing whether the requisite consent has been obtained by specifying this as an exemption to the prescribed requirements. Alternatively, consent may form an exception to the prescribed requirements, such that there would be no need for the transferring organisation to make an application to the PDPC for exemption. In the event the PDPC disagrees, we would recommend

[1] The United States was the first country to participate in the APEC CBPR system, and we understand that Mexico was recently accepted as the second participating economy. TRUSTe, which operates a privacy seal program, has also applied to be the first Accountability Agent in the APEC CBPR system.
[2] Per section 43(3)(a) of the PDPA.

that it should be clearly specified in the Proposed Regulations that the prescribed requirements apply despite the fact that the individual has consented to the transfer.

2.8 While this is strictly speaking outside the scope of the current public consultation, we would also add that the PDPC should also consider whether the obligation to comply with the prescribed requirements should be imposed on data intermediaries. We note that under the PDPA, data intermediaries are subject only to the provisions relating to protection and retention of personal data. It is the responsibility of the organisation that the data intermediary is processing personal data for to comply with the prescribed requirements for cross-border transfers of personal data. However, this may be unrealistic in the scenario where the data intermediary is the one transferring the personal data overseas. For example, let us assume that the cloud service provider in our previous example has a data centre in Singapore and the local organisation transfers personal data to a server that data centre. The cloud service provider also has a mirror server located in a data centre owned by an affiliate in another country. Assuming that cloud service provider is a data intermediary (i.e. it only processes personal data on behalf of the local organisation), should the obligation to comply with the prescribed requirements still fall on the local organisation?

Question 2: Do you have any views/ comments on the proposed requirements for contractual clauses and binding corporate rules to protect personal data transferred out of Singapore?

2.9 We note that the Proposed Regulations set out various elements that the binding contractual provisions or binding corporate rules used by organisations transferring personal data overseas should address (e.g. purpose, use and disclosure, accuracy, protection, retention, policies). We do not have any specific comments on the proposed requirements imposed.

2.10 However, we would recommend that the PDPC assist organisations in complying with the prescribed requirements by promulgating standard contractual provisions that would satisfy those requirements. This would make it easier for the transferring organisation to negotiate for the inclusion of those standard clauses in its contract with the recipient, and will likely save the parties substantial time and cost. Alternatively, the PDPC may consider if the use of the EU Model Clauses, or a modified form of the EU Model Clauses, would sufficient address the requirements set out in the Proposed Regulations.

2.11 Further, we would suggest that there should be a facility for transferring organisations to submit their proposed contractual provisions or binding corporate rules to the PDPC for review. The PDPC can ensure that the proposed contractual provisions or binding corporate rules meet the criteria set out in the Proposed Regulations, or provide further guidance to the transferring organisation on how those requirements can be met. We note that a similar procedure has to be followed before binding corporate rules may be used to legitimise transfers of personal data from an organisation in the EEA to affiliates in third countries which do not ensure an adequate level of protection. Even if the PDPC accepts the suggestions set out in the previous paragraph, the facility would still be useful for transferring organisations who wish to deviate from the standard contractual provisions promulgated by the PDPC.

<u>Questions in relation to individuals who may act for others under the PDPA</u>

Question 1: Do you have any views/ comments on the areas for which individuals may act for other individuals under the PDPA that should be prescribed?

2.12 We have no comments in this regard.

Question 2: Do you have any views/ comments on the extent to which minors should be able to exercise rights and powers conferred on them under the PDPA?

2.13 We agree with the proposition that minors should under appropriate circumstances be allowed to exercise the rights and powers conferred on them under the PDPA, for example by giving valid consent to the collection, use and disclosure of their personal data. Certainly, we agree that minors above the age of 18 should be allowed to exercise such rights and powers.[3] However, we are of the view that the proposed caveat allowing minors between the age of 14 and 18 to exercise such rights and powers is likely to prove problematic in practice. It would be unduly onerous for organisations to prove that minors within this intermediate age group understood the nature of such rights and powers, and the consequences of exercising such rights and powers.

2.14 Nevertheless, we understand that the practical need to allow minors under 18 years of age to exercise such rights and powers, particularly since many social media and other websites collect, use and disclose personal data belonging to minors under this age. As such, we support the lowering of the minimum age at which minors can exercise rights and powers under the PDPA below 18. Organisations who wish to collect, use or disclose personal data from minors under the minimum age should be required to ensure that the parent or legal guardian of such minors agree to the relevant terms of use and privacy policy on behalf of the minor.

2.15 We recognise that minors above the stipulated minimum age could have very different levels of maturity and understanding, even among minors in the same age group. If the PDPC considers that additional safeguards are required to prevent the exploitation of minors above the minimum age but below the age where full legal capacity is assumed (i.e. 18), we suggest that instead of requiring organisations to prove that such minors understand the nature of the right or power conferred under the PDPA, and the consequences of exercising such right or power, organisations should have a positive obligation to help minors better appreciate the bargain that they are entering into. For example, organisations collecting, using or disclosing personal data of minors in the intermediate age group may be required to put in place a layered privacy notice, with an additional shorter notice summarising in a easily-comprehensible manner the main terms of the full privacy notice, and the options available to the minors to control usage of their personal data. Whether the minor fully understood the rights and powers exercised may be a relevant factor in deciding whether it would be reasonable to enforce the terms of the relevant privacy notice against the minor, but should not determine whether the consent was validly given.

Question 3: In particular, do you have any views on the minimum age below which individuals should not exercise their own rights and powers under the PDPA?

2.16 As mentioned in our response to the previous question, we agree that minors above the age of 18 should have full legal capacity to exercise the rights and powers conferred under the PDPA, but support the lowering of the minimum age below the age of 18. However, we would propose to peg the minimum age at 13 instead of 14, as proposed in the public consultation paper. In our experience, most website terms of use or privacy statements stipulate that the minimum age of users should be 13 (no doubt due to the influence of the U.S. *Children's Online Privacy Protection Act*).[4] Stipulating that only minors above the age of 14 can give valid consent for the purposes of the PDPA is likely to add an unnecessary layer of complexity due to inconsistent regulations. On the other hand, lowering the minimum age from 14 to 13 is unlikely to have a

[3] As the PDPC noted, this is consistent with the *Civil Law Act*, which gives such minors legal capacity to enter into binding contracts.

[4] We note that the position in the proposed *EU General Data Protection Regulations* is similar, in that verifiable consent must be obtained from the parent or custodian of a child under the age of 13.

great impact, since it is doubtful that minors at the age of 14 would have a much higher level of maturity and understanding than minors who are 13 years old.

2.17 As mentioned above, we are of the view that there is no need for an intermediate age group, particularly in the form as proposed in the public consultation paper. However, should the PDPC feel that it would be beneficial for additional safeguards to be put in place in relation to minors between the age of 13 and 18, we would suggest organisations collecting, using or disclosing personal data from minors in this age range should have an obligation to assist such minors to understand the organisation's data protection policies and practices. Organisations collecting, using and disclosing personal data from minors below the age of 13 should not be able to rely on consent from the minor, but should instead be obliged to seek verifiable consent from the minor's parent or legal guardian.

Question 4: Do you have any views/ comments on the proposed priority list in relation to individuals that may act for deceased individuals?

2.18 We understand that the priority list proposed would only be relevant where there is no personal representative appointed to deal with the personal data of the deceased. In the event that an executor or administrator has been appointed to deal with the assets of the deceased, we would propose that the executor or administrator should also have the power to deal with the personal data of the deceased. We note that while personal data generally cannot be distributed among the beneficiaries of the deceased, some forms of personal data could have real value (e.g. username and password granting access to a popular website belonging to the deceased), and should be treated as such.

2.19 Further, the priority list should also only be relevant where there is more than one relative who wish to be appointed to deal with the personal data of the deceased. In other words, whichever scheme of priority chosen, any relative should be able to act in relation to the personal data of the deceased, so long as none of the other relatives with a higher priority objects to his/her so acting.[5] We note that this appears to be different from how the PDPC treats the priority list, based on paragraph 9.11 of the public consultation paper. However, we believe that this flexibility would prove useful in practice, and will help organisations avoid the need to figure out which relative has the highest priority, especially where this is based on another relative with a higher priority being "unable or unwilling" to act.

Question 5: In particular, do you have any views on the appropriate priority list and/or whether priority should be given equally to all relatives (or to relatives within certain categories such as spouse and children, parents and siblings, etc) for the purposes of the PDPA?

2.20 If our comments in response to the previous question accurately capture the intention of the PDPC in specifying the levels of priority as between different relatives of the deceased, the priority list is likely to have limited application in practice. That being the case, we would prefer the second scheme of priority where relatives are aggregated into different categories. The first scheme of priority is overly complex and is likely to prove unwieldy. Further, as the PDPC pointed out, '*there may not be strong reasons to prioritise one set of relations over the other.*'

2.21 We would however propose a minor tweak to the priority list as follows:

(a) spouse or adult child including an adult child by adoption;

(b) adult grandchild or other adult descendants to the remotest degree;

[5] We note that this appears to be slightly different from how the PDPC treats the priority list based on paragraph 9.11 of the public consultation paper.

(c) parent, adult brother or sister; and

(d) other adult relation by birth or adoption.

2.22 Where a conflict arises between relatives belonging to the same category, we propose that such conflict should be resolved based on the age of the potential candidates (i.e. the older relative would have higher priority). Again, this is based on the assumption set out in paragraph 2.19 above, which is that there should be nothing preventing the relative of lower priority from acting validly in respect of the personal data of the deceased, unless one of the relatives with higher priority objects. For example, as between the spouse of the deceased and an adult child, it is likely that the adult child would be in a better position to understand the rights and powers conferred under the PDPA, even though the spouse of the deceased would of course be older and have higher priority. The adult child should be able to act in respect of the personal data of the deceased without having to prove that the spouse of the deceased is unwilling or unable to act.

3. CONCLUSION

3.1 We hope that the above comments would prove useful to the PDPC in undertaking further review of the Proposed Regulations.

3.2 Please note that while the above comments are submitted by the author on behalf of the firm, they do not reflect the position adopted by any of the firm's clients. Responsibility for any error in this submission remains with the author.