PUBLIC CONSULTATION ISSUED BY THE PERSONAL DATA PROTECTION COMMISSION

PROPOSED REGULATIONS ON PERSONAL DATA PROTECTION IN SINGAPORE

5 FEBRUARY 2013

Part I: INTRODUCTION AND OVERVIEW

1 Introduction

1.1 This Consultation Paper seeks views from the public on the positions proposed for regulations to be made under the Personal Data Protection Act 2012 ("Regulations").

1.2 The Personal Data Protection Act 2012 ("PDPA") establishes a new data protection law in Singapore which governs the collection, use and disclosure of individuals' personal data by organisations. The Personal Data Protection Commission (the "Commission") is established under the PDPA with the key roles, amongst others, of promoting awareness of data protection in Singapore and administering and enforcing the PDPA.

1.3 Various sections of the PDPA provide for matters that may be prescribed by way of regulations to supplement the operation of the provisions of the PDPA. Among others, regulations may provide for:

a) the form, manner and procedures for making and responding to requests for access to or correction of personal data, including the period for such responses;

b) the requirements to be complied with by organisations for the transfer of personal data out of Singapore;

c) the classes of persons who may act for minors or other individuals who lack capacity to act and the manner in and extent to which any rights and powers of individuals under the PDPA may be exercised;

d) procedural and administrative matters such as the form, manner and procedures relating to applications and complaints to the Commission;

e) the form, manner and procedure for appeals to an Appeal Committee under the PDPA;

f) the composition of offences under the PDPA; and

g) various matters relating to the operation of the Do Not Call registry.

1.4 It is envisaged that issues (a) to (d) mentioned above will be contained in the Personal Data Protection Regulations. Issues (e), (f) and (g) are standalone matters and are likely to be contained in separate Regulations. This public consultation focuses on the positions relating to issues (a) to (c) above, which are the areas where organisations would require clarity as they adjust their processes in preparation for the substantive provisions of the PDPA coming into force. Issues (d) and (e) relate to processes that may be required after the data protection rules come into force, likely in mid 2014, may be prescribed at a later stage. Regulations to prescribe that offences under the PDPA will be compoundable will also be made (i.e. item (f) above). In addition, the Commission expects to consult on the regulations governing the processes for the Do Not Call registry (i.e. item (g) above) around mid-2013.

2 Overview of the PDPA

2.1 The PDPA governs the collection, use and disclosure of individuals' personal data by organisations in a manner that recognises both the right of individuals to protect their personal data and the need of organisations to collect, use and disclose personal data for purposes that a reasonable person would consider appropriate in the circumstances. The PDPA contains two main sets of provisions, covering data protection and the Do Not Call registry, which organisations are required to comply with.

2.2 The PDPA's data protection obligations are set out in Parts III to VI of the PDPA (the "Data Protection Provisions"). In brief, the Data Protection Provisions deal with the following matters:

a) Having reasonable purposes, notifying purposes and obtaining consent for collection, use or disclosure of personal data;

b) Allowing individuals to access and correct their personal data;

c) Taking care of personal data, which relates to ensuring accuracy, protecting personal data (including protection in the case of transfers) and not retaining personal data if no longer needed; and

d) Having policies and practices to comply with the PDPA.

2.3 The PDPA provides a number of exceptions to various Data Protection Provisions to address situations where organisations may have a legitimate need, for example, to collect, use or disclose personal data without consent or to refuse to provide an individual with access to his personal data. The PDPA's Do Not Call registry provisions are set out in Part IX of the PDPA (the "Do Not Call Provisions"). These deal with the establishment of Singapore's national Do Not Call registry (the "Do Not

Call Registry") and the obligations of organisations relating to the sending of certain marketing messages to Singapore telephone numbers.

PART II: ADMINISTRATION OF REQUESTS FOR ACCESS TO AND CORRECTION OF PERSONAL DATA

3 How organisations should respond to access and correction requests

3.1 Under Part V of the PDPA (which comprises sections 21 and 22 of the PDPA, extracted at **Annex A** for reference), individuals have the rights to obtain access to and request for correction of their personal data held by an organisation.

3.2 In particular, section 21 of the PDPA requires an organisation to respond to the request of an individual for access to personal data about the individual that is in the possession or under the control of the organisation (an "**access request**"). This will allow individuals to find out what personal data organisations have about them and how organisations have used or disclosed the personal data in the immediate preceding year.

3.3 Section 22 of the PDPA allows an individual to request an organisation to correct an error or omission in the individual's personal data (a "correction request"). This will enable the individual to ensure that the data used by the organisation is correct and updated.

3.4 Under the PDPA, an organisation is required to respond to an access request as soon as reasonably possible, subject to the exceptions in sections 21(2), (3) and (4). Section 21(2) refers to the list of exceptions in the Fifth Schedule of the PDPA (extracted at **Annex A**) for which an organisation is not required to provide access, such as opinion data kept solely for an evaluative purpose, examination results (prior to their release), personal data kept by an arbitral institution for the purpose of an arbitration, personal data collected, used or disclosed under the PDPA for an investigation if the investigation and associated proceedings are not yet completed, requests for information that is trivial or otherwise frivolous or vexatious.

3.5 Under section 21(3), an organisation is prohibited from providing access to personal data that can threaten the safety or physical or mental health of another individual, cause immediate or grave harm to the safety or physical or mental health of the individual making the request, reveal another individual's personal data, or that is contrary to national interest. In addition under section 21(4), an organisation is prohibited from informing the individual if his personal data has been disclosed to a law enforcement agency for an investigation or proceedings or under any other written law. However, if an organisation is able to provide an individual with his personal data and other information requested without the personal data that is subject to exceptions noted above, the organisation should provide the requesting individual with access to his personal data and other information without the data or information excluded under sections 21(2), (3) and (4).

3.6 Similarly, an organisation is required to make a correction requested in a correction request unless it is satisfied on reasonable grounds that the correction should not be made, or unless exceptions apply. An organisation is not required to correct an opinion (including a professional or expert opinion), or make corrections in the situations listed in the Sixth Schedule of the PDPA (extracted at **Annex A**). These include corrections to, amongst others, examinations, examination scripts and examination results (prior to their release), personal data of beneficiaries of private trusts kept solely for the purpose of administering the trust, personal data kept by an arbitral institution for the purposes of an arbitration and a document related to a prosecution if all proceedings relating to the prosecution have not yet been completed.

3.7 In relation to how an organisation responds to an access or a correction request, it is proposed that these Regulations will provide that:

a) An organisation shall make a reasonable effort to respond to an individual who makes an access request or a correction request as accurately and completely as possible. Where the organisation is required to provide the personal data requested for (in accordance with section 21 of the PDPA), the organisation shall make a reasonable effort to provide the individual with the personal data requested (which is in the possession or under the control of the organisation), or if the personal data cannot be provided, a reasonable opportunity to examine the data;

b) In relation to the obligation of an organisation under section 21(1) of the PDPA to provide the requested personal data as soon as reasonably possible, organisations will be required to provide the requested personal data:

i. within 30 days of the individual's request; or

ii. if it is not reasonably possible to provide the requested personal data within 30 days of the individual's request, by the reasonably soonest time. The organisation must inform the individual of when that reasonably soonest time will be within 30 days of the individual's request.

4 How access and correction requests should be made by individuals

4.1 In relation to how an individual makes an access request or a correction request, it is proposed that these Regulations will provide that an individual may make an access request or a correction request in writing or through any other manner accepted by the organisation and shall include sufficient details to enable the organisation to which the request is made to identify the individual and the personal data or correction he seeks under section 21 or 22.

5 Minimal fee for access request

5.1 Organisations shall be entitled to charge an individual who makes an access request a minimal fee to recover the incremental costs directly related to the request for the time and effort spent by the organisation in responding to the access request. Such incremental costs do not include costs that are normally incurred in capital purchases, for example purchasing new equipment in order to provide access to the requested personal data. In addition, the fee should be proportionate to the time and effort required to respond to the request. While the minimal fee may differ depending on, for example, the extent and type of personal data requested in an access request, some international data protection authorities have given guidance on what would constitute a minimal fee.

5.2 For example, in the guide to the Personal Information Protection Act of British Columbia[1] in Canada, it is stated that "Minimal means that what you charge must cover only the actual costs you incurred in producing the record. Typically, a minimal charge would include costs associated with locating, retrieving and producing a document, preparing it for disclosure, shipping it, and providing a copy of the document. Charging for services not required to create documents, such as the creation of an index for the documents, is not a minimal charge."

[1] "A Guide to B.C.'s Personal Information Protection Act for Businesses and Organizations", April 2012 (4th Publication).

5.3 If the individual concerned is required to pay a fee for the organisation to respond to his request, the organisation shall be required to provide the individual with a written estimate of the fee at the point when the request is made, or before providing the individual access to his personal data. The organisation is entitled to require a deposit in the amount determined by the organisation, provided that such deposit shall not exceed the total estimated fee required from the individual. In the event the deposit exceeds the fee payable by the individual for access to his personal data, the organisation shall refund the excess payment received.

5.4 If an individual does not agree to pay the fee or the deposit, the organisation shall not be required to provide access to the individual's personal data until the individual agrees to pay the fee or pays the deposit required. Where the individual disputes the fee required by the organisation, he may apply to the Commission to review the fee under section 28(1) of the Act, and the fee amount will be determined by the Commission under section 28(2) of the Act.

6 Key considerations in relation to the administration of access and correction requests

6.1 The proposed requirements on organisations and individuals in relation to making and responding to access and correction requests were formulated to ensure that organisations make a reasonable effort to respond to an access request or a correction request as accurately and completely as possible save for the exclusions specified in section 21(4) of the PDPA and paragraph 1(h) of the Fifth Schedule to the PDPA, while recognising that organisations may incur costs as a result of the time and effort spent to respond to such requests.

6.2 At the same time, the Commission considered the need for both organisations and individuals to be accorded with some flexibility in determining the manner in which to make or respond to an access or correction request. Particularly, in relation to the form of the access request or correction request, the Commission notes that while organisations may offer standard forms or procedures for individuals to submit access and/or correction requests to the organisation, organisations should also accept requests that are made in writing or by any other manner accepted by the organisation (with the required details) even if they do not comply with the standard forms offered by the organisation. However, the Commission also recognises that where an individual decides not to use the standard forms and procedures made available by an organisation, this may increase the time (and possibly, the effort) required for an organisation to respond to a request.

6.3 In relation to the time frame for organisations to respond to the individual, the Commission notes that some jurisdictions like the UK[2] and Canada's Personal Information Protection and Electronic Documents Act ("**PIPEDA**")[3] prescribe a time frame within which the organisation is required to respond to the individual. To strike a balance between giving a prompt response to the individual and cases where organisations may require a significant amount of time to prepare the requested data, these proposed Regulations provide that if organisations are unable to respond within 30 days of the request, they must inform the individual of the reasonably soonest time in which they will respond.

6.4 On the charging of fees, it is noted that the charging of fees for access requests is accepted in many jurisdictions given that organisations may incur associated costs. Some jurisdictions like the UK prescribe maximum fees chargeable[4], while others do not specify a quantitative cap. At this juncture, the Commission is not proposing to specify a maximum amount for the fees chargeable for access requests, given that it would be difficult to set a standard rate that would be applicable across the board, especially when organisations may not have existing processes to handle access and correction requests today. Rather, the prescribed principle would be that organisations will only be allowed to recover a minimal fee proportionate to the time and effort spent to respond to the access request.

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] In the case of the UK, the Data Protection Act provides that organisations should respond within 40 days of receiving the request or the required fee and the information required to fulfill the request.

[3] The Personal Information Protection and Electronic Documents Act require organisations to respond within 30 days, which may be extended under certain conditions.

[4] In the UK's case, the maximum fee is £10 for most types of access requests.

PART III: TRANSFER OF PERSONAL DATA OUTSIDE SINGAPORE

7 Requirements for transferring personal data outside Singapore

7.1 Under section 26 of the PDPA, an organisation may transfer personal data to a country or territory outside Singapore only if the organisation has complied with requirements prescribed under the PDPA to ensure that organisations provide a standard of protection to personal data so transferred that is comparable to the protection under the PDPA.

7.2 It is noted that some jurisdictions like the EU have detailed and comprehensive frameworks governing the transfer of personal data outside its jurisdiction. Specifically, the EU prohibits the transfer of personal data to another jurisdiction outside of the EU unless the European Commission has determined that the other jurisdiction offers an adequate level of protection ("**EU adequacy**"). In the absence of EU adequacy, the EU also allows for binding corporate rules, standard contractual clauses, and Safe Harbour[5] principles as other avenues of according appropriate safeguards for the transfer of personal data. Other jurisdictions such as Canada do not prescribe specific requirements on organisations.

7.3 In Singapore's context, the proposal is to allow organisations some flexibility to determine the means to provide a comparable standard of protection as the PDPA when personal data is transferred out of Singapore. At the same time, the standard of protection provided should be legally binding and should contain the appropriate safeguards.

7.4 In the case of inter-corporate transfers, it is noted that contracts may be the legally binding instrument used to provide appropriate safeguards for the personal data transferred. However, noting that contractual arrangements may not be suitable in the case of intra-corporate transfers, binding corporate rules would also be an acceptable avenue to safeguard personal data transferred overseas.

[5] A voluntary US-EU program that bridges the differences between US and EU approaches to privacy and data protection. Safe Harbour allows US companies to self-certify that they are in compliance with EU adequacy requirement.

7.5 It is proposed that these Regulations provide that organisations intending to transfer personal data to a country or territory outside Singapore may only do so in a manner consistent with their obligations under the other provisions of the PDPA (i.e. other than section 26) and pursuant to a legally binding instrument that contains the appropriate safeguards in the form of contractual clauses or binding corporate rules. In either case, the legally binding instrument shall contain provisions that implement the following obligations (where applicable, in a manner consistent with the other obligations of the transferring organisation under the PDPA):

a) *Purpose*: The receiving organisation shall not use or disclose transferred personal data for any purpose other than the purposes specified in the instrument (and such purposes shall be consistent with the purposes for which the transferring organisation may use and disclose the personal data in accordance with the PDPA);

b) *Use and disclosure*: The receiving organisation shall only use and disclose transferred personal data in a manner and to the extent permitted in the instrument (and such use and disclosure shall be consistent with the ability of the transferring organisation to use and disclose the personal data in accordance with the PDPA);

c) *Accuracy*: The receiving organisation shall make a reasonable effort to ensure that the transferred personal data is accurate and complete, if the personal data is likely to be (i) used by the receiving organisation to make a decision that affects the individual to whom the transferred personal data relates; or (ii) disclosed by the receiving organisation to another organisation;

d) *Protection*: The receiving organisation shall protect the transferred personal data in its possession or under its control by making reasonable security arrangements to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks;

e) *Retention*: The receiving organisation shall cease to retain its documents containing transferred personal data, or remove the means by which the transferred personal data can be associated with particular individuals, as soon as it is reasonable to assume that (i) the specified purposes are no longer being served by retention of the transferred personal data; and (ii) retention is no longer necessary for legal or business purposes;

f) *Policies*: The receiving organisation shall ensure that its employees, agents and sub-contractors who may receive or have access to any of the transferred personal data are aware of the obligations specified under this paragraph and agree to abide by the same.

7.6 Condition (c) mentioned above will not apply in relation to a contract in writing between an organisation in Singapore and a data intermediary located in a country or territory outside Singapore, since the PDPA does not impose an obligation on data intermediaries who will be processing the transferred personal data on behalf of and for the purposes of the organisation in Singapore pursuant to a contract to ensure the accuracy of the personal data in question.

7.7 As proposed, there is no requirement for the organisation to require the receiving party to allow access to or correction of personal data that has been transferred overseas. Where the transfer is between an organisation in Singapore and a data intermediary outside Singapore, it is noted that section 4(3) of the PDPA provides that the organisation in Singapore has the same obligations under the PDPA in respect of personal data processed by its data intermediary on its behalf. Hence, individuals wishing to obtain access to or correct their personal data may continue to make access and correction requests to the organisation in Singapore. Where the transfer is between an organisation in Singapore and a third party outside Singapore, the Commission considers that it may not be practical to require foreign organisations to respond to access and correction requests in respect of the personal data transferred since they would not have direct contact with the individuals in Singapore.

7.8 For clarity, the requirements described in paragraph 7.5 will not limit any other obligation of the transferring organisation under the PDPA, or the parties to a contract from including in their contract other clauses as they consider appropriate provided that no such clause is inconsistent with the provisions required under paragraph 7.5.

Contractual clauses

7.9 Where the transfer of personal data is pursuant to a contract, contractual clauses are to be contained in a legally binding contract that is enforceable against every organisation receiving personal data under the contract.

Binding corporate rules

7.10 Binding corporate rules are internal rules (such as a code of conduct) adopted by a multinational group of companies that define its global policy with regard to the international transfers of personal data within the same corporate group to entities located in other countries.

7.11 In general, for the purposes of the PDPA, binding corporate rules are to be legally binding and applicable to and enforced by every organisation within the transferring organisation's group.

7.12 In addition to the matters noted in paragraph 7.5 above, binding corporate rules must at least specify the following:

a) the structure and contact details of the organisation's group and its members;

b) the data transfers or set of transfers, including the categories of personal data, the purposes for which personal data is being transferred, the type of individuals affected and identification of each country or territory in question;

c) their legally binding nature, both within the organisation's group and externally; and

d) the mechanisms within the organisation's group aimed at ensuring the verification of compliance with the binding corporate rules.

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?

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?

PART IV: INDIVIDUALS WHO MAY ACT FOR OTHERS UNDER THE PDPA

8 Exercise of rights and powers of individuals

8.1 Under section 14(4) of the PDPA, any consent given or deemed to have been given by an individual includes any consent given or deemed to have been given by any person validly acting on behalf of that individual. Section 65(2) of the PDPA further provides that regulations be made for, amongst other matters, the classes of persons who may act under the PDPA for minors, deceased persons or any other individuals who lack capacity to act, as well as regulating the manner in which, and the extent to which, any rights and powers of individuals under the PDPA may be exercised on their behalf. It is proposed that these Regulations address how the rights and powers of minors and other individuals under the PDPA be exercised on their behalf.

8.2 As regards how individuals generally may exercise their rights and powers under the PDPA, it is proposed that these Regulations provide that –

a) any right or power conferred on an individual under the PDPA may be exercised by another individual validly acting on behalf of the first individual or otherwise acting in accordance with these Regulations;

and

b) where an individual has been authorised in writing by another individual to act on behalf of that other individual, the individual so authorised may exercise a right or power conferred on the other individual under the PDPA which falls within the scope of the authorisation given or otherwise relates to matters falling within the scope of the authorisation.

9 Minors and deceased persons

9.1 It is also proposed that these Regulations address how the rights and powers conferred on two specific classes of individuals under the PDPA may be exercised:

a) In respect of minors (that is, individuals who are below 21 years of age), in addition to existing situations where a parent or other legal guardian may exercise the rights and powers conferred on a minor under their care, it is proposed that an individual who is a minor may exercise any right or power conferred by the PDPA if the individual is –

i. 18 years of age or older[6]; or

ii. is less than 18 years of age but above 14 years of age and understands the nature of the right or power and the consequences of exercising the right or power; and

b) In respect of the personal data of deceased individuals that is protected under the PDPA (that is, for individuals who have been deceased for 10 years or less), it is proposed that the rights and powers in the PDPA relating to such personal data may be exercised by:

i. the personal representative of the deceased individual, to the extent specified in the deceased's will or otherwise to the extent required for the administration of the deceased's estate; and

ii. if there is no such personal representative, the nearest relative of the deceased individual (as described below).

Minimum age to exercise rights and powers under the PDPA

9.2 As regards minors, it is noted that in the specific context of data protection, there are likely to be situations where a minor may be capable of exercising rights and powers conferred on him under the PDPA. Limiting the age at which such individuals may exercise their rights and powers to 21 may prevent them from disclosing personal data in appropriate situations and to an appropriate extent would enable them to participate in, and benefit from, activities requiring such disclosure. At the same time, it is recognised that some minors may not understand the implications of disclosing their personal data or the consequences of exercising their rights and powers in a particular situation.

[6] This is aligned with the age prescribed in the Civil Law Act at which a minor may commence legal proceedings and enter into contracts.

9.3 As a balance, it is proposed that an individual may exercise rights and powers conferred on him under the PDPA if the individual is 18 years of age or older, or if the individual is under 18 years of age but above 14 years of age and understands the nature of the right or power and the consequences of exercising that right or power. While there is a possibility that individuals below 14 years of age may understand the nature of their rights under the PDPA, the Commission is of the view that setting a minimum age would provide greater certainty for organisations that collect, use and disclose personal data of young people as part of their business models.

9.4 On the minimum age for an individual to exercise his own rights under the PDPA, the Commission notes that there is no standard approach to determine the appropriate minimum age. Under the Children and Young Persons Act, a child is a person below the age of 14 years. Internationally, some data protection frameworks that protect the personal data of children, like the Children's Online Privacy Protection Act in the US, require verifiable parental consent to the collection, use and disclosure of personal data from individuals under the age of 13 years. The Commission welcomes views on what the minimum age should be for the PDPA, below which individuals may not exercise their own rights and powers under the PDPA.

9.5 The rights and powers conferred on minors who do not meet the criteria noted above may be exercised by their parents or other legal guardians.

Priority of nearest relatives to an individual

9.6 Given that the PDPA covers personal data of certain deceased individuals (i.e. those who have been deceased for 10 years or less), it is necessary to provide clarity on the parties who may act in relation to the personal data of deceased individuals under the PDPA. Under the PDPA, only the provisions pertaining to the disclosure of personal data and section 24 (protection of personal data) apply to the personal data of deceased individuals. That being the case, the powers conferred on parties who may act in relation to the personal data of the deceased will apply primarily to the disclosure of personal data, for example in giving or withdrawing consent for the disclosure of the personal data of the deceased. These parties are not required under the PDPA to comply with the other requirements.

9.7 It is noted that there is no standard approach to determine who may act on behalf of a deceased individual in respect of his personal data. While the property of a deceased (including documents containing personal data) may be distributed in accordance with his will or the applicable laws relating to succession, most, if not all, of the personal data of a deceased cannot be so distributed. For example, the name of the deceased (which forms part of his personal data) is not subject to distribution in this manner. Instead, any relative of the deceased may wish to refer to the deceased by name, as when referring to him as their spouse or parent.

9.8 For the purposes of the PDPA, one approach would be to establish a priority list based on the rules for distribution of the property of a deceased as prescribed in the Intestate Succession Act (Cap 146)[7]. However, it is noted that the considerations governing estates and the rights to act on behalf of a deceased individual for data protection may differ. The key consideration for protecting the personal data of a deceased in the PDPA was to mitigate the potential impact that inappropriate disclosure of the deceased's personal data may have on family members. As such, it may not be necessary for the priority accorded to individuals to follow exactly rules for distribution of a deceased's property.

9.9 As a start, it is proposed that where there is no personal representative appointed to act in relation to personal data of a deceased, the nearest relative of a deceased individual may exercise the rights and powers under the PDPA relating to the personal data of the deceased individual, where the nearest relative is determined as the first living individual[8] as determined under the following order of priority:

a) spouse;

b) adult[9] child including an adult child by adoption;

c) adult grandchild or other adult descendents to the remotest degree;

d) parent;

e) adult brother or sister;

f) adult child of a brother or sister;

---

[7] Section 7 of the Interstate Succession Act.

[8] Assuming they are of sound mind and no other legal instrument (e.g. will) overrides their authority.

[9] An adult refers to an individual above 21 years of age.

g) grandparent; and

h) other adult relation by birth or adoption.

9.10 Besides the proposed listing above, recognising that there may not be strong reasons to prioritise one set of relations over the other, another option would be to further aggregate the categories of relatives listed above and give the relatives in each category equal priority, for example as follows:

a) spouse or adult[10] child including an adult child by adoption;

b) parent, adult brother or sister, or adult grandchild or other adult descendents to the remotest degree; and

c) other adult relation by birth or adoption.

9.11 If two or more individuals share equal priority under the listings above, then priority passes to the individual who is eldest of the individuals and descend in order of age. Also, if the individual who is of the highest priority as determined in accordance with the above is unable or unwilling to make a decision concerning the exercise of the deceased individual's right or power under the PDPA, then priority shall pass to the individual who is next in priority.

9.12 While there are other cases where individuals may act for other individuals in relation to the rights and powers conferred under the PDPA, for example where an individual is mentally incapacitated, these are already governed by other existing legislation such as the Mental Capacity Act and hence will not be included in these proposed Regulations.

[10] An adult refers to an individual above 21 years of age.

<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?

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?

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?

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

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?

PART V: SUBMISSION OF COMMENTS

10 Submission of comments

10.1 The Commission would like to seek the views and comments on the proposed positions for these Regulations.

10.2 Parties that submit comments on this consultation paper should organise their submissions as follows:

a) Cover page (including particulars of the organisation and contact person);

b) Summary of major points;

c) Comments; and

d) Conclusion.

10.3 Supporting material may be placed in an Annex. All submissions should be clearly and concisely written, and should provide a reasoned explanation for any proposed revisions. Where feasible, parties should identify the specific section on which they are commenting and explain the basis for their proposals.

10.4 **All submissions should reach the Commission by 19 March 2013 (5pm)**.

Comments should be submitted:

i. in soft copy (in Microsoft Word format);
ii. with the email header “Public Consultation on Proposed Regulations on Personal Data Protection in Singapore”; and
iii. to the following e-mail address: pdpc_consultation@pdpc.gov.sg

10.5 The Commission reserves the right to make public all or parts of any written submission and to disclose the identity of the source. Commenting parties may request confidential treatment for any part of the submission that the commenting party believes to be proprietary, confidential or commercially sensitive. Any such information should be clearly marked and placed in a separate annex. If the Commission grants confidential treatment it will consider, but will not publicly disclose, the information. If the Commission rejects the request for confidential treatment, it will return the information to the party that submitted it and will not consider this information as part of its review. As far as possible, parties should limit any request for confidential treatment of information submitted. The Commission will not accept any submission that requests confidential treatment of all, or a substantial part, of the submission.

Annex A: EXTRACTS OF RELEVANT SECTIONS OF PDPA

Section 21: Access to personal data

(1) Subject to subsections (2), (3) and (4), on request of an individual, an organisation shall, as soon as reasonably possible, provide the individual with —

a) personal data about the individual that is in the possession or under the control of the organisation; and

b) information about the ways in which the personal data referred to in paragraph (a) has been or may have been used or disclosed by the organisation within a year before the date of the request.

(2) An organisation is not required to provide an individual with the individual's personal data or other information under subsection (1) in respect of the matters specified in the Fifth Schedule.

(3) An organisation shall not provide an individual with the individual's personal data or other information under subsection (1) if the provision of that personal data or other information, as the case may be, could reasonably be expected to —

a) threaten the safety or physical or mental health of an individual other than the individual who made the request;

b) cause immediate or grave harm to the safety or to the physical or mental health of the individual who made the request;

c) reveal personal data about another individual;

d) reveal the identity of an individual who has provided personal data about another individual and the individual providing the personal data does not consent to the disclosure of his identity; or

e) be contrary to the national interest.

(4) An organisation shall not inform any individual under subsection (1) that it has disclosed personal data to a prescribed law enforcement agency if the disclosure was made without the consent of the individual pursuant to paragraph 1(f) or (n) of the Fourth Schedule or under any other written law.

(5) If an organisation is able to provide the individual with the individual's personal data and other information requested under subsection (1) without the personal data or other information excluded under subsections (2), (3) and (4), the organisation shall provide the individual with access to the personal data and other information without the personal data or other information excluded under subsections (2), (3) and (4).

Section 22: Correction of personal data

(1) An individual may request an organisation to correct an error or omission in the personal data about the individual that is in the possession or under the control of the organisation.

(2) Unless the organisation is satisfied on reasonable grounds that a correction should not be made, the organisation shall —

a) correct the personal data as soon as practicable; and

b) subject to subsection (3), send the corrected personal data to every other organisation to which the personal data was disclosed by the organisation within a year before the date the correction was made, unless that other organisation does not need the corrected personal data for any legal or business purpose.

(3) An organisation (not being a credit bureau) may, if the individual consents, send the corrected personal data only to specific organisations to which the personal data was disclosed by the organisation within a year before the date the correction was made.

(4) When an organisation is notified under subsection (2)(b) or (3) of a correction of personal data, the organisation shall correct the personal data in its possession or under its control unless the organisation is satisfied on reasonable grounds that the correction should not be made.

(5) If no correction is made under subsection (2)(a) or (4), the organisation shall annotate the personal data in its possession or under its control with the correction that was requested but not made.

(6) Nothing in this section shall require an organisation to correct or otherwise alter an opinion, including a professional or an expert opinion.

(7) An organisation is not required to comply with this section in respect of the matters specified in the Sixth Schedule.

Fifth Schedule: Exceptions from Access Requirement

1. An organisation is not required to provide information under section 21(1) in respect of —

    a) opinion data kept solely for an evaluative purpose;

    b) any examination conducted by an education institution, examination scripts and, prior to the release of examination results, examination results;

    c) the personal data of the beneficiaries of a private trust kept solely for the purpose of administering the trust;

    d) personal data kept by an arbitral institution or a mediation centre solely for the purposes of arbitration or mediation proceedings administered by the arbitral institution or mediation centre;

    e) a document related to a prosecution if all proceedings related to the prosecution have not been completed;

    f) personal data which is subject to legal privilege;

    g) personal data which, if disclosed, would reveal confidential commercial information that could, in the opinion of a reasonable person, harm the competitive position of the organisation;

    h) personal data collected, used or disclosed without consent, under paragraph 1(e) of the Second Schedule, paragraph 1(e) of the Third Schedule or paragraph 1(f) of the Fourth Schedule, respectively, for the purposes of an investigation if the investigation and associated proceedings and appeals have not been completed;

    i) the personal data was collected or created by a mediator or arbitrator in the conduct of a mediation or arbitration for which he was appointed to act —

        i. under a collective agreement under the Industrial Relations Act (Cap. 136) or by agreement between the parties to the mediation or arbitration;
        ii. under any written law; or
        iii. by a court, arbitral institution or mediation centre; or

j) any request —

i. that would unreasonably interfere with the operations of the organisation because of the repetitious or systematic nature of the requests;
ii. if the burden or expense of providing access would be unreasonable to the organisation or disproportionate to the individual's interests;
iii. for information that does not exist or cannot be found;
iv. for information that is trivial; or
v. that is otherwise frivolous or vexatious.

Sixth Schedule: Exceptions from Correction Requirement

1. Section 22 shall not apply in respect of —

a) opinion data kept solely for an evaluative purpose;

b) any examination conducted by an education institution, examination scripts and, prior to the release of examination results, examination results;

c) the personal data of the beneficiaries of a private trust kept solely for the purpose of administering the trust;

d) personal data kept by an arbitral institution or a mediation centre solely for the purposes of arbitration or mediation proceedings administered by the arbitral institution or mediation centre; or

e) a document related to a prosecution if all proceedings related to the prosecution have not been completed.