CLOSING NOTE

FOR

PUBLIC CONSULTATION ISSUED BY THE PERSONAL DATA PROTECTION COMMISSION ON:

PROPOSED REGULATIONS UNDER THE PERSONAL DATA PROTECTION ACT IN SINGAPORE

16 MAY 2014

Part I

1 Background and Introduction

1.1 The Personal Data Protection Commission (the "**Commission**") launched a public consultation on 5 February 2013 on three sets of documents:

a) Advisory Guidelines on Key Concepts in the PDPA; and Advisory Guidelines on the PDPA for Selected Topics (together, "**Guidelines**"); and

b) Proposed Regulations under the PDPA ("**Regulations**").

1.2 The Regulations and Guidelines aim to give organisations and individuals greater clarity by elaborating on how the Commission will interpret specific obligations of organisations under the PDPA.

1.3 The consultation closed on 1 April 2013 with 35 responses from organisations (including business associations) representing various sectors. The majority of responses came from organisations in the Finance, Information Technology/Telecommunications and Legal/Academic sectors. Please refer to the Commission's website for the full list of respondents and their submissions[1]. The Commission thanks all respondents for their comments.

1.4 On 24 September 2013, the Commission had issued revised Guidelines which addressed comments from the consultation except in relation to the following matters:

a) The Access and Correction Obligation;

b) The Transfer Limitation Obligation; and

c) Individuals who may act for others under the PDPA.

1.5 This closing note seeks to summarise the key issues in relation to the three remaining matters above, and address common responses or queries on these issues which were raised by several respondents. Extracts of the relevant Regulations to be prescribed are also provided at **Annex A** for reference.

[1] http://www.pdpc.gov.sg/personal-data-protection-act/public-consultations/responses-received-at-1-april-2013

Part II: Overview of Key Issues

2 Avenues for transfer of personal data outside Singapore

Position consulted

2.1 Section 26 of the PDPA requires organisations to comply with requirements prescribed by the Minister that are intended to ensure a comparable standard of protection for personal data transferred overseas.

2.2 The Commission sought views on the prescription of two avenues for overseas transfer of personal data – through contracts and under Binding Corporate Rules ("**BCR**").

Feedback received

2.3 There were requests to consider other avenues for overseas transfers, especially for cases where legally binding instruments are not viable, or where legally-binding arrangements are disproportionate to the purpose of the transfer, such as for one-time transfers of personal data for specific purposes. In particular, the Commission was asked to consider allowing international transfers where (i) the individual whose personal data was transferred had consented to the transfer; or where (ii) the organisation transferring the personal data had a 'legitimate business purposes' for such transfer.

2.4 There were also suggestions for Singapore to consider accountability-based programs such as the APEC Cross Border Privacy Rules ("**CBPR**") System and to adopt the EU-style 'white list' of jurisdictions identified as having adequate safeguards.

Additional avenues for international transfer

2.5 The Commission notes the feedback that the use of contracts or BCRs may not be tenable in all circumstances. In particular, they may impose too much administrative burden on the organisation *vis-a-vis* the purpose or the frequency of the transfer. For example, it is impractical for a tour agency to enter into a contract with an overseas hotel simply so that it could transfer its customers' personal data to the hotel to enable room booking. In some cases, contracts and BCRs may also be counter-intuitive to data management norms or business practices[2]. Internationally, other jurisdictions like the UK and Australia recognise avenues for international

[2] As an illustration, small businesses that use cloud services may not have the ability or bargaining power to negotiate separate or customised contracts with cloud service providers, although there would be standard terms and conditions governing the activities of the cloud providers.

transfer apart from contracts or BCRs.

2.6 The Commission has therefore proposed that the Minister prescribe the following **avenues for international transfers of personal data.**

Self-assessment of legally enforceable obligations

2.7 Generally, personal data may be transferred to a recipient overseas where the transferring organisation has taken appropriate steps to ascertain whether and to ensure, that the recipient is bound by legally enforceable obligations to protect the personal data being transferred to a comparable standard as that accorded under the PDPA. The assessment may include consideration of factors such as any law, any contracts or binding corporate rules governing the transfer of the personal data or any other legally binding instrument. While this avenue provides more flexibility for organisations, it may also impose greater compliance risks as organisations would have to establish that they had taken appropriate steps to ensure such comparable standard of protection.

Legitimate reasons

2.8 There may be cases where **legitimate reasons for transferring personal data overseas** may exist despite the absence of the aforementioned avenues for transfer. For example, in the case of an individual who wishes to make a hotel booking in another, the PDPA does not prohibit the individual himself from providing his personal details to the overseas hotel regardless of the level of protection accorded to his personal details by the hotel. Similarly, if the individual himself requires or allows the international transfer regardless of the level of protection accorded to his personal data, for example, if an individual engages a travel agent to make the booking on his behalf, the PDPA should not oblige organisations to secure a level of protection higher than what the individual himself would accept before transferring such personal data himself.

2.9 Hence, it is also proposed that organisations may be taken to have satisfied the obligations regarding transfer of personal data outside Singapore where:

a) the individual whose personal data is to be transferred is provided a reasonable summary in writing of the extent to which the personal data to be transferred will be protected to a standard comparable to the protection under the PDPA;

b) the transfer is necessary for the performance of a contract between the individual and the organisation (including situations where the organisation is the data intermediary of the individual pursuant to a contract between them in relation to the transfer), or the transfer is done at the individual's request with a view to his entering into a contract with the organisation; or

c) the transfer is necessary to carry out or conclude a contract between the organisation and a third party entered into at the individual's request, or which a reasonable person would consider to be in the individual's interest.

Transfer of personal data in circumstances covered by a PDPA exception

2.10 Finally, the Commission has also proposed that cross-border transfers be permitted where:

a) the transfer is necessary for the personal data —

i. to be used under paragraph 1(a), (b) or (d) of the Third Schedule to the PDPA; or

ii. to be disclosed under paragraph 1(a), (b), (c), (e) or (o) of the Fourth Schedule to the PDPA,

and the organisation has taken reasonable steps to ensure that the personal data so transferred will not be used or disclosed by the recipient for any other purpose;

b) the personal data is data in transit; or

c) the personal data is publicly available in Singapore.

2.11 The purposes in sub-paragraphs a)(i) and a)(ii) pertain to situations where transfers are necessary in the individual's/national interest and for which consent has not been obtained. The purpose in sub-paragraphs b) and c) are included because it would not be reasonable for organisations to have to procure additional safeguards for personal data that is merely in transit through Singapore, or already available to the public, just because such data is being transferred overseas.

Sufficiency of existing avenues

2.12 In relation to the other avenues proposed, the Commission is assessing future participation in the APEC CBPR System as another avenue for cross-border transfer to organisations within APEC economies. On prescribing white lists of jurisdictions deemed as having comparable standards, the Commission is of the view that such an approach would be premature at this juncture. The Commission may consider such arrangements when the regime in Singapore is more mature.

2.13 Overall, the Commission is of the view that the revised list of routes by which organisations may make international transfers of personal data should suffice. Should organisations be unable to comply, they may seek an exemption of the international transfer requirements from the Commission under the PDPA for their specific circumstances.

Scope of contractual clauses

2.14 As organisations may decide to rely on appropriate contractual clauses to safeguard personal data that is transferred overseas, the Commission has considered the feedback of organisations and will also set out some guidance on the scope of contractual clauses for overseas transfers of personal data.

3 Individuals who may act for others under the PDPA

Minimum age to exercise rights and powers under the PDPA

Position consulted

3.1 The Commission sought views on the minimum age at which an individual may exercise his rights and powers under the PDPA in relation to giving consent for the collection, use and disclosure of his personal data. In the consultation, the Commission noted that international practices differed on this matter and suggested that an individual between the ages of 14 and 18 be eligible to exercise his rights under the PDPA if he understands the nature of his rights and powers ("**test of maturity**"). Individuals aged 18 and above may exercise their own rights and powers under the PDPA.

Feedback received

3.2 There were alternative suggestions for the minimum age, most notably the age of 13, so as to be in line with international norms for online activities, and 18, to be in line with the general age at which individuals may enter into contracts under the Civil Law Act (Cap. 43)[3]. In addition, industry feedback indicated a strong preference to remove the subjective test of maturity given the difficulty of determining if an individual was in fact mature. There were also queries as to whether parents have the right to override the consent given by minors with regard to the collection, use and disclosure of the minors' personal data.

Minimum age threshold

3.3 As noted in the consultation paper, international practices on when minors may exercise their own rights under data protection laws vary. For example, the Children's Online Privacy Protection Act ("**COPPA**") in the US requires certain organisations to obtain verifiable parental consent to collect personal data from children under 13 years old.

3.4 Similarly, a review of local legislation also reveals a range of ages at which minors may conduct different types of activities on their own or are accorded certain legal protections. For example:

a) the Civil Law Act provides that contracts entered into by minors who are at least 18 years of age generally have effect as if they were of full age;

[3] Section 35 of the Civil Law Act provides that most types of contracts entered into by a minor who has reached 18 years of age shall have effect as if he were of full age (that is, 21 years of age). This does not apply to certain contracts relating to land, interests in trusts and settlement of legal proceedings and claims in respect of which he is still regarded as a minor pursuant to any written law.

b) the Employment Act (Cap. 91) defines a child as one below 15 years of age and a young person as one between 15 and 16 years of age[4] for the purposes of according varying protections in respect of the different age groups and also provides for the general rule that a child 13 years of age or older may be employed in light work suited to his capacity in a non-industrial undertaking[5]; and

c) the Children and Young Persons Act (Cap. 38) defines a child as one who is below 14 years of age and a young person as one that is between 14 and 16 years of age for purposes of according varying protections under that Act.[6]

3.5 The Commission understands that the applicable test under English common law for when a minor can consent on his own behalf in matters relating to medical treatment (and several other areas)[7] would be the *Gillick* test. In brief, the *Gillick* test sets out that a minor may provide consent if he has sufficient understanding and intelligence to enable him to understand fully what is proposed. To-date, the *Gillick* test has not yet been adopted into Singapore law[8].

3.6 Nevertheless, the Commission is of the view that organisations should generally consider whether a minor has sufficient understanding of the nature and consequences of giving consent, in determining if he can effectively provide consent on his own behalf for purposes of the PDPA. The Commission notes that the age threshold of 13 years appears to be a significant one in relation to according protection to minors. The Commission also notes that, as a practical matter, organisations may already have policies or practices that take into account regulations or norms providing for an age threshold of 13 years in relation to consent. Bearing the above in mind, the

---

[4] Employment Act, section 67A.

[5] Employment Act, section 68(3).

[6] Children and Young Persons Act, section 2.

[7] While the holding in *Gillick v West Norfolk and Wisbech Area Health Authority* [1986] AC 112 may be argued to only apply narrowly in the context of consenting to medical treatment and advice, later UK cases have applied the *Gillick* principle to other areas. For instance, it was applied in determining if a minor was able to make a decision on divulging information about herself to the press. The Commission is however not aware of any UK cases which expressly applies the *Gillick* principle in the context of UK's data protection laws and in particular, in determining whether a minor can consent to the sharing of his personal data.

[8] To-date, there are no Singapore cases that have expressly applied *Gillick*, whether in the context of a minor consenting to receiving medical treatment, or in any other context. It therefore remains an open question whether or not the Singapore court will find the *GIllick* principle to have any relevance in determining whether a minor can exercise his legal rights, especially in the context of Singapore's own data protection framework.

Commission will adopt the practical rule of thumb that a minor who is at least 13 years of age would typically have sufficient understanding to be able to consent on his own behalf. However, the Commission would advise an organisation to obtain consent from an individual who is able to provide consent on a minor's behalf, if it has reason to believe or it can be shown that the minor does not have sufficient understanding of the nature and consequences of giving consent. The Commission would also advise organisations to take appropriate steps to ensure that the minor can effectively give consent on his own behalf in light of the circumstances of the particular case, including the impact on the minor in giving consent.

3.7 For avoidance of doubt, Parts III to VI of the PDPA do not affect any legal rights or obligations under other laws. Accordingly, whether a minor can give consent would be determined in accordance with any applicable legislation or the common law. Further, the Commission's position does not affect any right of a parent or legal guardian of a minor to exercise any right or power conferred on the minor under the PDPA on behalf of the minor. Thus, if a parent or legal guardian is empowered to provide consent or refusal on behalf of a minor, an organisation should generally rely on such consent or refusal given by the parent or legal guardian.

Priority of nearest relative to deceased individual

Position consulted

3.8 The Commission proposed two options in relation to the priority list for determination of the nearest relative (i.e. the first living individual[9]) where there is no personal representative appointed to act in relation to personal data of a deceased:

a) The first option set out the following order of priority:

i. spouse;

ii. adult[10] child including an adult child by adoption;

iii. adult grandchild or other adult descendents to the remotest degree;

iv. parent;

v. adult brother or sister;

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

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

vi. adult child of a brother or sister;

vii. grandparent; and

viii. other adult relation by birth or adoption.

b) The second option was to further aggregate the categories of relatives listed above and give the relatives in each category equal priority, for example as follows:

i. spouse or adult child including an adult child by adoption;

ii. parent, adult brother or sister, or adult grandchild or other adult descendents to the remotest degree; and

iii. other adult relation by birth or adoption.

Feedback received

3.9 Between the two options, the first was preferred by respondents who expressed a preference. There were also other suggestions, such as keeping close to the order specified in the Intestate Succession Act, requiring family members of a deceased individual to obtain a court order, or requiring the representative of a deceased individual to produce a Grant of Probate or Grants of Letters of Administration.

Adoption of revised priority list

3.10 Having considered the variety of opinions, the Commission is of the view that a priority list is still necessary to facilitate action by parties in relation to personal data of deceased individuals under the PDPA. However, the Commission recognises that there could be scope for simplifying the priority list. The Commission will thus adopt a revised version of the first option that covers only more 'immediate' relationships. The following order of priority will be prescribed in the Regulations:

a) spouse (at the time of the deceased individual's death);

b) legitimate, legitimated or adopted child;

c) parent;

d) brother or sister including a brother or sister by adoption; and

e) other relation by birth or adoption.

3.11 Generally, if there is more than one individual in a particular category, the priority shall pass to the oldest individual in that category, and descend among the individuals in that category in order of age.

3.12 For avoidance of doubt, this priority list will not affect any right or power conferred on the personal representative of a deceased individual by or under the individual's will or by law.

4 The Access and Correction Obligation

4.1 The Commission consulted on the manner in which individuals may make access or correction requests and how organisations are to respond to such requests. The key issues on which feedback was received, and the Commission's response, are set out below.

Scope and level of detail of information required

Feedback received

4.2 Several respondents asked for more guidance on the scope and level of detail of information required when responding to an access request.

Information required

4.3 If an individual requests information relating to the use or disclosure of his personal data by an organisation, the organisation is only required to provide information relating to how the personal data has been or may have been used or disclosed within the past year.[11] An organisation may develop (and update periodically) a standard list of all possible third parties to which personal data may have been disclosed, and provide that standard list to individuals who request for information relating to how the personal data has or may have been disclosed. Generally, in responding to a request for the organisations to whom personal data has been disclosed, organisations should individually identify each possible third party, instead of simply providing general categories of organisations (e.g. "pharmaceutical company ABC" as compared to "pharmaceutical companies") to which personal data has been disclosed to. This would allow individuals to directly approach the third party organisation to which his personal data has been disclosed. The actual response to be given may, of course, depend on the specific request.

[11] For avoidance of doubt, an organisation is not required to provide such information in response to an access request where an exception in the Fifth Schedule to the PDPA applies. Examples of exceptions include requests if the burden or expense of providing access would be unreasonable to the organisation or disproportionate to the individual's interests; and requests for information that does not exist or cannot be found.

4.4 Organisations should note that the obligation to provide access applies equally to personal data captured in unstructured forms such as personal data embedded in emails. Organisations are generally required to implement processes to keep track of the collection, use, and disclosures of all personal data under their control, including unstructured data. Exceptions to the obligation to provide access will equally apply to personal data in unstructured forms, such as if the access request is frivolous or vexatious, or if the burden or expense of providing access would be unreasonable to the organisation or disproportionate to the individual's interest.

4.5 The Commission notes that organisations which receive access requests soon after the data protection rules come into force on 2 July 2014 may not necessarily have put in place systems to appropriately capture how personal data has been used prior to 2 July 2014. The Commission acknowledges that since the transition period was given for organisations to prepare themselves to comply with the PDPA, organisations should not be expected to have captured information on how personal data might have been used during the transition period. The Commission will bear this in mind when determining whether any organisation has complied with an access request in the first year following 2 July 2014 and the directions to be issued if there is any non-compliance. The Commission will generally also consider whether the organisation has acted reasonably to respond to an access request and whether an exception applies[12]. The Commission would likely consider an organisation which receives an access request in the first year following 2 July 2014 to have fulfilled the Access Obligation, if the organisation has acted reasonably and made a best effort attempt to respond to an access request.

Fees chargeable for access requests

Position consulted

4.6 The Commission sought views on allowing organisations to charge a minimal fee for access requests to recover incremental costs directly related to the request, and for the time and effort spent by the organisation in responding to the access request. Organisations are not allowed to charge for correction of personal data required under section 22 of the PDPA.

[12] For example, paragraph 1(j)(iii) of the Fifth Schedule provides for an exception relating to any request for information that cannot be found.

Feedback received

4.7 Some organisations commented that organisations should be allowed to recover capital costs or the 'real' costs of allowing individuals to access their data, such as the costs of installing IT systems to facilitate responses to access requests. There were also several calls for prescribing a standard minimum, maximum, or range of fees that organisations can charge for fulfilling access requests.

Considerations for setting fees

4.8 The Commission considers that the costs incurred by organisations to respond to access requests in general should not be passed on to individuals making a particular access request, since these would include costs that are necessarily incurred for the organisation to comply with the PDPA regardless of whether an access request was actually made. For example, organisations might need to put in place systems to better classify the personal data in their custody to facilitate compliance with the PDPA and the obligation to provide access. However, the Commission recognises that there are incremental costs associated with responding to individual access requests, such as the cost of making physical copies of the personal data requested. Organisations may opt to recover all or a portion of such incremental costs by way of a fee.

4.9 In relation to the setting of a benchmark fee, i.e. an actual dollar amount that would be a reference point for organisations, the Commission maintains the view that it would be difficult to take a one-size-fits-all approach and set a standard fee at this juncture, especially with insufficient information about the operational realities that organisations may face when responding to access requests. However, the Commission does not rule out providing further guidance on fees chargeable for access requests if necessary in the future with more operational information from organisations.

Part IV

5 Conclusion

5.1 The Commission will continually assess the need to issue guidelines in future on other topics to facilitate understanding and compliance of the PDPA obligations. The Commission notes that some sector-specific issues have been raised through the consultation and other avenues and has worked with different sectoral regulators and representatives to develop sector-specific guidelines.

5.2 There are other resources available to organisations apart from guidelines issued by the Commission. Organisations should visit www.pdpc.gov.sg for more information on the following:

- How to contact the Commission for general queries
- Answers to Frequently Asked Questions
- Briefing sessions and workshops conducted by the Commission to help organisations gain further insights into the requirements of the PDPA
- The Commission's informal guidance process

5.3 This closing note should be read in conjunction with the finalised Advisory Guidelines and Regulations. Once again, the Commission thanks all respondents for their comments and participation in this public consultation.

Annex A

Extracts of the Regulations to be Prescribed

PART II

REQUESTS FOR ACCESS TO AND CORRECTION OF PERSONAL DATA

Definitions of this Part

2. In this Part, unless the context otherwise requires —

"applicant" means an individual who makes a request;

"data protection officer", in relation to an organisation, means an individual designated by the organisation under section 11(3) of the Act or an individual to whom the responsibility of the data protection officer has been delegated under section 11(4) of the Act;

"individual's personal data" means personal data about the individual;

"request" means a request made by an individual to an organisation under section 21(1) or 22(1) of the Act;

"use and disclosure information" means the information specified in section 21(1)(b) of the Act.

How to make request

3.—(1) A request must be made in writing and shall include sufficient detail to enable the organisation, with a reasonable effort, to identify —

(a) the applicant;

(b) in relation to a request under section 21(1) of the Act, the personal data and use and disclosure information requested by the applicant; and

(c) in relation to a request under section 22 of the Act, the correction requested by the applicant.

(2) A request must be sent to the organisation —

(a) in accordance with section 48A of the Interpretation Act (Cap.1);

(b) by sending it to the organisation's data protection officer in accordance with the business contact information provided under section 11(5) of the Act; or

(c) in such other manner as is acceptable to the organisation.

Duty to respond to request under section 21(1) of Act

4.—(1) Subject to section 21(2), (3) and (4) of the Act and regulations 6 and 7(3), an organisation must respond to each request under section 21(1) of the Act as accurately and completely as necessary and reasonably possible.

(2) The organisation must provide an applicant access to the applicant's personal data requested under section 21(1) of the Act —

(a) by providing the applicant a copy of the personal data and use and disclosure information in documentary form;

(b) if sub-paragraph (a) is impracticable in any particular case, by allowing the applicant a reasonable opportunity to examine the personal data and use and disclosure information; or

(c) in such other form requested by the applicant as is acceptable to the organisation.

Notification of timeframe for response

5. Subject to the requirement to comply with section 21(1) of the Act as soon as reasonably possible or section 22(2) of the Act as soon as practicable, if the organisation is unable to comply with that requirement within 30 days after receiving a request made in accordance with regulation 3, the organisation must within that time inform the applicant in writing of the time by which it will respond to the request.

Refusal to confirm or deny existence, use or disclosure of personal data

6. Subject to section 21(4) of the Act, an organisation may, in a response to a request under section 21(1) of the Act, refuse to confirm or deny —

(a) the existence of personal data referred to in paragraph 1(h) of the Fifth Schedule to the Act; or

(b) that the personal data has been used without consent under paragraph 1(e) of the Third Schedule to the Act or disclosed without consent under paragraph 1(f) of the Fourth Schedule to the Act, for any investigation or proceedings, if the investigation or proceedings and related appeals have not been completed.

Fees

7.—(1) Subject to section 28 of the Act, an organisation may charge an applicant who makes a request under section 21(1) of the Act a reasonable fee for services provided to the applicant to enable the organisation to respond to the applicant's request.

(2) An organisation must not charge a fee to respond to the applicant's request under section 21(1) of the Act unless the organisation has —

(a) provided the applicant with a written estimate of the fee; and

(b) if the organisation wishes to charge a fee that is higher than the written estimate provided under sub-paragraph (a), notified the applicant in writing of the increased fee.

(3) An organisation does not have to respond to an applicant's request under section 21(1) of the Act unless the applicant agrees to pay the following fee:

(a) where the organisation has notified the applicant of an increased fee under paragraph (2)(b) —

(i) if the Commission has reviewed the increased fee under section 28(1) of the Act, the fee allowed by the Commission under section 28(2) of the Act;

(ii) if sub-paragraph (i) does not apply, the increased fee notified under paragraph (2)(b); or

(b) where sub-paragraph (a) does not apply and the organisation has provided the applicant with an estimated fee under paragraph (2)(a) —

(i) if the Commission has reviewed the estimated fee under section 28(1) of the Act, the fee allowed by the Commission under section 28(2) of the Act;

(ii) if sub-paragraph (i) does not apply, the estimated fee provided under paragraph (2)(a).

(4) For the avoidance of doubt, an organisation shall not charge the applicant any fee to comply with its obligations under section 22(2) of the Act.

PART III

TRANSFER OF PERSONAL DATA OUTSIDE SINGAPORE

Definitions of this Part

8. In this Part, unless the context otherwise requires —

"data in transit" means personal data transferred through Singapore in the course of onward transportation to a country or territory outside Singapore, without the personal data being accessed or used by, or disclosed to, any organisation (other than the transferring organisation or an employee of the transferring organisation acting in the course of the employee's employment with the transferring

organisation) while the personal data is in Singapore, except for the purpose of such transportation;

"individual's personal data" means personal data about that individual;

"recipient", in relation to personal data transferred from Singapore to a country or territory outside Singapore, means any organisation that receives in a country or territory outside Singapore the personal data transferred to it by or on behalf of the transferring organisation, but does not include —

(a) the transferring organisation;

(b) any employee of the transferring organisation acting in the course of the employee's employment with that organisation;

(c) any organisation that received the personal data solely as a network service provider or carrier; or

(d) any organisation that received the personal data from a recipient of that personal data;

"transferring organisation" —

(a) in relation to any personal data transferred from Singapore to a country or territory outside Singapore, means the organisation that transfers the personal data from Singapore to the country or territory outside Singapore; or

(b) in relation to data in transit, means the organisation that transfers the personal data through Singapore to the country or territory outside Singapore;

"transportation" includes transmission in electronic form.

Requirements for transfer

9.—(1) For the purposes of section 26 of the Act, a transferring organisation must, before transferring an individual's personal data to a country or territory outside Singapore —

(a) take appropriate steps to ensure that it will comply with Parts III to VI of the Act, in respect of the transferred personal data while it remains in the possession or under the control of the transferring organisation; and

(b) if that personal data is transferred to a recipient in a country or territory outside Singapore, before transferring the individual's personal data, take appropriate steps to ascertain whether and to ensure that the recipient of the personal data is bound by legally enforceable obligations (in accordance with regulation 10) to provide to the transferred personal data a standard of protection that is at least comparable to the protection under the Act.

(2) A transferring organisation is taken to have satisfied the requirements of paragraph (1)(a) in respect of the transferred personal data while it remains in the possession or under the control of the transferring organisation if the personal data is —

(a) data in transit; or

(b) publicly available in Singapore.

(3) A transferring organisation is taken to have satisfied the requirements of paragraph (1)(b) in respect of an individual's personal data which it transfers to a recipient in a country or territory outside Singapore if —

(a) subject to paragraph (4), the individual consents to the transfer of the personal data to the recipient in that country or territory outside Singapore;

(b) the transfer of the personal data to the recipient is necessary for the performance of a contract between the individual and the transferring organisation, or to do anything at the individual's request with a view to the individual entering into a contract with the transferring organisation;

(c) the transfer of the personal data to the recipient is necessary for the conclusion or performance of a contract between the organisation and a third party which is entered into at the individual's request;

(d) the transfer of the personal data to the recipient is necessary for the conclusion or performance of a contract between the organisation and a third party if a reasonable person would consider the contract to be in the individual's interest;

(e) the transfer of the personal data to the recipient is necessary for the personal data to be used under paragraph 1(a), (b) or (d) of the Third Schedule to the Act or disclosed under paragraph 1(a), (b), (c), (e) or (o) of the Fourth Schedule to the Act, and the organisation has taken reasonable steps to ensure that the personal data so transferred will not be used or disclosed by any recipient for any other purpose;

(f) the personal data is data in transit; or

(g) the personal data is publicly available in Singapore.

(4) An individual is not taken to have consented to the transfer of the individual's personal data to a country or territory outside Singapore if —

(a) the individual was not, before giving his consent, given a reasonable summary in writing of the extent to which the personal data to be transferred to that country or territory will be protected to a standard comparable to the protection under the Act;

(b) the organisation required the individual to consent to the transfer as a condition of providing a product or service, unless the transfer is reasonably necessary to provide the product or service to the individual; or

(c) the organisation obtained or attempted to obtain the individual's consent for the transfer by providing false or misleading information about the transfer, or by using other deceptive or misleading practices.

(6) Nothing in this Part prevents an individual from withdrawing any consent given for the transfer of the personal data to a country or territory outside Singapore.

Legally enforceable obligations

10.—(1) For the purposes of regulation 9(1)(b), legally enforceable obligations include obligations imposed on the recipient under —

(a) any law;

(b) any contract in accordance with paragraph (2);

(c) any binding corporate rules in accordance with paragraph (3); or

(d) any other legally binding instrument.

(2) A contract referred to in paragraph (1)(b) must —

(a) require the recipient to provide to the personal data transferred to the recipient a standard of protection that is at least comparable to the protection under the Act; and

(b) specify the countries and territories to which the personal data may be transferred under the contract.

(3) The binding corporate rules referred to in paragraph (1)(c) —

(a) must require every recipient of the transferred personal data, that is related to the transferring organisation and does not already satisfy paragraph (1)(a), (b) or (d), to provide to the personal data transferred to the recipient a standard of protection that is at least comparable to the protection under the Act;

(b) must specify —

(i) the recipients of the transferred personal data to which the binding corporate rules apply;

(ii) the countries and territories to which the personal data may be transferred under the binding corporate rules; and

(iii) the rights and obligations provided by the binding corporate rules; and

(c) may only be used for recipients that are related to the transferring organisation.

(4) For the purposes of paragraph (3)(a) and (c), a recipient is related to the transferring organisation if —

(a) the recipient, directly or indirectly, controls the transferring organisation;

(b) the recipient is, directly or indirectly, controlled by the transferring organisation; or

(c) the recipient and the transferring organisation are, directly or indirectly, under the control of a common person.

PART IV

GENERAL

Exercise of rights under Act in respect of deceased individual

11.—(1) The persons specified in paragraph (2) may exercise the following rights in relation to section 24 of the Act (protection of personal data) or any provision of the Act relating to the disclosure of personal data, in respect of a deceased individual who has been dead for 10 years or fewer:

(a) the right to give or withdraw any consent for the purposes of the Act;

(b) the right to bring an action under section 32 of the Act;

(c) the right to bring a complaint under the Act.

(2) The following persons are specified for the purposes of paragraph (1):

(a) a person appointed by the deceased individual's will to exercise the right referred to in paragraph (1) or a personal representative of the deceased individual, unless the person or personal representative (as the case may be) has renounced the grant of such right; or

(b) if no person or personal representative referred to in sub-paragraph (a) is able to exercise such right or power, the deceased individual's nearest relative determined in accordance with the First Schedule.

(3) Subject to Part II of the Probate and Administration Act (Cap. 251) (if applicable), the renunciation of the grant of any right under paragraph (1) must be made expressly in writing.

(4) Any notice or other communication to be given under the Act concerning any consent, action or complaint referred to in paragraph (1) may be given to the person who may exercise the right related to that consent, action or complaint under paragraph (1).

(5) This regulation does not

(a) enable any person to exercise any right under paragraph (1) if that person is legally incapable of exercising such a right on that person's own behalf; or

(b) affect the authority of any person under any other law to exercise any right referred to in paragraph (1).

(6) A person does not cease to be a personal representative for the purposes of this regulation merely because that person has completed the administration of the deceased individual's estate.

FIRST SCHEDULE

Regulation 11(2)(b)

DETERMINATION OF NEAREST RELATIVE

1. Subject to paragraphs 2 and 3, the nearest relative of a deceased individual is the first living individual in the following order of priority:

(a) the deceased individual's spouse at the time of death;

(b) the deceased individual's child;

(c) the deceased individual's parent;

(d) the deceased individual's brother or sister;

(e) other relation of the deceased individual.

2. For the purposes of paragraph 1 —

(a) a reference to a deceased individual's child means a legitimate, legitimated or adopted child of the deceased individual;

(b) a reference to a deceased individual's brother, sister or relation includes, respectively, a brother, sister or relation of the deceased individual by adoption; and

(c) there shall be no distinction between those who are related to a deceased person through the father or the mother of the deceased person.

3. If 2 or more individuals share equal priority under paragraph 1, then the individual who is the elder shall have priority over the younger.

4. If the individual who is determined in accordance with this Schedule to be the nearest relative of the deceased individual —

(a) dies;

(b) is legally incapable of exercising the right referred to in regulation 11(1); or

(c) is unable or refuses to make a decision concerning the exercise of the right referred to in regulation 11(1),

the individual who is next in priority to the first-mentioned individual is regarded as the next nearest relative of the deceased individual.

5. For the purposes of this Schedule, an individual shall not be considered to be unable or to have refused to make a decision referred to in paragraph 4(c) merely due to a temporary inability or temporary unavailability to make such a decision.