RESPONSE TO THE MINISTRY OF INFORMATION, COMMUNICATIONS AND THE ART'S CONSULTATION PAPER ON THE PROPOSED PERSONAL DATA PROTECTION BILL

CONTACT PERSONS:

Mr Lam Chung Nian
d: +65 6416 8271
e: chungnian.lam@wongpartnership.com

Mr Jeffery Lim
d: +65 6416 8250
e: jeffrey.lim@wongpartnership.com

WONGPARTNERSHIP LLP
One George Street
#20-01
Singapore 049145
Tel: + 65 6416 8000
Fax: +65 6532 5711/+65 6532 5722
Email: contactus@wongpartnership.com
Website: www.wongpartnership.com

CONTENTS

SUMMARY OF MAJOR POINTS

1. The terms "collection" and "processing" require clarification.

2. The scope of liability for the conduct of the intermediary (its mandate by an instructing party) could be clarified, particularly with references to concepts of agency law.

3. The linkages with how the PDPA is to interact with other legislation could be clarified. For example, whether defences currently available to a network service provider under the Electronic Transactions Act in relation to the PDPA are to still apply and which Act would defer.

4. It is suggested that Part III of the PDPA be either migrated to guidelines, or revised as a defence. As currently drafted, smaller organisations may not be in a position to take on the cost of compliance.

5. The requirement of appropriateness of purposes in relation to the collection of personal data should be removed.

6. In relation to disclosure, it is currently not clear whether anonymised personal data would be subject to the requirement of consent.

7. Where disclosure is permitted under any other sector specific legislation, the PDPA should similarly permit collection, use and disclosure regardless of whether consent has been obtained.

8. The terms "legal obligation" and "frustrate" in section 18(5) should be clarified.

9. Section 22(4) excludes employment data from the exceptions in the Third to Fifth Schedules. This exclusion should be pared down as the exceptions continue to be needed in certain situations.

10. The requirement to provide access to and correction of personal data should be subject to additional safeguards to ensure that individuals do not abuse their rights.

11. The exclusion for business contact information should be extended to the entire record and not just the information itself.

12. The framework of penalties and enforcement under the PDPA should contain additional safeguards such as minimal threshold limits before enforcement may be initiated, removal of personal liability for officers, and limits on the right of private action.

13. The effect of registering a number on the DNC registry should be clarified, in particular, with regard to prior consents and previously collected data.

COMMENTS

1. INTRODUCTION

1.1. We are grateful for this opportunity to present our views on the Proposed Personal Data Protection Bill set out in the Consultation Paper issued by the Ministry of Information, Communications and the Arts. This paper aims to raise certain issues which, we respectfully submit, could assist in clarifying the manner in which the proposed Act would be implemented and points of general significance. Should the Ministry wish to clarify any points made herein, we would be happy for the further opportunities to engage in further dialogue.

1.2. In this response, the following terms have the following meanings:

(a) **Consultation Paper**: Consultation Paper issued by the Ministry of Information, Communications and the Arts on the Proposed Personal Data Protection Bill

(b) **DNC**: Do-Not-Call

(c) **DPA**: The United Kingdom Data Protection Act 1998

(d) **DPC**: Data Protection Commission

(e) **DP Officer**: An individual appointed to ensure compliance with the PDPA pursuant to section 13(3) of the PDPA.

(f) **ETA**: Electronic Transactions Act (Cap. 88, Rev. Ed. 2011)

(g) **MICA**: Ministry of Information, Communications and the Arts

(h) **NSP**: network service provider

(i) **PDPA**: The proposed draft Personal Data Protection Bill

(j) **PDPO**: The Hong Kong Personal Data (Privacy) Ordinance

2. CLARIFICATION OF CONCEPTS AND DEFINITIONS

2.1. The draft PDPA uses a number of terms which are not defined in the proposed Bill but for which the public could, in our view, benefit from further refinement or guidance. Similarly, we respectfully submit that certain definitions and their related concepts could also benefit from additional guidance within the Act. This section will address these concepts and definitions at a glance.

"Collection"

2.2. The PDPA does not currently define "collection" or its cognates.

2.3. We seek clarity on whether the concept of "collection" or "collecting" under the PDPA also covers scenarios where access to data is subsequently made available to a company.

"Collection" of information in its plain meaning can include an assembling together or gathering of that information.

2.4. For example, Company A using a flight reservation system into which data is collected from customers, feeds the information the system database for determining availability of seats on flights operated by Company B. Company B's system uses the information to assign a seat, and connects the passenger information to a passenger record for the purposes of creating a reservation record and issues the confirmation to Company A.

2.5. We note that in this case, Company B has, in its system database, a composite of all data collected by companies such as Company A (e.g., travel agents). Since the data is procured from customers by A, but fed to B by A, would this amount to "collection" by B? Or does the concept of collection involve an act of procurement of the information from the data subject? Company B has no direct relationship with the consumer, nor does it have control over whether Company A and the like procure relevant / adequate consents. Accordingly, it will therefore not be in a position to comply with the requirements of the PDPA.

2.6. It is suggested that to deal with this "collecting" could be defined to include the notion of an act of procurement from the data subject by or on behalf of the party said to be "collecting".

"Processing"

2.7. The term "processing" in the PDPA has been defined, in relation to personal data, as "the carrying out of any operation or set of operations in relation to the personal data, and includes any of the following:

"(a) recording;

"(b) holding;

"(c) organisation, adaptation or alteration;

"(d) retrieval;

"(e) combination;

"(f) transmission; or

"(g) erasure or destruction;"

2.8. We note that the definition is inclusive, and hence the enumerated items are not exhaustive of what would constitute "processing". We seek clarity on whether the concept of "processing" will encompasses mere analytical usage of information where a purely analytical and limited executor functions are encompassed.

2.9. For example, in the flight reservation system outlined above, Company B has essentially been given information to secure a seat on a flight. To do so, it must analyse the data to determine whether there are available seats, and if not, produce alternatives. The data would include passenger details and proposed flight plans. Company B then issues the results to Company

A. Company B may arguably have only "processed" the data and therefore be only a "data intermediary" in this respect.

2.10. It is not clear, however, given how the term is defined, that this would amount to "processing". Insofar as Company B executes these functions on behalf of Company A (and in this sense, shares a secondary support role to the business of Company A), the analytical and function of executing a booking would seem compatible with the concept of an "intermediary". It is suggested that it is not unreasonable, given this limited role, for Company B to be regulated as a data intermediary.

2.11. We would suggest that the term "processing" include the "analysis" of data.

"Data Intermediary" & Principal-Agency Liability

2.12. Section 4(3) provides that an organisation is liable for personal data processed by data intermediary on its behalf.

2.13. Whilst this position is consistent with the approach take under section 51(2) of the bill, ie. that a data intermediary, as an agent of its instructing party (the "I.P."), would be doing no more than carrying out the activities of the I.P. for which the I.P. must remain liable, we do note that the scope of the I.P.'s liability is not limited to the scope of the mandate of agency or instructions given to the data intermediary. Hence, if a data intermediary were to exceed the scope of its agency, it would not be just for an I.P. to be penalised for such conduct. We respectfully submit therefore that the PDPA should provide for a clear limitation on the scope of liability of the I.P. both under sections 4(3) and 51(2), to exclude situations where the data intermediary has acted outside the scope of its agency or mandate / instructions. Perhaps explicit recognition that these provisions do not alter and are meant to operate within the existing legal framework of principal-agency relationships, or further refinement for factual situations in Guidelines to be issued, could be catered for.

2.14. We note that in practice, the range of potential parties who fall under the role of "data intermediary" for the purposes of the PDPA may vary from intra-group company sharing of data (eg. shared resources models), to professional arms' length service provider arrangements (eg, outsourced arrangements). We respectfully submit that there should be some recognition of this variety of situations that an organisation may act as an "intermediary" in one capacity in one situation (eg. where it processes information solely for the purposes of meeting a request by the I.P.), and act in a different capacity in another situation (eg. where it acts on the information given to provide an additional service to the third party outside of the scope of its engagement such as in value-added services etc).

3. SECTION 4(7) – LINKAGES GENERALLY WITH OTHER LEGISLATION

3.1. In other parts of this paper, we have discussed further the interface between the PDPA and the Banking Act, as this is an area we feel merits particular mention the relevant sections. This section addresses generally some conceptual issues in connection with section 4(7) of the PDPA.

3.2. We recognize and welcome section 4(6) of the PDPA which indicates that nothing shall "affected any right or privilege conferred" under other written law. We do note however, that the word "defences" is not included and we query whether the omission is intentional. Other

legislation may have expressly provided a defence to address sector-specific issues which may have subsisted and worked well within the scope of the matters for which they have been addressed and it may be helpful to clarify that such defences do continue to apply.

Section 26 of the Electronics Transactions Act (Cap 88)

3.3. To take an example, it is suggested that the position of a NSP under the PDPA requires clarification, in particular, with respect to how the ETA is to apply in the context of the PDPA.

3.4. Currently, the ETA sets out a general defence of NSPs in section 26. The NSP defence applies where the NSP "merely" provides "the necessary technical means by which third-party material may be accessed and includes the automatic and temporary storage of the third-party material for the purpose of providing access" (section 26(3) of the ETA) and recognises the roles that NSPs play as a "conduit" for content.

3.5. However, this defence is stipulated to not affect:

"(b) the obligation of a network service provider as such under a... regulatory regime established under any written law;

"(c) any obligation imposed under any written law.... to ... block or deny access to any material".

3.6. Accordingly, where an NSP comes under an obligation under the PDPA in respect of data where it is acting as a conduit, the ETA would seem to suggest that the provisions of the PDPA would apply. It would, however, not be feasible for an NSP to ensure compliance with the PDPA in respect of the data of third parties. While the PDPA seems to seek to address this, the provisions could be made clearer and rationalised with the wording of the ETA:

(a) Under the PDPA, the obligations in Parts III to VI (except for section 26) do not apply to a data intermediary in respect of personal data processed by the data intermediary on behalf of another organisation. A "data intermediary" is in turn defined as "an organisation which processes personal data on behalf of another organisation", while processing includes, among other actions, the retrieval, combination, or transmission of data. There is some correlation between the concept of an NSP and with the concept of a data intermediary. However, there is no express indication that the two are the same.

(b) The PDPA itself provides that "[t]o the extent that any provision of this Act is inconsistent with any provision of other written law, the provision of the other written law shall prevail" (section 4(7) of the PDPA). Since both the ETA and the PDPA defer to other written law, it is not clear which would or should prevail.

3.7. In view of this, we propose that a clarification confirming that the PDPA does not affect the defence under section 26 of the ETA be included.

"Inconsistencies"

3.8. We also note that section 4(7) refers to "inconsistencies" between other laws and the PDPA, and we recognise that there may well be an inherent difficulty in making a comparison

between the provisions of the PDPA with the other provisions, given that the purpose and scope of other provisions may vary and be context-specific for which a judgment must be made as to whether there is an "inconsistency" when the provisions of the PDPA are concerned. In this regard, we would be grateful for clarification as to whether additional certainty will be provided by further Guidelines which address these overlaps.

4. OBLIGATIONS UNDER PART III OF THE PDPA

4.1. It is suggested that a matter of statutory drafting and construction, Part III of the PDPA might be removed. This is not to suggest that the obligations set out therein not be set out in some form. However, setting out such obligations as statutory obligations implies that there would be a statutory duty to comply, and hence, the tort of breach of statutory duty might arise in respect of any breaches.

4.2. In terms of the mischief targeted by the PDPA, it would not seem to matter whether an organisation has internal policies and processes to address data protection so long as it in fact complies with the requirements imposed. Furthermore, by mandating the development of policies, practices, and procedures, Part III appears to impose positive one-size-fits-all obligations on all organisations affected by the PDPA regardless of its size or complexity, and regardless of whether the circumstances of such organisations necessitate this. Smaller organisations, in particular, would be hard pressed to comply with the formalised requirements set out in Part III, and on a practical level, the need for such policies, practices, and procedures may not needed. For example, an organisation with only one or two individuals would not need to develop formal procedures in order to ensure that the obligations of the PDPA are met. It is suggested that the manner of ensuring compliance with the PDPA is a matter to be best left to the organisation to be determined in accordance with its own organisational culture, set-up, resources, and needs.

4.3. Insofar as Part III is intended to encourage the development of best practices, it is suggested that the following alternatives be considered:

(a) The obligations in Part III may set out in guidelines. Such an approach would afford greater flexibility to organisations seeking to comply with these new obligations, and at this nascent stage of implementation of the PDPA would allow more time for adaptation and the evolution of on-the-ground solutions.

(b) Rather than mandate the development and establishment of internal policies, practices, and procedures, it is suggested that the PDPA provide that where there is a breach of the requirements of the PDPA, it is a defence if the organisation can establish the reasonable policies, practices, and procedures have been developed implemented and that the breach occurred despite the policies, practices, and procedures in place. In this regard, we note that a similar approach has adopted in the Securities and Futures (Amendment) Act 2009 in relation to corporate liability for insider trading committed by its officers or employees. It is suggested that section 51(3) of the PDPA be amended to include similar wording.

5. COLLECTION, USE AND DISCLOSURE OF PERSONAL DATA

Collection and Use of Personal Data

5.1. Section 20(a) of the PDPA provides, inter alia, that "an organisation may collect … personal data only for purposes that a reasonable person would consider appropriate in the circumstances".

5.2. It is suggested that there is no policy reason to impose such a requirement in addition to the requirement for consent (section 15) and notification of purpose (section 20(b)). For example, a lifestyle magazine may require details of the individual's name and address for subscription purposes, and may also ask for additional information as to the individual's socio-economic background or likes and dislikes. It will be difficult for an organisation to determine whether the request for such personal data is, on an objective basis, appropriate or not under the circumstances. So long as an individual is clearly given the choice whether to provide the information, and is willing to do so, there should be no policy need to impose any additional mandatory legal restriction on the organisation's ability to collect that information.

5.3. Similarly, and as a related point, if an individual is willing to provide blanket consent for the use and disclosure of his personal data for any purpose whatsoever, there should be no further requirement to require notification in respect of use and disclosure that falls outside the purposes initially notified. This will reduce the regulatory burden and cost on organisations while at the same time individuals will continue to have a safeguard in the form of the ability to withdraw consent.

Disclosure of Personal Data

5.4. Sections 15 and 22 set out obligations to obtain consent for disclosure and notification of the purpose of disclosure of personal data. It is not clear, however, whether personal data that has been provided or disclosed on an anonymised basis is still regarded as personal data for the purposes of the two sections. From the perspective of the provider of the information, it would continue to meet the definition of "personal data" as it would still be in a position to identify the person concerned from that data and other information to which it has access. From the perspective of the recipient of the information, it should not be regarded as "personal data" as it does not have the means to determine the identity of the individual from the data.

5.5. The mischief which the PDPA is aimed, with respect to the provision or disclosure of personal data, is, among other things, the sale of personal data to third parties for marketing or other commercial purposes. However, if the data is anonymised, the mischief does not arise. It is suggested that either of the following amendments be considered:

(a) As sections 15 and 22 do not currently draw a distinction between the provider and the recipient of the data as to whether the data is personal data and hence subject to the obligations under sections 15 and 22, the sections could be amended to make this clearer.

(b) The definition of "personal data" could be amended to expressly exclude information that does not refer to a specific individual.

5.6. Section 18(5) states, in respect of a withdrawal of consent for disclosure of personal data, that an individual "may not withdraw consent if withdrawing the consent would frustrate the performance of a legal obligation". For completeness and for the avoidance of doubt, it is suggested that the reference to "legal obligation" be amended to cover all legal, contractual, and equitable obligations. We would suggest the following wording: "any obligation arising under any laws, regulations, notices, or codes and whether legal, contractual or equitable in nature".

5.7. In addition, it is suggested that the term "frustrate" may construed as a term of art and refer to the test of frustration under contract law, which sets a very high standard to be met. If this is not the intent, it suggested that the term "frustrate" be amended to "prevent or be contrary to".

Where Collection, Use and Disclosure of Personal Data Is Governed by Other Sector-Specific Requirements

5.8. The Third Schedule of the Banking Act (Cap. 19, Rev. Ed. 2008) sets out various circumstances in which a bank may disclose information without seeking customer consent to such disclosure. Unlike the PDPA, the Banking Act does not distinguish between collection, use and disclosure. The Third to Fifth Schedules do not currently deal with this.

5.9. It is suggested that where the law already governs the disclosure of personal data or customer information, its collection, use and disclosure should not require any further consents to be given under the PDPA. It is therefore suggested that the Third to Fifth Schedules include a further exception for collection, use and disclosure pursuant to and in accordance with any written law, notice, or direction.

Personal Data in Relation to Employment Relationships: Section 22(4)

5.10. Under section 22(4) an organisation must, on or before collecting, using or disclosing the personal data about an individual for the purpose of managing or terminating an employment relationship between the organisation and that individual, inform the individual of that purpose. This requirement applies notwithstanding the carve-outs in respect of the situations enumerated in the Third to Fifth Schedules. However, certain of these carve-outs should still continue to apply:

(a) The Third Schedule (Collection of Personal Data without Consent) allows for personal data to be collected without consent if, among other things, it is available to the public from a prescribed source (paragraph 1(c)), the collection is necessary for any investigation (paragraph 1(f)), or for prescribed evaluative purposes (paragraph 1(h)). However, as the Third Schedule does not apply in a section 22(4) situation, the collection of personal data of an employee under such circumstances would still need to be notified to the employee. It would be unnecessarily restrictive to the management of human resources if the collection of such information had to be notified to an employee, in particular if it concerned an investigation for the purposes of termination or for the evaluation of the employee for internal purposes.

(b) The Fifth Schedule (Disclosure of Personal Data without Consent) provides a carve-out where disclosure is for the purpose of a business acquisition (paragraph 1(s)). Accordingly, it would seem that an organisation would be required to disclose to its employees the news of an impending acquisition before it is finalised especially as

such an acquisition would in law involve the termination of their employment contracts with the target business and rehiring by the acquiror. This would be unfeasible. If the organisation is a listed company or is a subsidiary of a listed company, it should further be noted that notification as to a possible acquisition (if not already in the public domain) may well violate rules in the Listing Manual on selective disclosure of price sensitive information. It is suggested that the business acquisition exception should continue to apply to such personal data and section 22(4) should be amended correspondingly.

6. ACCESS TO AND CORRECTION OF PERSONAL DATA

6.1. Obligations for provision of access to and correction of personal data are currently imposed only on the organisation. While the Sixth and Seventh Schedule do set out exclusions from the obligation to provide access to and correction of personal data, including requests that are burdensome or vexatious (paragraph 1(k) of the Sixth Schedule) there is no actual obligation on individual to ensure that they act reasonably in making such requests.

6.2. It may be useful to consider the position in other jurisdictions as to the requirement to provide access to and correction of personal data.

6.3. In Hong Kong, the protection of personal data is governed by the PDPO. This contains the following features with respect to access to and correction of personal data:

(a) An organisation may refuse to comply with a data access request in the following situations:

(i) Where the organisation is not supplied with such information as it may reasonably require in order for it to be satisfied as to the identity of the requestor;

(ii) Where the request is not in writing in the English or Chinese language, the organisation is not supplied with such information as it may reasonably require to locate the personal data to which the request relates, and the request follows two or more similar requests made by the individual who is the data subject in respect of personal data to which the request makes, and it is unreasonable in all the circumstances for the data user to comply with the request;

(iii) Where the commissioner has specified that the access request should be made in a particular form, and the request has not been made according to that form.

(b) Individuals who provide false or misleading information to organisations in a data access request are subject to penalties.

6.4. In the United Kingdom, the DPA contains provisions dealing with access to and correction of personal data:

(a) An organisation is not obliged to supply any information in response to an access request unless the request is made in writing and such fee as it may require has been paid.

(b) An organisation is also not obliged to comply with the access request unless it is supplied with further information, where it reasonably requires such further information in order to satisfy itself as to the identity of the person making the access request and to locate the information which that person seeks, and has informed him of this requirement.

(c) The obligation to provide the data subject with a copy of the personal data being processed need not be complied with if the supply of such a copy would involve disproportionate effort or is not possible, or the data subject agrees otherwise.

6.5. It is suggested that some of these features should be adopted in the PDPA in order to provide a balance between the needs and interests of individuals and organisations. In particular, we feel that the following features should be considered for inclusion:

(a) Individuals should be provided with an option to 'opt-out' of the access and correction rights. Since the concept of consent in relation to collection, use and disclosure under the PDPA is subject to the principles of proportionality and there is also a right for consent to be withdrawn, individuals' interests would still be served if this right of consent can be extended to non-access of personal data.

(b) Procedures for making a request for access to or correction of personal data should be included, and organisations should be entitled to refuse access or correction if these procedures are not complied with.

(c) Where verification of the individual's identify cannot reasonably be carried out, organisations should have the right to deny access or reject any request for correction by the requestor.

(d) There should be some form of penalty for individuals who persistently make vexatious or frivolous requests.

6.6. It is suggested that the requirement to provide an individual with information as to the ways in which his personal data has been used by the organisation is unnecessarily onerous and burdensome. It would require organisations to keep track of each individual's record and to note when and how the record has been used or to whom it has been disclosed to bearing in mind the constant data exchange that takes place on a daily basis in any organisation.

7. BUSINESS CONTACT INFORMATION: SECTION 4(5)(B)

Section 4(5)(b) currently provides that Parts V and VI of the PDPA do not apply to business contact information included in a document or record produced in the course, and for the purposes, of the individual's employment, business or profession. It is suggested that the exclusion should extend to the document or record itself rather than only the information in the document or record.

8. IMPOSITION OF PENALTIES

8.1. Where an organisation breaches a provision of the PDPA, it and its officers face potential liability under a wide range of penalties and remedies:

(a) Financial penalties of up to SGD 1 million;

(b) Offences for certain wilful acts;

(c) Personal liability of officers of organisations; and

(d) Rights of private action under the PDPA.

8.2. In addition, the DPC will have extensive powers of investigation, and further, whistle-blower protections have also been introduced in the PDPA (section 57).

8.3. The stringency and range of remedies and penalties is inconsistent both with existing norms in Singapore in relation to other acts of misconduct, as well as equivalent legislation overseas in respect of data protection. It is further suggested the misconduct in relation to data protection is, on a holistic view, not so egregious an act as to merit such levels of punishment. In this respect, we would suggest that there should be greater correspondence between the gravity of the wrong and the punishment to be meted out.

Current Norms in Equivalent Singapore Statutes

8.4. Only the most serious forms of misconduct have, to date, merited a similar stringent and multifarious regime of penalties. These have included offences of corruption, insider trading, and money-laundering, each of which have a significant impact on the stability of Singapore's financial system and government. A breach of data protection rules, while undoubtedly important, is not as potentially threatening to the stability Singapore society as these other offences.

8.5. Other regulatory frameworks that deal with obligations of confidentiality of personal data do not impose penalties or liabilities as stringent or as heavy the proposed range of penalties and liabilities under the PDPA. The Banking Act, for example, which imposes strict requirements as to banking secrecy, does not provide for as heavy or as wide-ranging a set of penalties for breach of the same.

Current Norms in Other Data Protection Regimes

8.6. Unlike data privacy regimes overseas, what is also conspicuously absent is any threshold of materiality before liability for breaches of the PDPA arises.

8.7. Under the DPA, prior to the imposition of a monetary penalty, the commissioner serves an 'enforcement notice' on the organisation specifying such steps that must be taken by the organisation to rectify any contravention of the data protection principles. Furthermore, a test is built into the statute to ensure that an enforcement notice is only served where the commissioner considers that 'the contravention has caused or is likely to cause any person damage or distress'.

8.8. Further, monetary penalties are only imposed if the commissioner is satisfied that:

(a) there has been a 'serious contravention' of the data protection principles;

(b) the contravention was of the kind likely to cause substantial damage or substantial distress; and

(i) the contravention was deliberate; or

(ii) the organisation knew or ought to have known that there was a risk that the contravention would occur and that the contravention would be of a kind likely to cause substantial damage or substantial distress but failed to take reasonable steps to prevent the contravention.

8.9. In addition to the above, the organisation has also been conferred express rights of appeal against the commissioner's decisions.

8.10. Similar provisions are found in the Hong Kong PDPO.

8.11. We would also highlight that the statutory right of private action does not appear as such in the data protection legislations of major countries, including the UK, Hong Kong and Australia.

8.12. For example, in the UK, there are limits to claims for compensation, e.g., the data controller had taken such care as in all the circumstances was reasonably required to comply with the requirement concerned. Distress is only claimable where the individual has suffered damage or there was processing for special purposes. In Hong Kong, a claim for compensation must relate, whether in whole or in part, to personal data of which that individual is the data subject, and further, it is a defence to show that such care as in all the circumstances was reasonably required to avoid the contravention concerned had been taken; or an any case where the contravention concerned occurred because the personal data concerned were inaccurate, the data accurately record data received or obtained by the data user concerned from the data subject or a third party.

8.13. Clearly, therefore, there is no established norm that there must be a private right of action for privacy-related breaches as such, and hence we suggest that there should be such a right of action, particularly given that the PDPA will be a new regime.

Imposition of Financial Penalties

8.14. As with Hong Kong and the UK, it is suggested that the PDPA provide for minimum thresholds to be met before financial penalties may be imposed. In addition considering the requirements set by the UK and Hong Kong, we would suggest that financial penalties should only apply:

(a) Where there are repeated offences or the potential for the same;

(b) When notice for compliance has been given and there was flagrant and deliberate breach of the notice;

(c) Where there are numerous complaints.

8.15. In addition, the DPC should be given the powers to review or reconsider the corrective measures that an organisation may have taken and for the framework to allow an organisation to submit a request for reconsideration or review where the organisation feels aggrieved by any act, direction or decision of the DPC. In this way, it ensures that the enforcement process is flexible and fluid, and that there is an avenue for the DPC to address concerns that the corrective measures are unnecessary, burdensome or unduly broad.

Personal Liability of Officers

8.16. Section 13 requires that an organisation must appoint one or more "individuals" to ensure that the organisation complies with the PDPA. However, an organisation is not thereby relieved of its obligations under the PDPA. Furthermore, it is not clear as to the extent to which these individuals will have personal liability for breaches under the PDPA.

8.17. Section 13(6) merely states that the designation of an individual by an organisation shall not relieve the organisation of any of its obligations under the PDPA, but it is also noted that under section 50, "officers" of a body corporate (which is broadly defined to mean "any director, partner, member of the committee of management, 30 chief executive, manager, secretary or other similar officer of the body corporate and includes any person purporting to act in any such capacity") may be personally liable if they are found to have committed an offence under the PDPA knowingly or further, and unusually, there was "neglect" on the part of the officer.

8.18. Would the individual designated under section 13(3) be treated as an officer within the meaning of section 50? Further, the defence available to employees under section 51(3) does not apply to any employee who "was in a position to make or influence a decision regarding that act or conduct" (section 51(4)), and it would seem that a DP Officer would in a majority of cases fall within this exclusion. If so, as a practical matter, it will be difficult to engage any person who would be willing to undertake the role of such an officer since there would be a high risk of personal prosecution.

8.19. This concern is also compounded when one also considers that it is rare that corporate officers are subject to personal prosecution for negligence in relation to corporate acts in Singapore. For example, under section 157(1) read with section 157(3) of the Companies Act (Cap. 50, Rev. Ed. 2006), only a director (and not officers in general) is subject to personal prosecution where he has failed to act "honestly and use reasonable diligence" (and this imposes a higher standard of care than mere negligence). The punishment for such offences is a maximum fine of $5,000 or imprisonment for up to 12 months.

8.20. Under the Penal Code (Cap. 224, Rev. Ed. 2008), persons are at risk of prosecution for negligence only in very specific circumstances (see eg Part XIV). The closest analogy may perhaps be drawn with section 336, where an offence is created where a person "does any act so … negligently as to endanger human life or the personal safety of others", but even so, it is punishable "with imprisonment for a term which may extend to 3 months, or with fine which may extend to $1,500, or with both".

8.21. Further, the offence under the PDPA attracts "a fine not exceeding $10,000 or to imprisonment for a term not exceeding 3 years or to both and, in the case of a continuing offence, to a further fine not exceeding $1,000 for every day or part thereof during which the

offence continues after conviction", which is a far more severe punishment than for the existing offences relating to negligence discussed above.

8.22. It is suggested that introducing such personal liability for officers for PDPA offences is disproportionate and this concept should be removed from the PDPA. The severe financial penalties which may be imposed will already ensure that organisations will take their PDPA obligations seriously, and further, it is open to organisations to dismiss or take other steps against employees who have exposed the organisation to such prosecution without the need to further legislate for this.

Rights of Private Action

8.23. We would firstly suggest that it is unnecessary to provide for rights of private action as the common law already provides remedies for breach of confidence.

8.24. If, however, it is considered necessary to provide for such rights, we would suggest that these rights be given subject to certain limitations and safeguards already in use in other regulatory regimes:

(a) Much like there are groundless threats actions in various intellectual property statutes in Singapore to deter groundless claims of infringement, there should be a corresponding provision in the PDPA to punish individuals who make frivolous and vexatious complaints against organisations. This will help to ensure that private individuals will not "try their luck" with litigation.

(b) There should also be a limitation period within which complaints which may be brought by individuals against the organisation for alleged contraventions of the law – this should also be short, say no later than one year after the breach, having regard to the huge amounts of audit trails that corporations may need to maintain to defend against any potential complaints which may surface in the future.

(c) Civil proceedings may not be commenced against an organisation where the DPC has determined that no enforcement is necessary or where enforcement proceedings against the organisation have determined in the organisation's favour. In addition, where the DPC has commenced proceedings against the organisation, civil proceedings may not be commenced or must be stayed until the conclusion of enforcement proceedings. In this regard, we note that the Securities and Futures Act (Cap. 289, Rev. Ed. 2006) sets out similar limitations on the bringing of civil proceedings for market misconduct.

9. WITHDRAWAL OF CONSENT & PLACEMENT OF NUMBER ON THE DNC REGISTER

9.1. Section 44 of the PDPA allows a subscriber to add his Singapore telephone number to the DNC register. It is suggested that the effect of doing so in relation to telephone numbers previously provided by the subscriber should be clarified, in particular, whether this act works to negate all previous consents to the use of the subscriber's number (including contacting the subscriber for marketing purposes).

9.2. For example, on Day 1, Person A gives express permission to Company C to make marketing calls to Person A on his phone. On Day 2, Person A registers his number on the DNC registry.

On Day 3, Company C scrubs the list of numbers to call against the DNC list and finds that Person A's number has been removed from Company C's call list.

9.3. It is not clear whether Company C may ignore the DNC registry and proceed to call Person A based on the prior consent. Under section 18, a person can withdraw his consent to the use of his personal data by an organisation by giving "reasonable notice to the organisation". This suggests that the only way that a person can remove himself from an organisation's marketing list is to provide the organisation directly with a notice of withdrawal. However, it may be argued that an organisation receives such a notice of withdrawal if it scrubs a telephone call list against the DNC register and obtains a deletion of the consumer's phone number despite having obtained prior consent.

9.4. A similar argument may be made in respect of previously collected data under section 21 of the PDPA (i.e., data collected prior to the appointed day). In addition, in the context of such data, there may have been consents attached to such collected data for which, again, the mere placement of a number on the DNC registry should not be permitted to operate as an effective withdrawal.

9.5. For clarity, it is suggested that the PDPA include a provision stating that previously issued consents to call (or other use of data) will not be deemed to be withdrawn by the mere placement of a number by a subscriber on the DNC registry.

WongPartnership LLP
30 April 2012