PUBLIC CONSULTATION ISSUED BY THE PERSONAL DATA PROTECTION COMMISSION

PROPOSED ADVISORY GUIDELINES ON KEY CONCEPTS IN THE PERSONAL DATA PROTECTION ACT

05 FEBRUARY 2013

PART I: INTRODUCTION AND OVERVIEW 6

1 Introduction 6

2 Overview of the PDPA 6

PART II: IMPORTANT TERMS USED IN THE PDPA 9

3 Definitions and related matters 9

4 Individuals 9

5 Personal data 10

Data about an individual 10

True and false personal data 11

Identifying an individual 12

Personal data relating to more than one individual 14

Excluded personal data 14

Business contact information 15

Personal data of deceased individuals 16

6 Organisations 17

Excluded organisations 18

Individuals acting in a personal or domestic capacity 19

Individuals acting as employees 19

Public agencies and organisations acting on behalf of public agencies 19

Data intermediaries 20

Obligations of data intermediaries 20

Considerations for organisations using data intermediaries 21

Determination of who the data intermediary is 21

“Agents” who may be data intermediaries 24

7 Collection, use and disclosure 24

8 Purposes 25

9 Reasonableness 26

Part III THE DATA PROTECTION PROVISIONS 27

10 Overview 27

11 The Consent Obligation 29

Obtaining consent from an individual 30

Obtaining consent from a person validly acting on behalf of an individual 31

When consent is not validly given 31

Deemed consent 34

Obtaining personal data from third party sources with the consent of the individual 36

Obtaining personal data from third party sources without the consent of the individual 38

Withdrawal of consent 39

Exceptions to the Consent Obligation 42

Publicly available data 42

12 The Purpose Limitation Obligation 45

13 The Notification Obligation 46

When an organisation must specify its purposes 48

The manner of stating purposes and obtaining consent 48

Verbal notification and consent 49

Form of stating purposes/obtaining consent 50

Providing Notification through a Data Protection Policy and/or Online 52

Information to be included when stating purposes 53

Use and disclosure of personal data for a different purpose from which it was collected 54

14 The Access and Correction Obligation 55

Access to personal data 55

Exceptions to the obligation to provide access to personal data 57

Correction of personal data 60

Exceptions to the obligation to correct personal data 62

15 The Accuracy Obligation 62

16 The Protection Obligation 65

17 The Retention Limitation Obligation 68

Retention of personal data 68

Ceasing to retain or anonymising personal data 70

18 The Transfer Limitation Obligation 71

19 The Openness Obligation 71

PART IV: OTHER RIGHTS, OBLIGATIONS AND USES 74

20 Overview 74

21 Existing rights, etc under law 75

22 Other written law 75

23 Use of personal data collected before the appointed day 76

PART V: THE DO NOT CALL PROVISIONS 79

24 Overview 79

25 Locations of sender and recipient 80

26 Meaning of “specified message” 81

27 Exclusions from the meaning of “specified message” 83

28 Business to Business (“B2B”) marketing messages 85

29 Meaning of “sender” 85

30 Exclusions 87

31 Sending a specified message to a Singapore telephone number 88

32 Duty to check the Do Not Call Register 89

33 Obtaining consent for sending messages to Singapore telephone numbers 90

Clear and unambiguous consent 90

Consent evidenced in written or other form 91

Consent given before the prescribed day 91

Withdrawal of consent 92

No withdrawal by subsequent registration with the Do Not Call Registry 92

Other obligations relating to consent 93

34 Duty to identify the sender of a message 93

PART I: INTRODUCTION AND OVERVIEW

1 Introduction

1.1 The Personal Data Protection Act 2012 (the "PDPA") establishes a new general 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 functions, amongst others, of promoting awareness of data protection in Singapore and administering and enforcing the PDPA.

1.2 These advisory guidelines (these "Guidelines") are issued by the Commission pursuant to section 49(1) of the PDPA to provide guidance on the manner in which the Commission will interpret provisions of the PDPA. Where relevant, reference is made to the provisions of the regulations to be made under the PDPA ("Regulations").

1.3 These Guidelines are advisory in nature and are not legally binding on the Commission or any other party. They do not modify or supplement in any way the legal effect and interpretation of any laws cited including, but not limited to, the PDPA and any subsidiary legislation (such as regulations and rules) issued under the PDPA. Accordingly, these Guidelines shall not be construed to limit or restrict the Commission's administration and enforcement of the PDPA. The provisions of the PDPA and any regulations or rules issued thereunder will prevail over these Guidelines in the event of any inconsistency. The Guidelines do not constitute legal advice.

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 2 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 the 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.

2.4 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. The Do Not Call Registry will initially comprise 3 separate registers kept and maintained by the Commission under section 39 of the PDPA (the "Do Not Call Registers") which cover telephone calls, text messages and faxes. Users and subscribers will be able to register their Singapore telephone number(s) on one or more Do Not Call Registers depending on their preferences in relation to receiving marketing messages through telephone calls, text messages or fax.

2.5 Organisations have the following obligations in relation to sending certain marketing messages to Singapore telephone numbers:

a) Checking the relevant Do Not Call Register(s) to confirm if the Singapore telephone number is listed on the Do Not Call Register(s);

b) Providing information on the individual or organisation who sent or authorised the sending of the marketing message; and

c) Not concealing or withholding the calling line identity of the sender of the marketing message.

2.6 The PDPA recognises that organisations may not need to check the Do Not Call Registers in certain circumstances, in particular, when the user or subscriber of a Singapore telephone number has given clear and unambiguous consent in written or other accessible form to the sending of the marketing message to that number.

2.7 The Data Protection Provisions and the Do Not Call Provisions are intended to operate in conjunction when both sets of provisions come into force. Accordingly, organisations are required to comply with both sets of provisions when collecting and using Singapore telephone numbers that form part of individuals' personal data. Organisations need not comply with the Data Protection Provisions for Singapore telephone numbers that do not form part of an individual's personal data, but would still be required to comply with the Do Not Call Provisions.

2.8 Other parts of the PDPA (which are not specifically addressed in these Guidelines) deal with the administration of the PDPA and certain preliminary and general matters. The Commission may issue further advisory guidelines in due course addressing such matters.

PART II: IMPORTANT TERMS USED IN THE PDPA

3 Definitions and related matters

3.1 Before considering the various Data Protection Provisions, it is important to take note of some terms which are used throughout the Data Protection Provisions and which bear particular meanings for the purposes of the PDPA. Some of these terms are defined in Part I of the PDPA (specifically, in section 2(1)).

3.2 A good starting point is the statement of the PDPA's purpose, which is found in section 3 of the PDPA. This states:

"The purpose of this Act is to govern the collection, use and disclosure of 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 or disclose personal data for purposes that a reasonable person would consider appropriate in the circumstances." (emphasis added)

3.3 From the above statement of the PDPA's purpose, the following important terms should be noted:

a) "individuals"

b) "personal data"

c) "organisations"

d) "collection, use and disclosure"

e) "purposes"

f) "reasonable"

3.4 This section seeks to provide guidance on how the above terms may be understood and applied in the context of the Data Protection Provisions.

4 Individuals

4.1 The PDPA defines an individual as "a natural person, whether living or deceased".

4.2 The term "natural person" refers to a human being. This may be distinguished from juridical persons or "legal persons" which are other entities that have their own legal personality and are capable of taking legal action in their own name. An example of such a "legal person" is a body corporate such as a company. The term "natural person" would also exclude unincorporated groups of individuals such as an association which may take legal action in its own name[1].

4.3 Accordingly, since the various Data Protection Provisions are concerned with the personal data of individuals, only the personal data of natural persons is protected under the PDPA. Data relating to corporate bodies and other entities are not covered.

4.4 As the term "individual" includes both living and deceased individuals, the PDPA applies in respect of deceased individuals. However, as will be explained later, the PDPA applies to a limited extent in respect of the personal data of deceased individuals.

5 Personal data

5.1 Personal data is defined in the PDPA as "data, whether true or not, about an individual who can be identified —

a) from that data; or

b) from that data and other information to which the organisation has or is likely to have access.

5.2 The term "personal data" is not intended to be narrowly construed and covers all types of data from which an individual can be identified, regardless of whether such data is true or false or whether it is in electronic or other form. However, as will be highlighted later, the PDPA does not apply in relation to certain categories of personal data which are expressly excluded from the application of the PDPA.

Data about an individual

5.3 The most basic requirement for data to constitute personal data is that it is data about an individual. Data about an individual includes any data that relates to the individual.

[1] For example, a society registered under the Societies Act (Cap. 311) may sue or be sued in its registered name (Societies Act, section 35).

5.4 While some data will necessarily relate to an individual, such as an individual's name, other data may not, on its own, relate to an individual. Such data would not constitute personal data unless it is associated with, or made to relate to, a particular individual.

5.5 For example, a residential address on its own relates to a particular place and there could be several individuals, or even none, residing there. Hence whether a residential address constitutes personal data would depend on whether the address is associated with a particular identifiable individual so as to form part of the individual's personal data.

5.6 Generic information that does not relate to a particular individual may also form part of an individual's personal data when combined with personal data or other information to enable an individual to be identified.

Example:
John Tan is a male Singaporean of 21 years of age. By themselves, general characteristics such as "male", "Singaporean" and "21 years of age" are not able to identify a particular individual. John Tan fills up a membership form which asks for his full name, gender, nationality and age. In this case, all the information on the form, including the general characteristics, constitutes personal data of John Tan.

<u>True and false personal data</u>

5.7 It may be noted from the PDPA's definition of personal data that whether data is "personal data" does not depend on whether the data is true or false. In some cases, an individual may have appropriate reasons for using data that is not, strictly speaking, true, for example, when an individual uses a fictitious name or nickname as part of his or her personal email address.

5.8 As will be explained in greater detail later in the section on the Data Protection Provisions, organisations have an obligation in certain situations to make a reasonable effort to ensure that personal data collected is accurate and complete. If organisations collect personal data which is false, or if the data they collected has changed such that it is no longer true, such data will still be personal data and they are required to comply with this obligation. However, organisations may in certain circumstances be able to rely on personal data provided by an individual as they are not necessarily expected to verify the truth of information submitted directly by the individual.

Identifying an individual

5.9 An individual can be identified if that individual can be singled out from other individuals by an organisation based on one or more characteristics of the data or other pieces of information. Such characteristics or data would form part of the individual's personal data.

5.10 If an individual may be identified from a piece or set of personal data, such data may be referred to as "directly identifying data". As the term "data" may refer to a set of data, directly identifying data includes specific data points which can each identify an individual as well as data points which can identify an individual when combined as a set of data.

Example:
Personal data under the PDPA may include the following:

- Full name
- NRIC or FIN number
- Passport number
- Photograph or video image of an individual
- Mobile telephone number
- Personal email address
- Thumbprint
- DNA profile
- Name and residential address
- Name and residential telephone number

5.11 An individual can also be identified based on certain data and other information to which the organisation has or is likely to have access. Therefore, even if such data is not directly identifying data, it may still be considered personal data if the organisation has access to other information that, when taken together with the data, will allow the individual to be identified. Please also refer to the section on Anonymisation in the Advisory Guidelines on Selected Topics, which describes the conditions under which personal data may be rendered anonymous and hence no longer considered to be personal data for the purposes of the PDPA.

Example:
As part of a research study, a participant is requested to submit information to the research institute, comprising all of the following:

- The participant's name
- A general description of the participant, e.g. 30 year old married Chinese female of AB+ blood type;
- Educational institutions that the participant has attended; and
- The participant's occupation

The research institute replaces the participant's name with a randomly-generated tag in order to safeguard the participant's anonymity. Without the name, the research institute cannot use the rest of the information to identify a specific individual. However, the research institute continues to hold the key that can reverse the randomisation and reinstate the participant's name. In this case, all the participants' information held by the research institute would still be personal data held by the research institute.

5.12 Whether a certain piece or set of data is personal data will depend on the context. Data that may identify an individual in a certain situation may not in another. For example, an individual's residential address is often regarded as forming part of the individual's personal data. While this is true if the address is collected as part of other data about the individual, for example, with his name and other contact information, the address on its own may not be personal data in other contexts. For example, as noted earlier, the address may be used to identify the particular premises and there may be a number of individuals, or none, living at the address.

Example:
A business wishes to sell its products to households within a certain area around its location. It engages a service provider to distribute flyers advertising its products to all residential addresses within the area without collecting or using the names or other personal data of individuals living at those addresses. The residential addresses would not be personal data collected and used by the business.

5.13 An individual can also be identified even if one does not know his name. This is because there are other identifiers relating to the individual which enable one to identify him. Such identifiers are personal data.

Example:
John picks up a photograph from his friend's table which clearly shows the image of an individual. John is holding the personal data of that individual even though he does not know his name.

Personal data relating to more than one individual

5.14 Information about one individual may contain information about another individual. In that circumstance, the same information could be personal data of both the individuals.

5.15 Organisations should note that how they are required to handle personal data in such situations may differ for each individual or that such data will need to be handled collectively.

Example:
An adventure camp company records emergency contact information for all the participants in the adventure camp. This emergency contact information comprises the name, address and telephone number of the individual whom the organisation will contact in the event of an emergency.

Bernie's emergency contact is her husband, Bernard, and she provides his contact details to the company as her emergency contact information. Bernard's name, address and telephone number form part of the personal data of Bernie. As such, the company is holding personal data about two individuals. When obtaining Bernard's personal data from Bernie, the organisation would need to consider if they are required to obtain Bernard's consent or whether one or more of the exceptions provided in the PDPA may apply.

In addition, since Bernard's personal data also forms part of Bernie's personal data (specifically, the details of her emergency contact), organisations would need to protect it as part of Bernie's personal data.

Excluded personal data

5.16 The PDPA does not apply to certain categories of personal data. The collection, use and disclosure of such personal data are accordingly not governed by the PDPA and organisations are not required to comply with any of the Data Protection Provisions in respect of such personal data.

5.17 The PDPA does not apply to the following categories of personal data:

a) Business contact information;

b) Personal data that is contained in a record that has been in existence for at least 100 years; and

c) Personal data about a deceased individual who has been dead for more than 10 years.

5.18 For personal data about a deceased individual who has been dead for 10 years or less, the PDPA applies to a limited extent. For such personal data, only the provisions relating to the disclosure and protection of personal data will apply. These provisions are considered further below.

Business contact information

5.19 The PDPA does not apply to business contact information. Business contact information is defined in the PDPA as "an individual's name, position name or title, business telephone number, business address, business electronic mail address or business fax number and any other similar information about the individual, not provided by the individual solely for his personal purposes".

5.20 Organisations are not required to obtain consent before collecting, using or disclosing any business contact information or comply with any other obligation in the Data Protection Provisions in relation to business contact information.

Example:
At the registration booth of a corporate seminar, Sharon drops her business name card into a glass bowl by the side of the registration booth as she wishes to be on the seminar organiser's mailing list for future invitations to similar seminars.

Sharon's business name card contains her name, position, business telephone number, business address, business electronic mail address and business fax number. As Sharon did not provide her business name card solely for personal purposes, the information on it will be considered business contact information. Accordingly, the seminar organiser does not need to seek Sharon's consent to contact her about future seminars through her business contact information. The seminar organiser is also not required to care for such information, or provide access to and correction of the business contact information collected.

5.21 The definition of business contact information is dependent on the purpose for which such contact information may be provided by an individual as it recognises that an individual may provide certain work-related contact information solely for personal purposes. In such situations, the information would not constitute business contact information and organisations would be required to comply with the Data Protection Provisions in respect of such information.

Example:
Sharon is signing up for a gym membership. She provides her business name card to the gym staff so that they can record her name and contact details in order to register her for the package. In this case, the information provided by Sharon would not be business contact information as she is providing it solely for her personal purposes. The PDPA would apply to the information contained in her business name card.

5.22 Since sole proprietorships and partnerships are also businesses, the contact information of sole proprietors and partners is considered business contact information where such information has not been provided solely for personal purposes.

Example:
Damien is a choral instructor who is the sole proprietor of a music studio. He decides to engage a real estate agent to assist him in searching for a suitable property unit as a second branch. Damien passes his contact details to the real estate agent so that the real estate agent can update him from time to time on property units which he might like.

The real estate agent shares Damien's contact details with his colleagues, so that more agents can assist Damien with his property search. Damien's consent to the sharing of his contact information is not required because it is business contact information. As Damien has provided his contact details for the purpose of a property search, this information is considered business contact information and can be passed on by the real estate agent subsequently without Damien's prior consent. In turn, other persons can also collect, use and disclose Damien's business contact information freely, without requiring Damien's consent.

Personal data of deceased individuals

5.23 As noted earlier, the term "individual" includes both living and deceased individuals. Hence, the provisions of the PDPA will apply to protect the personal data of deceased individuals to the extent provided in the PDPA.

5.24 Specifically, the PDPA provides that the obligations relating to the disclosure and protection of personal data will apply in respect of the personal data about an individual who has been dead 10 years or less. These provisions relate to the following matters, which are explained in greater detail later in the section on the Data Protection Provisions:

a) Notification of purposes for disclosure of personal data (part of the "Notification Obligation" as explained later);

b) Obtaining consent for disclosure of personal data (part of the "Consent Obligation" as explained later);

c) Disclosing personal data for purposes which a reasonable person would consider appropriate in the circumstances (part of the "Purpose Limitation Obligation" as explained later);

d) Making a reasonable effort to ensure the accuracy and completeness of personal data that is likely to be disclosed to another organisation (part of the "Accuracy Obligation" as explained later); and

e) Making reasonable security arrangements to protect personal data (part of the "Protection Obligation" as explained later).

5.25 The above obligations will apply in respect of the personal data of a deceased individual for 10 years from the date of death. This is intended to minimise any adverse impact of unauthorised disclosure of such data on family members of the deceased.

5.26 When complying with their obligations under the PDPA, Organisations should take note of the individuals who may act on behalf of the estate of the deceased individual in respect of matters relating to the deceased's personal data, as prescribed in regulations to be issued under the PDPA.

5.27 Other than the provisions noted above, organisations do not have additional obligations relating to personal data of deceased individuals. Organisations should note that while the PDPA does not apply to personal data of individuals who have been deceased for more than 10 years, there may still be other legal or contractual requirements that companies should be mindful of.

6 Organisations

6.1 The PDPA defines an organisation as "any individual, company, association or body of persons, corporate or unincorporated whether or not formed or recognised under the law of Singapore; or resident, or having an office or a place of business, in Singapore".

6.2 The term "organisation" broadly covers natural persons, corporate bodies (such as companies) and unincorporated bodies of persons (such as associations), regardless of whether they are formed or recognised under the law of Singapore or whether they are resident or have an office or place of business in Singapore.

6.3 Every organisation is required to comply with the PDPA in respect of activities relating to the collection, use and disclosure of personal data in Singapore unless they fall within a category of organisations that is expressly excluded from the application of the PDPA.

6.4 Although individuals are included in the definition of an organisation, they would not be required to comply with the PDPA if they fall within one of the excluded categories as elaborated below.

Excluded organisations

6.5 The PDPA provides that the Data Protection Provisions do not impose any obligations on the following entities. These categories of organisations are therefore excluded from the application of the Data Protection Provisions:

a) Any individual acting in a personal or domestic capacity;

b) Any employee acting in the course of his or her employment with an organisation;

c) Any public agency; and

d) Any organisation in the course of acting on behalf of a public agency in relation to the collection, use or disclosure of personal data.

6.6 In addition, organisations which are data intermediaries are partially excluded from the application of the Data Protection Provisions, as explained further below.

6.7 Organisations which are not within an excluded category should note that they are required to comply with the PDPA when dealing with an organisation that is within an excluded category.

Example:
A travel agency collects personal data from Tom about his wife, Jane, when Tom books a travel package for a family holiday. Tom is not subject to the Data Protection Provisions as he is acting in a personal or domestic capacity. However, the travel agency must comply with the Data Protection Provisions. It can only collect Jane's personal data with her consent unless it is able to, as would be likely from this example, rely on one or more exceptions provided in the PDPA.

Individuals acting in a personal or domestic capacity

6.8 Although individuals are included in the definition of an organisation, they benefit from two significant exclusions in the PDPA. The first is in relation to individuals who are acting in a personal or domestic capacity. Such individuals are not required to comply with the Data Protection Provisions.

6.9 An individual acts in a personal capacity if he or she undertakes activities for his or her own purposes.

6.10 The term "domestic" is defined in the PDPA as "related to home or family". Hence, an individual acts in a domestic capacity when undertaking activities for his home or family.

Individuals acting as employees

6.11 The second significant exclusion for individuals in the PDPA relates to employees who are acting in the course of their employment with an organisation. Employees are excluded from the application of the Data Protection Provisions. The PDPA defines an employee to include a volunteer. Hence, individuals who undertake work without an expectation of payment would fall within the exclusion for employees.

6.12 Notwithstanding this exclusion for employees, organisations remain responsible for the actions of the employees (including volunteers) which result in a contravention of the Data Protection Provisions.

Public agencies and organisations acting on behalf of public agencies

6.13 The PDPA defines a public agency to include the following:

a) the Government, including any ministry, department, agency, or organ of State;

b) any tribunal appointed under any written law; or

c) any statutory body specified by the Minister by notice in the *Gazette*.

6.14 The definition of a public agency covers the various ministries, departments, agencies and organs of state which form part of the Government as well as the specific statutory bodies specified by the Minister. Public agencies are excluded from the application of the Data Protection Provisions.

6.15 Organisations which are acting on behalf of a public agency in relation to the collection, use or disclosure of personal data are also excluded from the application of the Data Protection Provisions when they are so acting. However, such organisations may be subject to obligations under other laws and their contract with the relevant public agency. Such organisations also remain responsible to comply with the Data Protection Provisions in relation to other aspects of their business, for example, in relation to their employee's personal data or personal data of other customers.

Data intermediaries

6.16 The PDPA defines a data intermediary as "an organisation that processes personal data on behalf of another organisation but does not include an employee of that other organisation". In line with the exclusion for employees (noted above), a data intermediary does not include an employee.

Obligations of data intermediaries

6.17 The PDPA provides that a data intermediary that processes personal data on behalf of and for the purposes of another organisation pursuant to a contract which is evidenced or made in writing will only be subject to the Data Protection Provisions relating to protection of personal data (later referred to as the "Protection Obligation") and retention of personal data (later referred to as the "Retention Obligation") and not any of the other Data Protection Provisions.

6.18 A data intermediary remains responsible for complying with all Data Protection Provisions in respect of other activities which do not constitute processing of personal data on behalf of and for the purposes of another organisation pursuant to a contract which is evidenced or made in writing.

6.19 The term "processing" is defined in the PDPA 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;

g) erasure or destruction."

6.20 Items (a) to (g) above represent an indicative but non-exhaustive list of activities which could be considered processing. From the above list, it may be seen that activities which form part of processing by a data intermediary may also form part of collection, use or disclosure by the organisation on whose behalf they are acting. Please refer to the section below on "Collection, Use and Disclosure" for more details on this. As will be seen later, notwithstanding the partial exclusion for some data intermediaries, the PDPA provides that organisations shall have the same obligations under the PDPA in respect of personal data that is processed on its behalf and for its purposes by a data intermediary as if the personal data were processed by the organisation itself.

Considerations for organisations using data intermediaries

6.21 Section 4(3) provides that an organisation has the same obligations under the PDPA in respect of personal data processed on its behalf by a data intermediary as if the personal data were processed by the organisation itself. As such, it is good practice for an organisation to undertake an appropriate level of due diligence to assure itself that a potential data intermediary is capable of complying with the PDPA.

Determination of who the data intermediary is

6.22 There is a diverse range of scenarios in which organisations may be considered data intermediaries for another organisation. An organisation may be a data intermediary of another even if the written contract between the organisations does not clearly identify the data intermediary as such. The PDPA's definition of "data intermediary" would apply in respect of all organisations that process personal data on behalf of another. Hence it is very important that an organisation is clear as to its rights and obligations when dealing with another organisation and, where appropriate, include provision in their written contracts to clearly set out each organisation's responsibilities and liabilities in relation to the personal data in question including whether one organisation is to process personal data on behalf of and for the purposes of the other organisation.

6.23 If Organisation A engages Organisation B, pursuant to a written contract for B to provide services relating to any processing of personal data on behalf of A and for A's purposes, then B may be considered a data intermediary of A in relation to the processing of such personal data. In such a case, A should ensure that its written contract with B clearly specifies B's obligations and responsibilities in order to ensure its own compliance with the PDPA. It is important to note that if B uses or discloses personal data in a manner which goes beyond the processing required by A under the contract, then B will not be considered a data intermediary in respect of such use or disclosure. B will be required to comply with all Data Protection Provisions in respect of such use or disclosure.

Example:
Organisation ABC is a market research firm that has been engaged by Organisation XYZ. The written contract specifies that ABC has been engaged to collect personal data on behalf of XYZ and produce a report, exclusively for the use of XYZ, which illustrates the correlation between investment habits and income, profession and marital status of at least 1000 working Singaporeans aged 25-40. In addition to types of investments made, income, profession and marital status, the contract specifies that ABC has to collect the NRIC number and residential address of each person surveyed.

The contract neither specifies the methods or processes ABC should undertake to collect the data and produce the report, nor the specific individuals that ABC are to survey. However, all raw data collected is to be given to XYZ and ABC is not permitted to keep any copies of the data or use it for any other purpose. In this situation, ABC may still be considered a data intermediary of XYZ insofar as it is processing personal data for the sole purpose of producing the report for XYZ.

As ABC is XYZ's data intermediary, XYZ has the same obligations under the PDPA in respect of the personal data processed by ABC. Hence, it may wish to include additional requirements in its contract to ensure that ABC fulfils XYZ's obligations under the PDPA.

6.24 It is possible for an organisation that is part of a corporate group of organisations to act as a data intermediary for other members of the group.

Example:
Organisation XYZ undertakes payroll administration for a number of organisations, including organisations which belong to the same corporate group to which XYZ belongs. XYZ holds records of such organisations' employees, such as the employees' full names, duration of employment, salary and bank account numbers. XYZ processes such personal data solely for the purpose of payroll administration pursuant to instructions contained within its written contracts with these other organisations. Hence, XYZ is considered a data intermediary for these other organisations in relation to its processing of such personal data.

6.25 An organisation can be considered a data intermediary in respect of a set of personal data while at the same time be bound by all Data Protection Provisions in relation to other sets of personal data.

Example:
In the example above, XYZ is a data intermediary in relation to its processing of personal data of the employees of other organisations for payroll administration purposes. However, in respect of the personal data of XYZ's own employees, XYZ is not a data intermediary, and it is required to comply with all the Data Protection Provisions.

XYZ holds records of such organisations' employees, such as the employees' full names, salary and bank account numbers. XYZ does not take reasonable security arrangements to ensure that those records are secure, and unauthorised disclosure occurs to one of XYZ's employees. XYZ may be liable under the Protection Obligation for failing to protect personal data in its possession or control through the provision of reasonable security arrangements

6.26 In relation to network service providers, the Commission notes previous industry feedback clarifying the liabilities of network service providers that merely act as conduits for the transmission of personal data and highlights that section 67(2) of the PDPA amends the Electronic Transactions Act such that network service providers will not be liable under the PDPA in respect of third party material in the form of electronic records to which it merely provides access.

"Agents" who may be data intermediaries

6.27 Generally, the legal relationship of agency refers to a relationship that exists between two persons, an agent and a principal. An agent is considered in law to represent the principal, in such a way so as to be able to affect the principal's legal position in respect of contracts and certain other dealings with third parties, so long as the agent is acting within the scope of his authority ("legal definition of "agent").

6.28 Persons that carry the title of "agent" (e.g. "Insurance agent" or "Property agent") can fall within or outside the "legal definition of agent" depending on the particular circumstances at hand. Whether a person is an "agent" does not depend on whether he uses the title "agent" as part of his job title, e.g. a "sales agent", but on whether he is acting on behalf of the other person in a particular matter or transaction.

6.29 Persons who fall within the "legal definition of agent" or who carry the title of "agent" have to comply with all obligations in the PDPA except to the extent that it is processing personal data on behalf of and for purposes of another organisation pursuant to a contract which is evidenced or made in writing (i.e. they are considered to be data intermediaries for another organisation). In short, there is no difference in how an agent or any other organisation is treated under the PDPA in relation to whether they qualify as a data intermediary.

7 Collection, use and disclosure

7.1 Part IV of the PDPA sets out the obligations of organisations relating to the collection, use and disclosure of personal data. The PDPA does not define the terms "collection", "use" and "disclosure". These terms would apply as they are commonly understood to cover the common types of activities undertaken by organisations in respect of personal data that may fall under collection, use or disclosure respectively.

7.2 In general, the terms collection, use and disclosure may be understood to have the following meanings:

a) *Collection* refers to any act or set of acts through which an organisation obtains control over or possession of personal data.

b) *Use* refers to any act or set of acts by which an organisation employs personal data. A particular use of personal data may occasionally involve collection or disclosure that is necessarily part of the use.

c) *Disclosure* refers to any act or set of acts by which an organisation discloses, transfers or otherwise makes available personal data that is under its control or in its possession to any other organisation.

7.3 Organisations should bear in mind that collection, use and disclosure may take place actively or passively. Both forms of collection, use and disclosure will be subject to the same obligations under the PDPA although what may be considered reasonable purposes may vary based on the circumstances of the collection, use or disclosure.

Example:
When applying for an insurance plan, Karen is interviewed by an insurance agent who asks her for various personal details as well as information about her health. This is a form of active collection of personal data.

In comparison, Karen attends a reception and writes her name in the unattended guestbook placed near the entrance. This is a form of passive collection of personal data.

8 Purposes

8.1 The PDPA does not define the term "purpose". As will be seen later, a number of Data Protection Provisions refer to the purposes for which an organisation collects, uses or discloses personal data. For example, an organisation is required to notify individuals of the purposes for which it is collecting, using or disclosing personal data (referred to later as the "Notification Obligation"). Hence in order to notify such purposes, an organisation would need to determine what its purposes are.

8.2 The term "purpose" does not refer to activities which an organisation may intend to undertake but rather to its objectives or reasons. Hence, when specifying its purposes relating to personal data, an organisation is not required to specify every activity which it may undertake, but its objectives or reasons relating to personal data.

Example:
A retailer intends to ask an individual for his name and residential address in order to arrange the delivery of certain products purchased from the retailer by the individual. The retailer may specify that it would like to collect, use and disclose the personal data as necessary for the purpose of delivering the goods bought by the individual. The retailer need not specify activities relating to exactly how the personal data will be stored and used by the retailer, for example, that it will be entered into the retailer's customer database, printed on delivery notes and packaging of the items to be

delivered, transmitted to the delivery agent and so on.

9 Reasonableness

9.1 A number of provisions in the PDPA make reference to the concept of reasonableness. For example, section 11(1) states that an organisation shall, in meeting its responsibilities under the PDPA, consider what a reasonable person would consider appropriate in the circumstances. Other Data Protection Provisions similarly make reference to something or some set of circumstances which is reasonable.

9.2 Section 11(1) does not impose a separate obligation on organisations but requires them to consider "what a reasonable person would consider appropriate in the circumstances" when they undertake any action that is subject to the Data Protection Provisions. In seeking to comply with the Data Protection Provisions, organisations should therefore act based on what a reasonable person would consider appropriate in the circumstances.

9.3 The PDPA recognises that a balance needs to be struck between the need to protect individuals' personal data and the need of organisations to collect, use or disclose personal data. The PDPA seeks to provide such a balance by allowing organisations to collect, use and disclose personal data for purposes which a reasonable person would consider appropriate in the circumstances and similarly requires organisations to act based on this standard of reasonableness.

9.4 In determining what a reasonable person would consider appropriate in the circumstances, an organisation should consider the particular circumstances it is facing. Taking those circumstances into consideration, the organisation should determine what would be the appropriate course of action to take in order to comply with its obligations under the PDPA based on what a reasonable person would consider appropriate.

9.5 A "reasonable person" is judged based on an objective standard and can be said to be a person who exercises the appropriate care and judgement in the particular circumstances.

Part III THE DATA PROTECTION PROVISIONS

10 Overview

10.1 Organisations are required to comply with the Data Protection Provisions in Parts III to VI of the PDPA. When considering what they should do to comply with the Data Protection Provisions, organisations should note that they are responsible for personal data in their possession or under their control.[2] In addition, when an organisation employs a data intermediary to process personal data on its behalf and for its purposes, organisations have the same obligations under the PDPA as if the personal data were processed by the organisation itself.[3]

10.2 Broadly speaking, the Data Protection Provisions contain nine main obligations which organisations are required to comply with if they undertake activities relating to the collection, use or disclosure of personal data. These obligations may be summarised as follows. The sections of the PDPA which set out these obligations are noted below for reference.

a) The Consent Obligation (PDPA sections 13 to 17)

An organisation must obtain the consent of the individual before collecting, using or disclosing his personal data for a purpose.

b) The Purpose Limitation Obligation (PDPA section 18)

An organisation may collect, use or disclose personal data about an individual only for purposes that a reasonable person would consider appropriate in the circumstances and, if applicable, have been notified to the individual concerned.

c) The Notification Obligation (PDPA section 20)

An organisation must notify the individual of the purpose(s) for which it intends to collect, use or disclose the individual's personal data on or before such collection, use or disclosure of the personal data.

[2] See PDPA section 11(2).

[3] See PDPA section 4(3).

d) The Access and Correction Obligation (PDPA sections 21 and 22)

An organisation must, upon request:

i. provide an individual with his or her personal data in the possession or under the control of the organisation and information about the ways in which the personal data may have been used or disclosed during the past year; and

ii. correct an error or omission in an individual's personal data that is in the possession or under the control of the organisation.

e) The Accuracy Obligation (PDPA section 23):

An organisation must make a reasonable effort to ensure that personal data collected by or on behalf of the organisation is accurate and complete if the personal data is likely to be –

i. used by the organisation to make a decision that affects the individual concerned; or

ii. disclosed by the organisation to another organisation.

f) The Protection Obligation (PDPA section 24)

An organisation must protect 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.

g) The Retention Limitation Obligation (PDPA section 25)

An organisation must cease to retain documents containing personal data, or remove the means by which the personal data can be associated with particular individuals as soon as it is reasonable to assume that:

i. the purpose for which the personal data was collected is no longer being served by retention of the personal data; and

ii. retention is no longer necessary for legal or business[4] purposes.

h) The Transfer Limitation Obligation (refer to PDPA section 26)

An organisation must not transfer personal data to a country or territory outside Singapore except in accordance with the requirements prescribed under the PDPA.

i) The Openness Obligation (refer to PDPA sections 11 and 12)

An organisation must implement the necessary policies and procedures in order to meet its obligations under the PDPA and shall make information about its policies and procedures publicly available.

10.3 Some of the nine obligations mentioned above may have other related requirements which organisations must comply with. In addition, some of the nine obligations are subject to exceptions or limitations specified in the PDPA. The following sections of these Guidelines consider each of the above obligations in greater detail, together with the additional requirements and exceptions or limitations that may apply.

11 The Consent Obligation

11.1 Section 13 of the PDPA prohibits organisations from collecting, using or disclosing an individual's personal data unless the individual gives, or is deemed to have given, his consent for the collection, use or disclosure of his personal data. This requirement to obtain consent does not apply where collection, use or disclosure of an individual's personal data without consent is required or authorised under the PDPA or any other written law. This obligation to obtain the individual's consent is referred to in these Guidelines as the Consent Obligation.

11.2 Sections 14 to 17 of the PDPA deal with a number of issues relating to the Consent Obligations, which are explained below.

[4] The term "business" is defined in section 2(1) of the PDPA to include activities of non-profit organisations. Specifically, "business" refers to the activity or any organisation, whether or not carried on for gain or conducted on a regular, repetitive or continuous basis, but does not include an individual acting in a personal or domestic capacity.

11.3 An important point to note is that the PDPA does not affect existing legal or regulatory requirements that organisations have to comply with. Organisations may collect, use and disclose (as the case may be) personal data without the individuals' consent if permitted to do so under law, although the organisations may need to comply with other requirements of the Data Protection Provisions which are not inconsistent with its obligations under written law. For more information on this, please refer to the section on Existing Rights, Obligations and Uses.

Obtaining consent from an individual

11.4 Section 14(1) of the PDPA states how an individual gives consent under the PDPA. In particular, an individual has not given consent unless the individual has been notified of the purposes for which his personal data will be collected, used or disclosed and the individual has provided his consent for those purposes. If an organisation fails to inform the individual of the purposes for which his personal data will be collected, used and disclosed, any consent given by the individual would not amount to consent under section 14(1). Further details on the organisation's obligation to notify the individual are explained in the section on the "Notification Obligation".

11.5 Consent can be obtained in a number of different ways. As a best practice, an organisation should obtain consent that is in writing or recorded in a manner that is accessible for future reference, for example, if the organisation is required to prove that it had obtained consent.

11.6 An organisation may also obtain consent verbally although it may correspondingly be more difficult for an organisation to prove that it had obtained consent. For such situations, it would be prudent for the organisation to document the consent in some way, for example, by recording the fact that oral consent was provided by an individual for certain purposes, together with the date and time of such consent.

11.7 Organisations should note that the PDPC's default position is that an individual's failure to opt-out would not constitute consent. Failure to opt-out would only be considered consent in certain limited circumstances. Failure to opt-out (or other instances of inaction) may be due to other reasons than the individual's desire to give consent, or it may not be clear how the individual's inaction amounts to consent. Organisations should also note that it may be more challenging to prove that consent has actually been given through an individual's inaction.

Example:
A retailer has collected personal data from its customers for the purpose of delivering products purchased by the customers. The retailer subsequently mails a flyer to the customers which states that a customer would have consented to their personal data being used for a different purpose, namely for marketing, unless the customer writes back to the retailer to opt out by a certain date. In this case, the customer's inaction does not signify consent since it may be due to other reasons not related to a desire to consent (e.g. not having opened the mailbox or read the flyer).

A second retailer hands out a form to each customer who makes a purchase at its store to obtain their personal data. The form states clearly that the retailer wishes to use the customer's personal data for marketing purposes and contains a box that the resident may tick to opt-out. The staff member handing out the form explains the purpose and the process of opting out to each customer. In this case, the retailer is more likely to be able to rely on the customer's inaction as consent where the customer submits the form with his personal data and does not tick the box provided.

Obtaining consent from a person validly acting on behalf of an individual

11.8 Section 14(4) of the PDPA provides that consent may be given, or deemed to have been given, by any person validly acting on behalf of the individual for the collection, use or disclosure of the individual's personal data. Regulations issued under the PDPA will also provide for some specific situations in which an individual person may give consent on behalf of another.

11.9 In order to obtain consent from a person validly acting on behalf of an individual, the person would similarly have to be notified of the purposes for which the individual's personal data will be collected, used and disclosed and the person must have given consent for those purposes on behalf of the individual. The following sections on when consent is not validly given and deemed consent would also apply.

When consent is not validly given

11.10 Section 14(2)(a) of the PDPA sets out additional obligations that organisations must comply with when obtaining consent. This subsection provides that an organisation providing a product or service to an individual must not, as a condition of providing the product or service, require the individual to consent to the collection, use or disclosure of his personal data beyond what is reasonable to provide the product or service. The subsection also prohibits organisations from obtaining or attempting to obtain consent by providing false or misleading information or using deceptive or misleading practices.

11.11 Section 14(3) provides that any consent obtained in such circumstances is not valid. Hence an organisation may not rely on such consent, and if it collects, uses or discloses personal data in such circumstances, it would have failed to comply with the Consent Obligation.

11.12 Section 14(2)(a) addresses the specific situation where an organisation may seek to require individuals to consent as a condition of providing a product or a service. Provided that an organisation does not seek to impose such a requirement, the organisation may collect, use or disclose personal data for purposes beyond those that are reasonable for providing the product or service to the individual by obtaining the individual's consent in accordance with the PDPA.

Example:
Sarah wants to signs up for a spa package. The terms and conditions include a provision that the spa may share her personal data with third parties, including selling her personal data to third party marketing agencies. Sarah does not wish to consent to such a disclosure of her personal data and requests the spa not to disclose her personal data to third party marketing agencies. The spa refuses to act on her request and informs her that the terms and conditions are standard, and that all customers must agree to all the terms and conditions. Sarah is left either with the choice of accepting all the terms and conditions (i.e. giving consent for use and disclosure of her data as described) or not proceeding with the sign up. In this case, even if Sarah consents for the disclosure of her data to third party marketing agencies, the consent would not be considered valid since it is beyond what is reasonable for the provision of the spa's services to its customers, and the spa had required Sarah's consent as a condition for providing its services.

Instead of requiring Sarah to consent to the disclosure and sale of her personal data to third parties as a condition of providing the service, the spa should separately request Sarah's consent to do so. That is, Sarah should be able to sign up for the spa package without having to consent to the disclosure and sale of her personal data to third parties. The spa is then free to ask Sarah if she would consent, and if she does, would be considered to have obtained valid consent.

11.13 Section 14(2)(a) does not address other situations in which an organisation may seek to require consent as a condition of providing a product or service. For example, organisations are not prohibited from providing offers, discounts or lucky draw opportunities to individuals that are conditional on the collection, use or disclosure of their personal data for specified purposes. Ultimately, such practices would be subject to other requirements of the Data Protection Provisions including, in particular, the requirement that the organisation's purposes must be what a reasonable person would consider appropriate in the circumstances. Further details on this are explained in the section on the "Purpose Limitation Obligation".

Example:
A fashion retailer makes it a condition for every customer who wants to participate in the lucky draw it is administering to provide his mobile telephone number for the purpose of being contacted in future for promotions. As the lucky draw is not tied to a provision of a product or service, the fashion retailer can require that customers who want to participate in the lucky draw provide their mobile telephone numbers.

11.14 When collecting personal data through a form, it is a good practice for organisations to indicate which fields that collect personal data are compulsory and which are optional, and to state the purposes for which such personal data will be collected, used and/or disclosed.

11.15 It follows from section 14(2)(a) that an organisation may require an individual to consent to the collection, use or disclosure of his personal data as a condition of providing a product or service where it is reasonably required in order to provide the product or service.

11.16 In particular, where an organisation would be unable to provide the product or service to the individual if the individual did not consent (or withdrew consent) to the collection, use or disclosure of his personal data for that purpose, the organisation may consider whether to require the individual to consent as a condition or providing such a product or service.

Example:
An individual wishes to obtain certain services from a telecom service provider and is required by the telecom service provider to agree to its terms and conditions for provision of the services. The telecom service provider can stipulate, as a condition of providing those services, that the individual agrees to the collection, use and disclosure of specified items of personal data which is reasonably required by the telecom service provider to supply the services. Such items of personal data may include the name and address of the individual as well as personal data collected in the course of providing the services such as the individual's location data.

11.17 Section 14(2)(b) addresses the situation where an organisation obtains or attempts to obtain consent by providing false or misleading information or using misleading and deceptive practices. Such practices may include situations where the purposes are stated in vague or inaccurate terms, in an illegible font or placed in an obscure area of a document or a location that is difficult to access.

Deemed consent

11.18 Section 15 of the PDPA addresses two situations in which an individual may be deemed to consent even if he has not actually given consent. The first is where an individual voluntarily provides his personal data for a purpose. Under section 15(1), an individual is deemed to consent to the collection, use and disclosure of his personal data for a purpose if the individual voluntarily provides the personal data to the organisation for that purpose and it is reasonable that the individual would do so.

Example:
Sarah makes a visit to a spa for a facial treatment. After the treatment is completed, she makes her way to the cashier to make payment. The cashier tells her that the facial will cost her $49.99. She hands over her credit card to the cashier for the purpose of making payment. The cashier processes the payment and transmits Sarah's credit card details (which comprise some of her personal data) to the bank that handles the payment.

In such a situation, the cashier need not ask for Sarah's consent to collect, use or disclose her credit card number and any other required personal data to process the payment. Sarah would be deemed to have consented to the collection, use and disclosure of her personal data for processing of the payment as she voluntarily provided her credit card with the required personal data and it is reasonable that Sarah would provide her credit card details to pay for her facial.

11.19 For the deemed consent under section 15(1) to apply, the onus would be on the organisation involved to ensure that the individual was aware of the purpose for which his personal data would be collected, used or disclosed.

Example:
Sarah calls a taxi operator's hotline to book a taxi. The customer service officer asks for her name and number in order to inform her of the taxi number, which Sarah provides voluntarily. Sarah is deemed to have consented to the taxi company using her name and number to call or text her when her taxi arrives.

However, if the taxi operator runs a limousine service and wanted to use Sarah's information to market this service to her, Sarah would not be deemed to have consented to the use of her personal data for this purpose. This is because Sarah provided her personal data for the purpose of booking a taxi for a single trip, and not for the purpose of receiving marketing information about the limousine service.

11.20 An individual may sometimes be regarded as voluntarily providing personal data where the individual takes some action that allows the data to be collected, without actually providing the data himself. Hence the onus will be on the organisation involved to establish that the individual wanted to provide his or her personal data and took the action required for it to be collected by the organisation.

Example:
Sarah goes for a medical check-up at a clinic. For the purposes of the check-up, the clinic will be conducting a series of tests which include measuring her height and weight. Sarah is aware that such tests will be conducted as the clinic has provided this information on the registration form that Sarah filled out and submitted prior to the tests. Sarah will be deemed to have consented to the collection of her personal data by submitting to the tests even though she did not directly provide the data to the clinic.

11.21 Section 15(1) also requires that it be reasonable for the individual to have voluntarily provided his or her personal data. Hence, consent will not be deemed to have been given where the individual could not reasonably be expected in the circumstances to have provided his or her personal data for a purpose.

11.22 The second situation in which consent may be deemed is where an individual consents to the disclosure of his personal data by one organisation ("A") to another ("B"). Under section 15(2), if an individual gives or is deemed to have given consent for disclosure of his personal data by A to B for a purpose, the individual is deemed to consent to the collection of his personal data by B for that purpose.

Example:
In an example above, Sarah was deemed to have consented to a facial company collecting, using or disclosing her credit card details to process the payment for her facial. In the course of processing the payment, her credit card details are transmitted to the bank who handles the payment. Since Sarah is deemed to consent to the disclosure of her credit card details by the facial company to the bank, she is also deemed to consent to the collection of her credit card details by the bank for the purpose of processing the payment to the facial company.

11.23 Although organisations may rely on deemed consent instead of obtaining actual consent from the individual, it is good practice for an organisation to review its business processes to determine the situations where it should obtain actual consent instead of seeking to rely on deemed consent. Relying on deemed consent requires an organisation to be able to establish the following:

a) an individual voluntarily provided his personal data;

b) the individual was aware of the purpose for which the personal data was provided; and

c) the circumstances are such that it is reasonable for the individual to have provided his personal data.

11.24 In some situations, as in the examples noted above, it may be clear that the deemed consent provision would apply. However, if it is not clear as to whether the deemed consent provision applies, obtaining consent from the individual would avoid disputes where an individual claims that he did not consent to the collection of his personal data for a purpose and that he did not voluntarily provide personal data for the purpose.

<u>Obtaining personal data from third party sources with the consent of the individual</u>

11.25 As noted above, there are two situations in which organisations may obtain personal data about an individual with the consent of the individual but from a source other than the individual (a "third party source"). These are, in brief:

a) where the third party source can validly give consent to the collection, use and disclosure of the individual's personal data (under section 14(4) of the PDPA); or

b) where the individual has consented, or is deemed to have consented, to the disclosure of his or her personal data by the third party source (under section 15(2) of the PDPA).

11.26 Examples of the above situations could be a referral from an existing customer, where an individual has allowed another (the existing customer) to give consent to the collection of his personal data by the organisation, or the purchase of a database containing personal data from a database reseller who had obtained consent for the disclosure of the personal data.

11.27 Organisations obtaining personal data from third party sources should exercise the appropriate due diligence to check and ensure that the third party source can validly give consent for the collection, use and disclosure of personal data on behalf of the individual (under section 14(4)) or that the source had obtained consent for disclosure of the personal data (under section 15(2)).

11.28 In the event the third party source could not validly give consent, or had not obtained consent for disclosure to the collecting organisation but concealed this from the collecting organisation, the actions taken by the collecting organisation to verify such matters before collecting the personal data from the third party source would be considered a possible mitigating factor by the Commission should there be a breach of the PDPA relating to such collection or the collecting organisation's use or subsequent disclosure of the personal data.

11.29 Related to the foregoing, an organisation ("A") collecting personal data from another organisation ("B") under section 15(2) is not required to obtain documents containing or evidencing the consent given by the individuals' concerned to B to disclose the personal data. As a practical matter, it may not be possible for such documents to be provided to A, for example, where such documents contain personal data which cannot be disclosed to A without the individuals' consent. In such circumstances, A may instead seek to obtain an undertaking by B, for example, given as a term of a contract between A and B, that the disclosure by B to A for A's purposes is within the scope of the consent given by the individuals' concerned for B to disclose the personal data and therefore in compliance with the PDPA.

11.30 An organisation collecting personal data from a third party source is required to notify the source of the purposes for which it will be collecting, using and disclosing the personal data (as applicable). For further details on this, please refer to the section on the "Notification Obligation".

Obtaining personal data from third party sources without the consent of the individual

11.31 An organisation ("A") may collect personal data from a third party source ("B") (as described in the previous section) without the consent of the individual in the circumstances described in the Second Schedule to the PDPA. If B is an organisation that is required to comply with the PDPA, it would only be able to disclose the personal data without the consent of the individual in one of the circumstances set out in the Fourth Schedule of the PDPA. These circumstances include, for example, where

a) the disclosure is necessary to respond to an emergency that threatens the life, health or safety of the individual or another individual;

b) the personal data is publicly available; and

c) the disclosure is for the purpose of contacting the next-of-kin or a friend of any injured, ill or deceased individual.

11.32 As consent of the individual is not required, A is not required to verify that B had notified the individual of the purposes for which his personal data would be collected, used and disclosed and obtained the individual's consent. However, B would need to know the purpose for which A is collecting the personal data in order to determine if its disclosure of the data to the organisation would be in accordance with the PDPA. The Data Protection Provisions thus require A to inform B of its purposes. In particular, section 20(2)[5] of the PDPA requires A to provide B with sufficient information regarding its purpose for collecting the personal data to allow B to determine whether disclosure would be in accordance with the PDPA.

[5] Section 20(2) states that – "An organisation, on or before collecting personal data about an individual from another organisation without the consent of the individual, shall provide the other organisation with sufficient information regarding the purpose of the collection to allow that other organisation to determine whether the disclosure would be in accordance with this Act."

Withdrawal of consent

11.33 Section 16 of the PDPA provides that individuals may at any time withdraw any consent given or deemed to have been given under the PDPA in respect of the collection, use or disclosure of their personal data for any purpose by an organisation. Upon withdrawal of consent, the organisation must cease (and cause its data intermediaries and agents to cease) collecting, using or disclosing the personal data, as the case may be, unless the collection, use or disclosure of the personal data without consent is required or authorised under the PDPA or any other written law.

11.34 Section 16 sets out a number of requirements that must be complied with by either the individual or the organisation in relation to a withdrawal of consent. In brief, they are:

a) the individual must give reasonable notice of the withdrawal to the organisation (section 16(1));

b) on receipt of the notice, the organisation must inform the individual of the consequences of withdrawing consent (section 16(2)); and

c) an organisation must not prohibit an individual from withdrawing consent, although this does not affect any legal consequences arising from such withdrawal (section 16(3)).

11.35 In general, organisations must allow an individual who has previously given (or is deemed to have given) his consent to the organisation for collection, use or disclosure of his personal data for a purpose to withdraw such consent by giving reasonable notice. In this regard, considerations for whether reasonable notice has been given would include the amount of time needed to give effect to the withdrawal of consent and the manner in which notice was given.

11.36 In order to enable and facilitate withdrawal, organisations are advised to make an appropriate consent withdrawal policy easily accessible to the individuals concerned. This withdrawal policy should, for example:

a) advise the individuals on the form and manner to submit a notice to withdraw their consent for specific purposes;

b) indicate the person to whom, or the means by which, the notice to withdraw consent should be submitted; and

c) distinguish between purposes necessary and optional to the supply of the good/services or the service of the existing business relationship. (Individuals must be allowed to withdraw consent for optional purposes without concurrently withdrawing consent for the necessary purposes).

11.37 Organisations should not have inflexible consent withdrawal policies that seek to restrict or prevent individuals from withdrawing consent in accordance with the PDPA.

11.38 Once an organisation has received a notice to withdraw consent, the organisation should inform the individual concerned of the likely consequences of withdrawing his consent. This could simply be that the organisation would cease to collect, use or disclose the individual's personal data for the purpose specified by the individuals, or that the organisation would be unable to continue providing services to the individual.

11.39 An organisation must not prohibit an individual from withdrawing his consent to the collection, use or disclosure of personal data about the individual himself. For example, if an organisation requires certain personal data from an individual in order to fulfil a contract with the individual to supply products or services, it may not stipulate as a term of the contract that the individual cannot withdraw consent to the collection, use or disclosure of the individual's personal data for the purposes of the contract. However, this does not affect any legal consequences arising from such withdrawal.

Example:
An individual wishes to obtain certain services from a telecom service provider, Operator X and is required by the telecom service provider to agree to its terms and conditions for provision of the services. Operator X can stipulate as a condition of providing the services that the individual agrees to the collection, use and disclosure of specified items of personal data by the organisation for the purpose of supplying the services. Such items of personal data may include the name and address of the individual as well as personal data collected in the course of providing the services such as the individual's location data. The individual provides consent for those specified items of personal data but subsequently withdraws that consent.

The withdrawal of consent results in Operator X being unable to provide services to the individual. This would in turn entail an early termination of the service contract. Operator X should inform the individual of the consequences of the early termination, e.g. that the individual would incur early termination charges.

11.40 With regard to personal data that is already in an organisation's possession, withdrawal of consent would only apply to an organisation's continued use or future disclosure of the personal data concerned. Upon receipt of a notice of withdrawal of consent, the organisation must inform its data intermediaries and agents about the withdrawal and ensure that they cease collecting, using or disclosing the personal data for the organisation's purposes.

11.41 Apart from its data intermediaries and agents, an organisation is not required to inform other organisations to which it has disclosed an individual's personal data of the individual's withdrawal of consent. This does not affect the organisation's obligation to provide, upon request, access to the individual's personal data in its possession or control and information to the individual about the ways in which his personal data may have been disclosed. Hence the individual may find out which other organisations his personal data may have been disclosed to and withdraw consent to them directly. For more information about an organisation's obligation to provide access to an individual's personal data and information relating to how it may have been disclosed, please refer to the section on the "Access and Correction Obligation".

11.42 Although an individual may withdraw consent for the collection use, or disclosure of his personal data, section 16 does not require an organisation to delete or destroy the individual's personal data upon request. Organisations may retain personal data in its documents and records in accordance with the Data Protection Provisions. For more information on this, please refer to the section on the "Retention Limitation Obligation".

Example:
Andy had previously given his consent to Y Electronics to collect, use and disclose his contact details (which form part of his personal data) for the purpose of providing him with marketing information and promotional offers on computers and other IT products. Y Electronics discloses Andy's contact details to its outsourced marketing agent and some other third party companies offering computers and other IT products, in each case, for the purpose of marketing computers and other IT products to Andy. Andy changes his mind and submits a notice to withdraw the consent he gave to Y Electronics.

Y Electronics is required to notify Andy of the consequences of his withdrawal, in this case, simply that Y Electronics and its marketing agents will cease to send information on computer and IT products to Andy and will not disclose Andy's personal data to any third party after Andy's withdrawal of consent. Y Electronics is also required to cease using Andy's contact details for marketing computer and IT products and to instruct its outsourced

marketing agent about the withdrawal of consent (so that it will cease sending marketing information to Andy).

However, Y Electronics will not be required to inform the third party companies to which it disclosed Andy's contact details, and Andy will have to approach those companies to withdraw consent if he wishes to do. The withdrawal of consent also does not affect Y Electronics' ability to retain Andy's personal data that it requires for legal or business purposes. For example, Y Electronics may still retain Andy's personal data in its database for the purpose of servicing an ongoing warranty, or records of his purchases that are necessary for audit purposes.

Exceptions to the Consent Obligation

11.43 Section 17 of the PDPA permits the collection, use and disclosure of personal data without consent (and, in the case of collection, from a source other than the individual) only in the circumstances provided in the Second Schedule (Collection of personal data without consent), Third Schedule (Use of personal data without consent) and Fourth Schedule (Disclosure of personal data without consent) to the PDPA respectively. These exceptions to the Consent Obligation do not affect rights or obligations arising under any other law. Hence, even if an exception applies under the PDPA, organisations are required to comply with their other legal obligations, for example, to protect confidential information or under a contract.

Publicly available data

11.44 One significant exception in the Second, Third and Fourth Schedules to the PDPA relates to personal data that is publicly available. The term "publicly available" is defined in section 2(1) of the PDPA and refers to personal data (about an individual) that is generally available to the public, including personal data which can be observed by reasonably expected means at a location or an event at which the individual appears and that is open to the public.

11.45 The explanation "generally available to the public" refers to the commonly understood meaning of the term "publicly available". Personal data is generally available to the public if any member of the public could obtain or access the data with few or no restrictions. In some situations, the existence of restrictions may not prevent the data from being publicly available.

11.46 For example, if personal data is disclosed to a closed online group but membership in the group is relatively open and members of the public could join with minimal effort, then the disclosure may amount to making the data publicly available. Conversely, if personal data is disclosed to a close circle of the individual's family and friends or it is inadvertently disclosed to a single member of the public who is not personally known to the individual concerned, the disclosures may not make the personal data publicly available.

Example:
Alan is a member of an online social network that is open to the public[6]. His membership profile which is publicly searchable lists his name, date of birth and the university at which he is currently enrolled. Alan also regularly updates his profile picture. The data (including pictures of him) which Alan has shared on this online social network is very likely to be personal data that is publicly available, since any other user of the social network would be able to gain access to the data, even if they accessed his profile page by accident and any member of public may join the online social network.

Bob is a member of the same social network. However, Bob's membership profile is only accessible by a few users who are personally known to him and to whom he has granted permission to access his profile. Bob has also placed restrictions on the re-posting of his profile. The personal data on Bob's membership profile is less likely to be considered publicly available since access to the data is strictly limited.

11.47 Publicly available personal data also includes a category of personal data that is specifically included in the definition, that is, personal data observed in public. For this to apply, there are two requirements relating to how and where the personal data is observed:

a) the personal data must be observed by reasonably expected means; and

[6] The Commission notes that organisations which operate websites or applications may subject their users to a standard set of terms and conditions, which could include reserving the right to make the personal data of users publicly available (or disclose the personal data in specified ways) that could be contrary to their users' personal preferences to restrict access to their personal data. In such cases, whether the organisation had obtained valid consent from users would depend on whether the organisation had obtained consent in accordance with the PDPA, for example whether it had fulfilled the Consent, Purpose Limitation and Notification Obligations.

b) the personal data must be observed at a location or event at which the individual appears and that is open to the public.

11.48 Personal data is observed by reasonably expected means if the individual whose personal data is being observed could reasonably expect their personal data to be collected in that particular manner at that location or event.

Example:
Jeff is strolling down the aisles in a shopping mall. It would be reasonably expected that his image would be captured by CCTVs installed for security reasons.

Jeff subsequently enters a store to make a purchase. It would not be reasonably expected for Jeff to be photographed by a photographer engaged by the store if the store did not put up notices on the presence of the photographer.

11.49 A location or event would be considered "open to the public" if members of the public can enter or access the location with few or no restrictions. Similar to the term "generally available to the public", the existence of some restrictions may not prevent the location from being regarded as open to the public. For example, events that may be entered only upon payment of a fee by a member of the public may be considered to be open to the public for the purposes of the PDPA. Similarly, special events for members of a retailer's loyalty programme may also be considered open to the public, depending on factors such as whether the event was open to a large number of members.

11.50 In some situations, a private event may be held at a location that is usually open to the public. For example, an individual may book an entire restaurant for a private dinner. In such situations, as members of the public cannot enter the location during the event, the event is not open to the public.

11.51 A location is not open to the public merely because members of the public may look into the premises or location. For example, if members of the public are not able to enter residential premises or commercial premises that are closed for a private event, the ability to observe what is happening inside the premises would not make the premises open to the public.

Example:
Charles wishes to organise a birthday party for his son David. Charles books a private room within a fast food restaurant for the occasion and invites twenty of David's friends and their parents. The private room is right by the general dining area and the interior can be seen by other patrons through the glass

windows. The fast food restaurant management puts up a sign at the entrance of the private room which says "Reserved for Private Event: David's 8th birthday party". Charles keeps the door closed at all times and keeps an eye on it to ensure that only invited guests enter. The birthday party would not be considered open to the public because members of the public (who are not invited to attend) are unlikely to be able to gain access to the event.

Mary similarly wishes to organise a birthday party for her daughter Jane. She invites twenty of Jane's friends and parents to gather at the same fast food restaurant at a particular date and time but she does not book a private room or area within the restaurant. Her guests occupy a large area within the fast food restaurant's general dining area. Mary's birthday party would be considered open to the public even though she did not open attendance to the public, because members of the public may enter the general dining area of the restaurant and may seat themselves close to or even within the area where her party guests are seated.

12 The Purpose Limitation Obligation

12.1 Section 18 of the PDPA limits the purposes for which and the extent to which an organisation may collect, use or disclose personal data. Specifically, section 18 provides that an organisation may collect, use or disclose personal data about an individual only for purposes:

a) that a reasonable person would consider appropriate in the circumstances; and

b) where applicable, that the individual has been informed of by the organisation (pursuant to the Notification Obligation).

12.2 The obligation of organisations to collect, use and disclose personal data for the limited purposes specified in section 18 of the PDPA is referred to in these Guidelines as the Purpose Limitation Obligation.

12.3 The main objective of the Purpose Limitation Obligation is to ensure that organisations collect, use and disclose personal data only for purposes that are reasonable. Consistent with the Notification Obligation, the Purpose Limitation Obligations also limits the purposes for which personal data may be collected, used or disclosed to those which have been informed to the individuals concerned pursuant to the Notification Obligation (where applicable).

12.4 For the purposes of section 18 (and as stated in that section), whether a purpose is reasonable depends on whether a reasonable person would consider it appropriate in the circumstances. Hence the particular circumstances involved need to be taken into account in determining whether the purpose of such collection, use or disclosure is reasonable. For example, a purpose that is in violation of a law or which would be harmful to the individual concerned is unlikely to be considered appropriate by a reasonable person.

Example:
A fashion retailer is conducting a membership drive. It states in the membership registration form that the purposes for which it may use the details provided by individuals who register including providing them with updates on new products and promotions and any other purpose that it deems fit.

In this case, providing updates on new products and promotions may be a reasonable purpose but the fashion retailer's unqualified reference to 'any other purpose that it deems fit' would not be considered reasonable. (As noted in the section on the "Notification Obligation", this may also be an inadequate notification to the individual of the purposes for which his or her personal data will be collected, used and disclosed.)

13 The Notification Obligation

13.1 As noted in the previous sections on the Consent Obligation and the Purpose Limitation Obligation, organisations must inform individuals of the purposes for which their personal data will be collected, used and disclosed in order to obtain their consent. The organisation's collection, use and disclosure is limited to the purposes for which notification has been made to the individuals concerned.

13.2 Section 20 of the PDPA sets out the obligation of organisations to inform individuals of these purposes. In particular, section 20(1) requires an organisation to inform the individual of:

a) the purposes for the collection, use and disclosure of his personal data, on or before collecting the personal data; or

b) any purpose for use or disclosure of personal data which has not been informed under sub-paragraph (a), before such use or disclosure of personal data for that purpose.

13.3 This obligation to inform individuals of the purposes for which their personal data will be collected, used and disclosed is referred to in these Guidelines as the Notification Obligation.

13.4 The Notification Obligation does not apply in the circumstances specified in section 20(3). That is, organisations are not required to inform individuals of the purposes for which their personal data will be collected, used or disclosed if:

a) the individual is deemed to have consented to the collection, use or disclosure of his or her personal data under section 15 of the PDPA; or

b) the organisation is collecting, using or disclosing the personal data without the consent of the individual concerned in accordance with section 17 of the PDPA (that is, in the circumstances specified in the Second, Third and Fourth Schedules to the PDPA).

13.5 It is important for an organisation to identify the purposes for which it is collecting, using or disclosing personal data by establishing the appropriate policies and procedures. These would enable the organisation to identify what personal data it needs to collect, use and disclose for its business purposes and to ensure that the personal data collected is consistent with the purposes identified. It would also minimise the risk of collecting, using or disclosing personal data in contravention of the Data Protection Provisions.

13.6 The following paragraphs consider three important issues relating to the Notification Obligation:

a) when an organisation must inform the individual of its purposes;

b) the manner and form in which the organisation should inform the individual; and

c) the information and details to be included when an organisation states its purposes.

When an organisation must specify its purposes

13.7 Under section 20 (1) and (4), an organisation must inform the individual of the purposes for which his personal data will be collected, used or disclosed on or before such collection, use or disclosure (as the case may be). For example, this may take place when an individual is entering into a contract with an organisation under which the organisation requires certain personal data from the individual. In other situations, an organisation may need to inform the individual before entering into a contract with the individual. For example, an insurance advisor may need to obtain certain personal data from an individual before the insurance company enters into a contract of insurance with the individual. Where an organisation needs to collect, use and/or disclose personal data on a periodic basis, it must inform the individual before the first collection of the data.

The manner of stating purposes and obtaining consent

13.8 The PDPA does not specify the manner or form in which an organisation is to inform an individual of the purposes for which it is collecting, using or disclosing the individual's personal data. An organisation should determine the appropriate form and manner of doing so in order to ensure that the individual is provided with the required information in a manner and form that allows the individual to understand the purposes. An organisation may select the appropriate manner and form to notify an individual based on the relevant factors, which may include the following:

a) the circumstances in which it will be collecting the personal data;

b) the amount of personal data to be collected; and

c) the frequency at which the data will be collected.

13.9 It is generally good practice for an organisation to state its purposes in written form so that the individual is clear about its purposes and, in the event of a dispute or a complaint on this issue, both parties will be able to refer to a clearly documented statement of the organisation's purposes. For the purposes of the PDPA, consent in writing includes consent given in electronic form (such as in an email).

13.10 For example, information about an organisation's purposes may be stated in an agreement between the organisation and the individual or may be stated in a separate data protection notice provided to the individual. The latter may be appropriate in situations where an organisation needs to obtain personal data from an individual either before, or independently of, any agreement with the individual. The document setting out the organisation's purposes may be made available to the individual in physical or electronic form (e.g. online).

Example:
Sarah signs up for a spa membership over the Internet. The terms and conditions for the spa membership outline and explain how Sarah's personal data will be used and disclosed. For example, it states that Sarah's address details will be used for sending her a spa membership card and other communications from the spa. Sarah clicks on the "Accept" button at the bottom of the terms and conditions, to indicate her acceptance of, and agreement to, the terms and conditions. In this case, the spa has obtained Sarah's consent for collection, use and disclosure of her personal data in connection with the stated purposes.

Jane signs up for another spa, Spa B over the internet. Spa B has terms and conditions with a provision which states that when a member accepts the terms and conditions, he or she also consents to the collection, use and disclosure of his or her personal data for the purposes set forth in the spa's data protection policy. However, no information is provided on where the spa's data protection policy is located (even if it is available elsewhere on the spa's website) and no means are provided for Jane to view the policy before signifying her agreement to the spa's terms and conditions. In this case, the spa is not considered to have notified Jane of its purposes, and any consent obtained from Jane would not be valid under the PDPA.

Verbal notification and consent

13.11 In situations where the organisation cannot conveniently obtain consent in from an individual in writing, it may do so verbally. However, it is a good practice for the organisation to follow up to document the consent in writing (which may be in electronic or physical form).

13.12 Organisations may alternatively record the individual's verbal consent in some manner, for example, by recording the telephone conversation between the organisation and the individual. However, where this results in the collection of additional personal data, such as the voice recording of the individual, the organisation must also notify the individual of the collection and seek his consent.

Example:
An individual wishes to sign up for certain services with a service provider over the telephone. The service provider may request for the individual's consent to the collection and use of his personal data for the service provider's purposes and obtain the personal data from the individual over the telephone.

It would be good practice for the service provider to subsequently contact the individual and confirm his consent in writing, for example, by sending an email to the individual setting out the personal data provided by the individual and recording his consent to collection, use and disclosure by the service provider for the service provider's purposes (which may be set out in its terms and conditions and/or other information provided in the email).

13.13 Organisations should note that the Do Not Call Provisions in the PDPA require consent to be obtained in written or other accessible form. Hence for the purposes of the Do Not Call Provisions, verbal consent would be insufficient unless it can be recorded in a form which is accessible for subsequent reference.

Form of stating purposes/obtaining consent

13.14 Informing the individual of the purposes for which his personal data will be collected, used or disclosed is an important aspect of obtaining consent for the purposes of the Data Protection Provisions. As a best practice, organisations should ensure that the notification is provided in a form that is readily accessible and easy for the individual to comprehend. The notification should also be clear and concise, and provide appropriate information on the purposes for which consent is sought (as explained further in the next section).

Example:
A supermarket conducts a survey of shoppers on its premises to find out ways to improve customer experience. It collects personal data such as the names and contact details of the shoppers. It clearly and legibly states at the top of the survey form, "Your personal data may be used by the supermarket or its appointed survey company for analysis of survey responses, or to contact survey respondents for follow-up queries on the survey responses." The supermarket may be considered to have provided appropriate notification in this scenario.

A real estate agency places a guest book at the reception counter in a show flat and requests individuals who visit the show flat to provide their name and contact details in the guest book. However, the purposes for collecting the

individuals' personal data are not stated anywhere in or near the guest book. Individuals could have provided their personal data for a variety of different reasons – e.g. for the purpose of being contacted in relation to their visit to the show flat, to receive information about other properties marketed by the agency, or for other purposes. In addition, different individuals who provide their personal data in this manner may have different purposes in mind. The real estate agency should specify the purposes in order to provide appropriate notification to the individuals from whom it would be collecting personal data.

13.15 While an organisation may determine the manner and form in which it informs the individual of its purposes, it may not do so by providing false or misleading information or using deceptive or misleading practices (as explained in the section on the "Consent Obligation"). Any consent obtained in such circumstances is invalid and the collection, use or disclosure of personal data relying upon such invalid consent would be a contravention of the Data Protection Provisions.

Example:
Another supermarket conducts a similar survey of shoppers on its premises, with the additional intent of marketing new products to the survey respondents. However, this supermarket only indicates on the survey form, "Your personal data may be used by the supermarket or its appointed survey company for analysis of survey responses, or to contact survey respondents for follow-up queries on the survey responses" and does not make any mention of its marketing purposes. It further attempts to pass off the marketing of new products as following up on survey responses. This supermarket is unlikely to be considered as having provided the required information on its purposes in this scenario.

Providing Notification through a Data Protection Policy and/or Online

13.16 The PDPA requires organisations to develop and implement policies and procedures that are necessary for the organisation to meet its obligations under the PDPA. In addition, organisations are required to make information available on such policies and procedures. Organisations may wish to develop a Data Protection Policy (also referred to as a Privacy Policy) to set out its policies and procedures for complying with the PDPA.[7] An organisation may choose to notify individuals of the purposes for which it collects, uses and discloses personal data through its Data Protection Policy.

13.17 The Data Protection Policy may be provided to individuals as required, in the form of a physical document, on the organisation's website or some other manner. Organisations which choose to provide notification to individuals through a Data Protection Policy should note the following:

a) Where the policy is not made available to an individual as a physical document, the organisation should provide the individual with an opportunity to view its Data Protection Policy before collecting the individual's personal data. For example, when an individual signs up for services at an organisation's retail shop, the retailer could provide the individual with an extract of the most relevant portions of the Data Protection Policy in a physical document.

b) If an organisation's Data Protection Policy sets out its purposes in very general terms (and perhaps for a wide variety of services), it may need to provide a more specific description of its purposes to a particular individual who will be providing his personal data in a particular situation (such as when subscribing for a particular service), to provide clarity to the individual on how his personal data would be collected, used or disclosed.

13.18 For the avoidance of doubt, organisations are not required to make available to individuals all matters relating to internal organisational governance as part of their Data Protection Policy.

[7] Please see the Section on "The Openness Obligation" more information

Information to be included when stating purposes

13.19 In stating its purposes, an organisation should provide appropriate and specific details of its purposes for the individual to determine the reasons for which the organisation will be collecting, using or disclosing his personal data. As explained earlier in the Guidelines, in stating its purposes, an organisation need not state every activity it will undertake when collecting, using or disclosing personal data.

13.20 In considering how specific to be when stating its purposes, organisations may have regard to the following:

a) whether the purpose is stated clearly and concisely;

b) whether the purpose is required for the provision of products or services (as distinct from optional purposes);

c) whether purposes that may be of special concern to the individual have been highlighted;

d) if the personal data will be disclosed to other organisations, how the organisations should be made known to the individuals;

e) whether stating the purpose to a greater degree of specificity would be a help or hindrance to the individual understanding the purpose(s) for which his personal data would be collected, used, or disclosed, and

f) what degree of specificity would be appropriate in light of the organisation's business processes.

Example:
An electronics store sells products online through its website. It informs individuals purchasing products through its website of the purposes for which it will be collecting, using and disclosing personal data, including that the contact details provided by the customers will be disclosed to other companies in its corporate group and its outsourced marketing company for the purpose of marketing their products to the individual from time to time. In this case, the electronics store would be considered to have stated a sufficiently specific purpose.

In another case, the electronics store informs individuals purchasing products through its website that the personal data provided may be used and disclosed for valid business purposes. In this case, the electronics store is would not be considered to have stated a sufficiently specific purpose.

Use and disclosure of personal data for a different purpose from which it was collected

13.21 The Data Protection Provisions recognise that there will be circumstances in which an organisation would like to use or disclose an individual's personal data for purposes which it has not yet informed the individual of or for which it has not yet obtained the individual's consent. There could also be situations where it would be too impractical or costly for an organisation to exhaustively list all possible purposes for which it would like to use or disclose the individual's personal data upfront at the point of collection.

13.22 Where an organisation wishes to use or disclose personal data for purposes which it has not yet informed the individual or for which it has not yet obtained the individual's consent, organisations need to inform individuals of those purposes and obtain consent (the "Notification" and "Consent Obligation").

13.23 In determining if personal data can be used or disclosed for a particular purpose without obtaining fresh consent, an organisation should determine:

a) whether the purpose is within the scope of the purposes for which the individual concerned had originally been informed, for example, if it would fall within the organisation's servicing of the existing business relationship with the individual;

b) whether consent can be deemed to have been given by the individual in respect of use or disclosure for that purpose; and

c) whether the purpose falls within the exceptions from consent in the Third and Fourth Schedules to the PDPA.

If the purpose does not fall within sub-paragraphs (a) to (c) above, then the organisation must obtain the individual's fresh consent for use and disclosure for the new purpose.

Example:
Sarah has signed up with a spa membership. Her spa wants to use her personal data for the purposes of sending her greeting cards and reminders to when her spa membership is expiring in the post. These purposes would fall within sub-paragraph (a) above, as part of the organisation's servicing of the existing business relationship with the individual, for which consent would have been previously obtained.

Sarah's financial advisor Paul wants to send her an analytical report providing information on the 'Goldmine Fund', which Sarah holds. Paul does not need to obtain fresh consent for this purpose as it falls within sub-paragraph (a)

above, as part of his service to Sarah as her financial advisor. However, Paul would need to obtain Sarah's consent before sending materials containing generic information, e.g. his company's annual newsletter, as that is unlikely to fall within sub-paragraphs (a) to (c) above.

14 The Access and Correction Obligation

14.1 Sections 21 and 22 of the PDPA set out the rights of individuals to request for access to their personal data and for a correction to their personal data held by an organisation and the corresponding obligations of the organisation to provide access to, and correction of, the individual's personal data. These obligations are collectively referred to in these Guidelines as the Access and Correction Obligation as they operate together to provide individuals with the ability to verify their personal data held by an organisation.

Access to personal data

14.2 Section 21(1) of the PDPA provides that, upon request by an individual, an organisation shall provide the individual with the following as soon as reasonably possible:

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 that personal data has been or may have been used or disclosed by the organisation within a year before the date of the individual's request.

14.3 Section 21(1) allows an individual to submit a request to an organisation for access to personal data about him that is in the possession or under the control of the organisation (an "access request"). An organisation that receives an access request from an individual is required to provide the information requested by the individual under section 21(1). This may include:

a) some or all of the individual's personal data (as specified in the request); and

b) information about the ways the personal data has been or may have been used or disclosed by the organisation (as specified in the request).

14.4 An organisation is required to respond to an access request in respect of personal data in its possession as well as personal data that is under its control (which may not be in its possession). For example, if an organisation has transferred personal data to a data intermediary that is processing the personal data under the control of the organisation, the organisation's response to an access request must take into account the personal data which is in the possession of the data intermediary.

14.5 As stated in section 21(1), if an individual requests for information relating to the use or disclosure of his personal data by the 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. In this regard, an organisation may develop (and update periodically) a standard list of all possible third parties to whom personal data may have been disclosed by the organisation instead of a list that specifically relates to the personal data of a particular individual. The organisation may provide this standard list as part of its response to all access requests that asks for such information.

Example:
Sarah makes an access request to her spa, requesting information relating to how her personal data has been used or disclosed. The request was made on 5th February 2013. The spa is only required to provide information on how her personal data has been used or disclosed with the past year – that is, the period from 6th February 2012 to the date of the request, 5th February 2013.

14.6 The obligation in section 21(1) is subject to a number of exceptions in section 21(2) to (4) including some mandatory exceptions relating to situations where an organisation must not provide access. These exceptions are considered below. However, if the personal data or information requested by an individual includes data and information that is not excluded under section 21(2) to (4) (as well as data and information that is so excluded), section 21(5) of the PDPA requires the organisation to provide the personal data and information which is not excluded under section 21(2) to (4).

14.7 Organisations may charge an individual a fee for access to personal data about the individual.[8]

[8] The Commission is currently also consulting on proposed regulations on this issue.

Exceptions to the obligation to provide access to personal data

14.8 Section 21(2) of the PDPA provides that an organisation is not required to provide individuals with the personal data or other information specified in section 21(1) in respect of the matters specified in the Fifth Schedule to the PDPA. An organisation is not prohibited from providing information in respect of the matters specified in the Fifth Schedule and may do so if it decides to, in which event the organisation may charge a fee for access to the personal data. If organisations do not provide access to personal data in respect of the matters specified in the Fifth Schedules, organisations may, as good practice, inform individuals of the relevant reason(s).

14.9 The exceptions specified in the Fifth Schedule include the following matters:

a) opinion data kept solely for an evaluative purpose;[9]

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) the personal data was collected by an arbitrator or mediator in the conduct or an arbitration or mediation for which he was appointed to act –

f) under a collective agreement under the Industrial Relations Act (Cap. 136);

i. by agreement between the parties to the arbitration or mediation;

ii. under any written law; or

iii. by a court, arbitral institution or mediation centre;

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

[9] The term “evaluative purpose” is defined in section 2(1) of the PDPA.

h) personal data which is subject to legal privilege;

i) 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;

j) personal data collected, used or disclosed without consent for the purposes of an investigation if the investigation and associated proceedings and appeals have not been completed;[10] or

k) 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.

Example:
A shopping centre receives a request from an individual to view all CCTV footage of him recorded at the shopping centre over the past year. In this scenario, even if the shopping centre is able to remove images of other individuals captured in the CCTV footage, reviewing all CCTV footage from the past year to find records of the individual making the request would require considerable time and effort. The burden of providing access would be unreasonable to the shopping centre and likely disproportionate to the individual's interests as the individual is making a general request for all CCTV footage. Hence the shopping centre need not provide the requested personal data (if available) under the Access and Correction Obligation.

A shop in the shopping centre receives a request from an individual to view a photograph of him taken by the official photographer at a private event held recently that the individual was invited to. The individual provides the shop with sufficient information to determine when the event was held. The provision of access in this case would be reasonable and the shop should provide the photo which the individual requested.

14.10 In addition to the matters specified in the Fifth Schedule to the PDPA, section 21(3) specifies a number of situations in which an organisation must not provide the personal data or other information specified in section 21(1). A contravention of section 21(3) may render an organisation liable to the penalties and other remedies specified in the PDPA and possibly civil proceedings in accordance with the PDPA.

14.11 The situations specified in section 21(3) are where the provision of personal data or other information under section 21(1) 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.[11]

14.12 Section 21(4) of the PDPA contains an additional obligation of organisations in relation to the Access and Correction Obligation. That subsection provides that where an organisation has disclosed personal data to a prescribed law enforcement agency without the consent of the individual pursuant to paragraph 1(f) or (n) of the Fourth Schedule[12] or under any other written law, the organisation shall not inform the individual of that fact (that is, that personal data has been so disclosed). A contravention of section 21(4) will similarly render the organisation liable to the penalties and remedies specified in the PDPA.

Correction of personal data

14.13 Section 22(1) of the PDPA provides that an individual may submit a request for an organisation to correct an error or omission in the individual's personal data that is in the possession or under the control of the organisation (a "correction request"). Upon receipt of a correction request, the organisation is required to consider whether the correction should be made. In particular, section 22(2) goes on to provide that unless the organisation is satisfied on reasonable grounds that the correction should not be made, it should –

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

b) 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 request was made, unless that other organisation does not need the corrected personal data for any legal or business purpose.

14.14 The obligation in section 22(1) is subject to a number of exceptions in section 22 (6) and (7) considered below.

[11] The term "national interest" is defined in section 2(1) of the PDPA as including national defence, national security, public security, the maintenance of essential services and the conduct of international affairs.

[12] Paragraph 1(f) : the disclosure is necessary for any investigation or proceedings, or Paragraph 1(n): the personal data is disclosed to any officer of a prescribed law enforcement agency, upon production of written authorisation signed by the head or director of that law enforcement agency or a person of a similar rank, certifying that the personal data is necessary for the purposes of the functions or duties of the officer.

14.15 Regarding the obligation to notify other organisations of a correction, section 22(3) of the PDPA allows an organisation other than a credit bureau, with the consent of the individual concerned, to send the corrected personal data only to specific organisations to which the data was disclosed by the organisation within a year before the date the correction was made.

14.16 The other organisations which are notified of a correction made by an organisation responding to a correction request are required under section 22(4) to similarly correct the personal data in its possession or under its control unless satisfied on reasonable grounds that the correction should not be made.

Example:
An online retailer receives a request from a customer to update his address (which forms part of the customer's personal data). The retailer decides that there are no reasonable grounds to reject the customer's request and proceeds to correct the customer's address in its database.

The retailer also sends the corrected address to its affiliate which is responsible for servicing the customer's warranty as the affiliate may require such information for its own legal or business purposes. The affiliate determines that it does not require the corrected address for any legal or business purpose as the customer's warranty has expired. The affiliate therefore decides that a correction should not be made to all its records relating to the customer and makes a note that it has not made the correction.

The retailer determines that it need not send the corrected address to a courier company which had previously delivered certain products purchased from the retailer by the customer as the courier company was engaged to make the particular delivery and does not require an updated address of the customer for its own legal or business purposes.

14.17 If an organisation is satisfied upon reasonable grounds that a correction should not be made (whether the organisation is responding to a correction request or has been notified of a correction made by such an organisation), section 22(5) requires the organisation to annotate (that is, make a note to) the personal data in its possession or under its control indicating the correction that was requested but not made. As a good practice, the organisation may also wish to annotate the reasons why it has decided that the correction should not be made.

Exceptions to the obligation to correct personal data

14.18 Section 22(6) provides that an organisation is not required to correct or otherwise alter an opinion, including a professional or an expert opinion. In addition, section 22(7) provides that an organisation is not required to make a correction in respect of the matters specified in the Sixth Schedule. These include:

a) opinion data kept solely for an evaluative purpose;[13]

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; and

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

15 The Accuracy Obligation

15.1 Section 23 of the PDPA requires an organisation to make a reasonable effort to ensure that personal data collected by or on behalf of the organisation is accurate and complete, if the personal data:

a) is likely to be used by the organisation to make a decision that affects the individual to whom the personal data relates; or

b) is likely to be disclosed by the organisation to another organisation.

15.2 This obligation to ensure that personal data is accurate and complete is referred to in these Guidelines as the Accuracy Obligation.

[13] The term "evaluative purpose" is defined in section 2(1) of the PDPA.

15.3 Personal data may be inaccurate if it is incorrect or not updated. Similarly, personal data is incomplete if a relevant part of the data is missing or has not been included. The aim of the Accuracy Obligation is to ensure that where personal data may be used to make a decision that affects the individual, the data is reasonably correct and complete so as to ensure that the decision is made taking into account all relevant parts of accurate personal data.

15.4 In order to ensure that personal data is accurate and complete, an organisation must make a reasonable effort to ensure that:

a) it accurately records personal data which it collects (whether directly from the individual concerned or through another organisation);

b) personal data it collects includes all relevant parts thereof (so that it is complete);

c) it has taken the appropriate (reasonable) steps in the circumstances to ensure the accuracy and correctness of the personal data; and

d) It has considered whether it is necessary to update the information.

15.5 The Accuracy Obligation requires organisations to make a reasonable effort to ensure the accuracy and completeness of personal data. Hence the effort required of an organisation depends on the exact circumstances at hand. In determining what may be considered a reasonable effort, an organisation should take into account factors such as the following:

a) the nature of the data and its significance to the individual concerned (e.g. whether the data relates to an important aspect of the individual such as his health);

b) the purpose for which the data is collected, used or disclosed;

c) the reliability of the data (e.g. whether it was obtained from a reliable source or through reliable means);

d) the currency of the data (that is, whether the data is recent or was first collected some time ago); and

e) the impact on the individual concerned if the personal data is inaccurate or incomplete (e.g. based on how the data will be used by the organisation or another organisation to which the first organisation will disclose the data).

15.6 To be clear, an organisation is not required to check the accuracy and completeness of an individual's personal data each and every time it makes a decision about the individual. However, it would be prudent for an organisation to do so if it intends to make a decision that will significantly impact the individual concerned.

15.7 An organisation may, in many circumstances, presume that personal data provided directly by the individual concerned is accurate. However, an organisation should be alert to the circumstances where it should not make such a presumption, e.g. where it is in the individual's interest to provide inaccurate personal data. In addition, where the currency of the personal data is important, the organisation should take steps to verify that the personal data provided by the individual is up to date (for example, before making a decision affecting the individual).

15.8 An organisation should also be more careful when collecting personal data about an individual from a source other than the individual in question. It is allowed to take differing approaches to ascertain the accuracy and completeness of personal data it collects depending on the reliability of the source of the data. For example, the organisation may obtain confirmation from the source of the personal data that the source had verified the accuracy and completeness of that personal data. However, if the organisation has reason to believe that the source may not be reliable or if the organisation will be using the personal data in a manner that significantly affects the individual in question, it may need to take further action to verify the data. It may also conduct further independent verification if it deems prudent to do so.

Example:
Nick applies for a home loan from a bank. The bank asks Nick to provide relevant details such as his name, address, current employment status and income, which constitute personal data, in order to assess whether to provide the loan to Nick. Related to this, the bank asks Nick to provide supporting documents including an identity document and his most recent payslip, in order to verify the information provided by Nick. It also asks Nick to declare that the information he has provided is accurate and complete. In this scenario, the bank has made a reasonable effort to ensure that the personal data collected from Nick is accurate and complete.

Nick will be attending an adventure camp for his company's team-building purposes. The adventure camp operator obtains relevant health check-up records from his company to determine whether Nick is sufficiently fit to participate in the adventure activities. The records were from eight years ago when Nick first joined the company. In this scenario, the adventure camp

company should consider requesting that Nick or his company updates his health check-up records to provide a more accurate indication of Nick's fitness for the adventure camp.

15.9 Similar considerations apply when deciding whether personal data should be updated. Not all types of personal data require updates. Obvious examples include factual data, for example, historical data. However, where the use of outdated personal data in a decision-making process could affect the individual, then it would be prudent for the organisation to update such personal data.

Example:
A company is considering whether an existing employee, John, should be transferred to take on a different role in its IT department. One of the criteria for the transfer is the possession of certain qualifications and professional certifications. The company has information about John's qualifications and professional certifications that was provided by John (which form part of his personal data) when he joined the company five years before.

The company asks John to update them with any additional qualifications or certifications he may have obtained in the last five years (since joining the company) but does not ask him to re-confirm the information he provided when he joined the company. In this scenario, the company is likely to have met its obligation to update John's personal data.

16 The Protection Obligation

16.1 Section 24 of the PDPA requires an organisation to make reasonable security arrangements to protect personal data in its possession or under its control in order to prevent unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks. This obligation of organisations to protect personal data is referred to in these Guidelines as the Protection Obligation.

16.2 There is no 'one size fits all' solution for organisations to comply with the Protection Obligation. Each organisation should consider adopting security arrangements that are reasonable and appropriate in the circumstances, for example, taking into consideration the nature of the personal data, the form in which the personal data has been collected (e.g. physical or electronic) and the possible impact to the individual concerned if an unauthorised person obtained, modified or disposed of the personal data. For example, in the employment context, it would be reasonable to expect a greater level of security for highly confidential employee appraisals as compared to more general information about the projects an employee has worked on.

16.3 In practice, an organisation should:

a) design and organise its security arrangements to fit the nature of the personal data held by the organisation and the possible harm that might result from a security breach;

b) identify reliable and well-trained personnel responsible for ensuring information security;

c) implement robust policies and procedures for ensuring appropriate levels of security for personal data of varying levels of sensitivity; and

d) be prepared and able to respond to information security breaches promptly and effectively.

16.4 In addition, it might be useful for organisations to undertake a risk assessment exercise to ascertain whether their information security arrangements are adequate. In so doing, the following factors may be considered:

a) the size of the organisation and the amount and type of personal data it holds;

b) who within the organisation has access to the personal data; and

c) whether the personal data is or will be held or used by a third party on behalf of the organisation.

16.5 Security arrangements may take various forms such as administrative measures, physical measures, technical measures or a combination of these. The following tables list examples of such measures.

Examples of administrative measures an organisation may use to protect personal data:

- Requiring employees to be bound by confidentiality obligations in their employment agreements;
- Implementing robust policies and procedures (with disciplinary consequences for breaches) regarding confidentiality obligations;
- Conducting regular training sessions for staff to impart good practices in handling personal data and strengthen awareness of threats to security of personal data;
- Ensuring that only the appropriate amount of personal data is held, as holding excessive data will also increase the efforts required to protect personal data;
  and
- Implementing a business continuity plan as a contingency measure in the event that personal data is lost.

Examples of physical measures an organisation may use to protect personal data:

- Marking confidential documents clearly and prominently;
- Storing confidential documents in locked file cabinet systems;
- Restricting employee access to confidential documents on a need-to-know basis;
- Using privacy filters to minimise unauthorised personnel from viewing personal data on laptops;
- Proper disposal of confidential documents that are no longer needed, through shredding or similar means;
- Implementing an intended mode of delivery or transmission of personal data that affords the appropriate level of security (e.g., registered post instead of normal post where appropriate);
- Providing a summary of the personal data contained in storage so that personal data is accessed only when necessary; and
- Confirming that the intended recipient of personal data is the correct recipient to avoid undue disclosure of personal data.

Examples of technical measures an organisation may use to protect personal data:

- Ensuring computer networks are secure;
- Adopting appropriate access controls (e.g. considering stronger authentication measures where appropriate);
- Encrypting personal data to prevent unauthorised access;
- Activating self-locking mechanisms for the computer screen if the

computer is left unattended for a certain period;
- Installing appropriate computer security software and using suitable computer security settings;
- Disposing of personal data in IT devices that are to be recycled, sold or disposed;
- Using the right level of email security settings when sending and/or receiving highly confidential emails;
- Updating computer security and IT equipment regularly; and
- Ensuring that IT service providers are able to provide the requisite standard of IT security

17 The Retention Limitation Obligation

17.1 Section 25 of the PDPA requires an organisation to cease to retain its documents containing personal data, or remove the means by which the personal data can be associated with particular individuals, as soon as it is reasonable to assume that the purpose for which that personal data was collected is no longer being served by retention of the personal data, and retention is no longer necessary for legal or business purposes. This obligation to cease to retain personal data is referred to in these Guidelines as the Retention Limitation Obligation.

Retention of personal data

17.2 The Retention Limitation Obligation prevents organisations from retaining personal data in perpetuity where it does not have legal or business reasons to do so. Holding personal data for an indeterminate duration of time increases the risk of a contravention of the Data Protection Provisions. However, as each organisation has its own specific business needs, the Retention Limitation Obligation does not specify a fixed duration of time for which an organisation can retain personal data. Instead, the duration of time for which an organisation can legitimately retain personal data is assessed on a standard of reasonableness, having regard to the purposes for which the personal data was collected and other legal or business purposes for which retention of the personal data may be necessary.

17.3 It should be noted that although the PDPA does not prescribe a specific retention period for personal data, organisations would need to comply with any legal or specific industry-standard requirements that may apply.

17.4 In practice, the retention period for personal data under the PDPA will depend on the following factors:

a) The purpose(s) for which the personal data was collected. That is:

i. personal data may be retained so long as one or more of the purposes for which it was collected remains valid; and

ii. personal data should not be kept by an organisation "just in case" it may be needed.

Example:
A dance school has collected personal data of its tutors and students. It retains and uses such data (with the consent of the individuals), even if a tutor or student is no longer with the dance school, for the purpose of maintaining an alumni network. As the dance school is retaining the personal data for a valid purpose, it is not required to cease to retain the data under the Retention Limitation Obligation.

A retailer retains billing information, including personal data, collected from its customers beyond the Point of Sale for the purposes of accounting and billing administration. As the retailer is retaining the personal data for a valid purpose, it is not required to cease to retain the data under the Retention Limitation Obligation.

b) Other legal or business purposes for which retention of the personal data by the organisation is necessary. For example, this may include situations where:

i. the personal data is required for an ongoing legal action involving the organisation;

ii. retention of the personal data is necessary in order to comply with the organisation's obligations under other applicable laws, regulations, international/regional /bilateral standards which require the retention of personal data; or

iii. the personal data is required for an organisation to carry out its business operations, such as to generate annual reports, or performance forecasts.

Example:
Under the Limitation Act (Cap. 163), actions founded on a contract (amongst others) must be brought within 6 years from the date on which the cause of action accrued. Hence an organisation may wish to retain records relating to its contracts for 7 years from the date of termination of the contract and possibly for a longer period if an investigation or legal proceedings should commence within that period.

17.5 An organisation should review the personal data it holds on a regular basis to determine if that personal data is still needed. An organisation which holds a larger quantity of different types of personal data may have to implement varying retention periods for each type of personal data as appropriate.

17.6 In many instances, organisations may already have their own policies regarding retention of documents, which may touch on the duration for which such documents should be kept. These policies will now be subject to the requirements of the Retention Limitation Obligation. As a best practice, organisations should prepare an appropriate personal data retention policy which sets out the organisation's approach to retention periods for personal data that they hold. Where personal data is held for a relatively long period of time, an organisation should set out its rationale for doing so in its personal data retention policy.

Ceasing to retain or anonymising personal data

17.7 Where there is no longer a need for an organisation to retain personal data, it must take prompt action to ensure it does not hold such personal data in either one of the two ways set out under the PDPA. That is, an organisation may cease to retain the documents containing personal data or it may remove the means by which the personal data may be associated with particular individuals (that is, to anonymise the data).

17.8 An organisation ceases to retain documents containing personal data where, for example, these documents are destroyed or disposed of in an appropriate manner, returned to the individual concerned or transferred to another person on the instructions of the individual concerned.

17.9 An organisation would not have ceased to retain documents containing personal data where it has merely filed the documents in a locked cabinet, warehoused the documents or transferred them to a party who is subject to the organisation's control in relation to the documents. In such circumstances, the organisation would be considered to be retaining the documents. This also applies to documents in electronic form. Hence, documents in electronic form which are archived or to which access is limited are also considered to be retained for the purposes of the Retention Limitation Obligation.

17.10 An organisation will be considered to have removed the means by which the personal data can be associated with particular individuals if such personal data is anonymised. Anonymisation is the process of removing identifying information, such that the remaining data does not identify any particular individual. More details are available in the section on Anonymisation in the Advisory Guidelines on Selected Topics in the PDPA.

18 The Transfer Limitation Obligation

18.1 Section 26 of the PDPA limits the ability of an organisation to transfer personal data outside Singapore. In particular, section 26(1) provides that an organisation must not transfer any personal data to a country or territory outside Singapore except in accordance 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. This requirement not to transfer personal data unless in accordance with the prescribed requirements is referred to in these Guidelines as the Transfer Limitation Obligation.

18.2 The requirements relating to the transfer of personal data under section 26(1) may include putting in place the appropriate contractual arrangements or binding corporate rules to govern the transfer of the personal data.[14]

19 The Openness Obligation

19.1 The Data Protection Provisions contain a number of obligations in various sections which require organisations to develop and implement policies and practices that are necessary for the organisation to meet its obligations under the PDPA ("data protection policies and practices") and to make information about their data protection policies and practices available. These obligations are collectively referred to in these Guidelines as the Openness Obligation.

19.2 In particular:

a) section 12 of the PDPA requires organisations to undertake a number of tasks relating to their data protection policies and practices; and

[14] The Commission is currently consulting on these matters in the Proposed Regulations for Personal Data Protection in Singapore.

b) the following sections of the PDPA require organisations to designate one or more individuals to be responsible for the organisation's compliance with the PDPA and to answer questions relating to certain of their data protection policies and practices:

i. section 11;

ii. section 20(1)(c); and

iii. section 20(4).

19.3 Section 12 of the PDPA sets out the general obligations of an organisation in respect of its data protection policies and practices. Under section 12, organisations are required to:

a) develop and implement its data protection policies and practices (that is, policies and practices that are necessary for the organisation to meet its obligations under the PDPA);

b) develop a process to receive and respond to complaints that may arise with respect to the application of the PDPA;

c) communicate to its staff information about its data protection policies and practices; and

d) make information available on request about its data protection policies and practices and its process to receive and respond to complaints.

19.4 Section 11 of the PDPA sets out the general obligation of an organisation to designate an individual responsible for ensuring its compliance with the PDPA. In particular, section 11(3) provides that an organisation shall designate one or more individuals to be responsible for ensuring that the organisation complies with the PDPA. Section 11(4) further provides that an individual so designated by an organisation may delegate the responsibility conferred by that delegation to another individual. These provisions require organisations to designate the appropriate individuals, who may in turn delegate certain responsibilities to other officers, to ensure that the organisation complies with the PDPA.

19.5 Section 11(6) clarifies that the designation of an individual by an organisation does not relieve the organisation of any of its obligations under the PDPA. That is, legal responsibility for complying with the PDPA remains with the organisation and does not "pass" to the individual designated by the organisation.

19.6 Section 11(6) requires an organisation to make available the business contact information of at least one individual designated by the organisation under section 11(3) while sections 20(1)(c) and 20(4) require an organisation to make available the business contact information of a person who is able to answer questions on behalf of the organisation relating to the collection, use or disclosure of personal data. These individuals and persons may be the same individual or the organisation may have different persons undertake such roles.

19.7 As a best practice, the business contact information of the relevant person should be readily accessible from Singapore, operational during Singapore business hours and in the case of telephone numbers, be Singapore telephone numbers. This would facilitate the organisation's ability to respond promptly to any complaint or query on its data protection policies and practices.

Accountability

19.8 An important point to note in respect of the Data Protection Provisions is that organisations are accountable for their compliance with the Data Protection Obligations in a number of ways:

a) individuals may request for access to their personal data in the possession or under the control of an organisation, which enables them to find out which of their personal data may be held by an organisation and how it has been used;

b) individuals may submit a complaint to the Commission and the Commission may review or investigate an organisation's conduct and compliance with the PDPA;[15]

c) the Commission may, if satisfied that an organisation has contravened the Data Protection Provisions, give directions to the organisation to ensure compliance including (amongst others) imposing a financial penalty of up to $1 million; and

d) individuals who suffer loss or damage directly as a result of a contravention of Parts IV, V or VI of the PDPA by an organisation may commence civil proceedings against the organisation.[16]

[15] Sections 28 and 29 of the PDPA specify what the PDPA may do upon a review or investigation respectively.

PART IV: OTHER RIGHTS, OBLIGATIONS AND USES

20 Overview

20.1 The Data Protection Provisions will come into operation on a date specified by the Minister, referred to in the PDPA as the "appointed day". Before the appointed day, organisations may have collected, used and disclosed personal data and there may be existing contracts, between organisations or between an organisation and an individual, which relate to the personal data of individuals in some way. In addition, there may be existing laws that confer rights or impose obligations relating to personal data.

20.2 Once the Data Protection Provisions take effect on the appointed day, organisations will be required to comply with the Data Protection Provisions and hence some of the existing rights, obligations and legal relationships will be affected. In this regard, the PDPA includes provisions that specify how the Data Protection Provisions will apply in relation to, amongst other things, existing rights, obligations and uses of personal data. The PDPA's provisions specify the following:

a) The Data Protection Provisions will not affect any authority, right, privilege, immunity, obligation or limitation arising under the law, except that performance of a contractual obligation shall not be an excuse for contravening the PDPA;

b) Other written laws shall prevail over the Data Protection Provisions in the event of an inconsistency between them; and

c) An organisation may continue to use personal data that was collected before the appointed day for the purposes for which it was collected unless consent is withdrawn under the PDPA or the individual had otherwise indicated that he does not consent to such use.

20.3 Each of the above is considered in greater detail in the following sections.

---

[16] Parts IV, V and VI of the PDPA relate respectively to (a) collection, use and disclosure of personal data, (b) access to and correction of personal data and (c) care of personal data (containing provisions relating accuracy, protection, retention and transfer of personal data).

21 Existing rights, etc under law

21.1 Section 4(6)(a) of the PDPA provides that the Data Protection Provisions will not affect any authority, right, privilege or immunity conferred, or obligation or limitation imposed, by or under the law, except that performance of a contractual obligation shall not be an excuse for contravening the PDPA. This applies whether such rights, obligations, etc. arise under any written law, such as obligations within Codes of Practice, licences, regulatory directives issued under written law, or under the common law.[17]

21.2 However, section 4(6)(a) does not apply in respect of rights and obligations arising under a contract as an organisation's performance of a contractual obligation will not excuse it from complying with the PDPA. Hence, an organisation will not be able to claim that they are exempt from, or need not comply with, the PDPA while performing a contractual obligation.

Example:
A retailer has entered into a contract with a data aggregator under which it has agreed to sell certain personal data about its customers to the aggregator. The personal data involved includes the customers' names, contact details and certain information on products they have purchased from the retailer. However, the retailer did not obtain the consent of the customers to disclose their personal data. With effect from the appointed day, the retailer must comply with the Data Protection Provisions and cannot assert its contractual obligations to the aggregator as a reason that it does not need to obtain the consent of its customers.

22 Other written law

22.1 Section 4(6)(b) of the PDPA provides that the provisions of other written law shall prevail over the Data Protection Provisions to the extent that any Data Protection Provision is inconsistent with the provisions of the other written law. Other written law includes the Constitution of Singapore, Acts of Parliament and subsidiary legislation such as regulations.[18]

[17] Please refer to section 5.3 of these Guidelines for more information concerning written law.

[18] More specifically, section 2(1) of the Interpretation Act (Cap. 1) defines "written law" as "the Constitution and all previous Constitutions having application to Singapore and all Acts, Ordinances and enactments by whatever name called and subsidiary legislation made thereunder for the time being in force in Singapore".

22.2 Under section 4(6)(b) of the PDPA, in the event that a particular provision in the PDPA is inconsistent with a provision in any other written law in some way, then the provision in the other written law will prevail to the extent of the inconsistency. That is, the provision of the other written law will apply only in respect of the matter(s) which is inconsistent between the two provisions. Other provisions in the PDPA which are not inconsistent with the other written law will continue to apply.

Example:
Section 47 of the Banking Act (Cap. 19) permits a bank to disclose customer information for such purposes and to such persons as are specified in the Third Schedule to the Banking Act (subject to the conditions specified). To the extent that any of the Data Protection Provisions is inconsistent with a provision the Third Schedule to the Banking Act, for example, in relation to obtaining consent for disclosure of personal data for a purpose specified in the Third Schedule to the Banking Act, the provisions in the Third Schedule shall prevail. However, the Data Protection Provisions will continue to apply in respect of other purposes which are not specified in the Third Schedule and also to the extent they are not inconsistent with the provisions of the Third Schedule.

23 Use of personal data collected before the appointed day

23.1 The Data Protection Provisions in the PDPA will only take effect on the appointed day. Section 19 of the PDPA provides that notwithstanding the other provisions of Part III of the PDPA (which relate to collection, use and disclosure of personal data), an organisation may use personal data collected before the appointed day for the purposes for which the personal data was collected, unless consent for such use is withdrawn or the individual indicates or has indicated to the organisation that he does not consent to the use of the personal data. Such 'use' could include disclosure that is necessarily part of the organisation's use of such personal data. However, the PDPA does not include any similar provision in relation to the collection of or disclosure of such personal data.

23.2 Hence, in relation to personal data that was collected before the appointed day, the PDPA applies as follows:

a) For collection:

i. the PDPA does not apply to collection of personal data before the appointed day; and

ii. if an organisation intends to collect the same type of personal data on or after the appointed day (e.g. where a service provider collects certain personal data from a customer before and after the appointed day), the organisation must comply with the Data Protection Provisions in relation to such collection;

b) For use:

i. the PDPA does not apply to any use of such personal data before the appointed day; and

ii. an organisation may use such personal data on or after the appointed day in accordance with section 19 (noted above) or otherwise in accordance with the other Data Protection Provisions (e.g. by obtaining consent for a new use); and

c) For disclosure:

i. the PDPA does not apply to any disclosure of such personal data before the appointed day; and

ii. if an organisation intends to disclose the personal data on or after the appointed day (other than disclosure that is necessarily part of the organisation's use of the personal data), the organisation must comply with the Data Protection Provisions in relation to such disclosure.

23.3 The effect of Section 19 is that organisations can continue to use personal data collected before the appointed day for the same purposes for which the personal data was collected without obtaining fresh consent, unless the individual has withdrawn consent (whether before on, or after the appointed day). Organisations should note that Section 19 only applies to 'reasonable existing uses' of personal data collected before the appointed day.

Example:
Organisation ABC has been using the personal data of their customers to send them desktop calendars once every year. This would be considered a reasonable existing use So long as their customers have not indicated to ABC that they no longer wish to receive these calendars (i.e. withdrawing their consent for the purpose of receiving calendars once every year), ABC can continue to do so without obtaining fresh consent after the appointed day.

Organisation XYZ has been selling databases containing personal data. This would be considered a disclosure of personal data and not a

reasonable existing use under Section 19. After the appointed day, XYZ needs to ensure that consent has been obtained before selling these databases again.

23.4 Section 19 permits the use of personal data for the purposes for which it was collected. It is not necessary that such purposes have been specified in some manner or notified to the individuals concerned. However, as such purposes may not necessarily have been made clear, an organisation should consider documenting such purposes so that it will have such information readily available in the event a question arises as to whether it is using personal data for the purposes for which the data was collected or other purposes (in which case, the organisation is required to comply with Part III of the PDPA). In particular, when considering whether a purpose falls within the scope of the original purposes for which personal data was collected, an organisation may consider the following:

a) how the purpose relates to the original purposes of collection e.g. whether it is necessary to fulfil the original purpose of collection; and

b) whether it would be clear to the individual concerned that the purpose falls within the scope of the original purposes.

23.5 An organisation can use personal data under section 19 unless the individual withdraws consent in accordance with section 16 of the PDPA or the individual indicates, whether before or after the appointed day, that he does not consent to that use of his or her personal data. Hence if an individual had indicated at some point, for example, when he provided the personal data (before the appointed day) that he did not consent to a particular use, the organisation would not be able to use personal data in that manner. Similarly, if an individual withdraws consent to the use of his personal data, the organisation should cease to use the personal data and comply with the other obligations in section 16 of the PDPA.

PART V: THE DO NOT CALL PROVISIONS

24 Overview

24.1 In addition to the Data Protection Provisions, organisations are required to comply with the Do Not Call Provisions in Part IX of the PDPA.[19] The Do Not Call Provisions contain a number of obligations that apply in relation to an organisation sending specified messages to Singapore telephone numbers.[20] In particular, organisations are required to perform the following obligations (the specific sections of the PDPA under which these obligations arise are noted for reference):

a) Duty to check the Do Not Call Register – before sending a specified message to a Singapore telephone number, the organisation must check with the Do Not Call registry established by the Commission under the PDPA (the "Do Not Call Registry") to confirm that the number is not listed on a Do Not Call Register established by the Commission as part of the Do Not Call Registry, unless it has obtained the consent of the user or subscriber of the number[21] (section 43 of the PDPA);

b) Duty to identify the sender of a message – when sending a specified message to a Singapore telephone number, the organisation must:

i. include information identifying the sender and how the individual can contact the sender (section 44 of the PDPA); and

[19] As drafted, the Do Not Call Provisions impose obligations on a "person" sending specified messages and not an "organisation". However, as may be seen from the respective definitions of "person" and "organisation" in section 2(1) of the Interpretation Act and section 2(1) of the PDPA, both terms include natural persons as well as companies, associations and other bodies of persons, corporate or unincorporated. For the avoidance of doubt, the term "organisation" as used in this section of the Guidelines shall be construed as a reference to a "person".

[20] The term "Singapore telephone number" is defined in section 36(1) of the PDPA to include a telephone number beginning with the digit 3, 6, 8 or 9 that is in accordance with the National Number Plan issued by the Infocomm Development Authority of Singapore (as referred to in regulation 12A of the Telecommunications (Class Licence) Regulations (Cap. 323, Rg 3).

[21] The term "subscriber" is defined in section 36(1) as the subscriber of the telecommunications service to which the Singapore telephone number in question is allocated.

ii. not conceal or withhold from the recipient the sender's calling line identity[22] (section 45 of the PDPA).

24.2 In order to understand how the Do Not Call Provisions apply, it is important to take note of what constitutes a "specified message", who is a "sender" and what constitutes sending a message to a Singapore telephone number under the PDPA. These issues, as well as the scope of the above obligations, are explained in the following sections.

25 Locations of sender and recipient

25.1 It should be noted that the locations of the sender and recipient of the specified message affects whether the Do Not Call Provisions apply. Section 38 of the PDPA provides that the Do Not Call Provisions apply where:

a) the sender of the specified message is in Singapore when the message is sent; or

b) the recipient of the specified message is in Singapore when the message is accessed.

25.2 Under section 38, the Do Not Call Provisions do not apply if both the sender and the recipient are not in Singapore when the message is sent and accessed respectively. This may be the situation, for example, when the recipient is travelling in another country and receives a message sent by an organisation in that country. However, the Do Not Call Provisions would apply if the recipient is travelling in another country and the sender is an organisation in Singapore. The Do Not Call Provisions also apply if the recipient returns to Singapore from overseas when he accesses the message. This requirement addresses the situation where one of the senders is located overseas while another is located in Singapore.

Example:
Charles subscribes to the services of Operator X, a Singapore telecommunications service provider. He leaves Singapore and starts roaming on the network of an overseas telecommunications provider, Operator A. He receives a specified message from Operator A, a telecommunications service provider in the other country, about Operator A's services. The sending of this specified message will not be subject to the application of the Do Not Call Provisions.

[22] The term "calling line identity" is defined in section 36(1) as the telephone number or information identifying the sender.

Later in the day (while Charles is still in the other country), he receives another specified message, this time from his insurance agent who was in Singapore when the message was sent. The sending of the specified message by Charles' insurance agent will be subject to the application of the Do Not Call Provisions.

A few days later, Charles returns to Singapore. Shortly thereafter, he receives a third specified message, now from an overseas number. However, Charles discovers that the specified message was sent on behalf of his bank in Singapore which had outsourced part of its marketing operations to an overseas call centre and authorised the call centre to send the message. The sending of the specified message by the bank (through the overseas call centre) will also be subject to the application of the Do Not Call Provisions.

26 Meaning of "specified message"

26.1 The Do Not Call Provisions contain obligations which relate to the sending of a "specified message". Section 37 of the PDPA defines what constitutes a "specified message" for the purposes of the Do Not Call Provisions. Under section 37(1), a message is a specified message if the purpose of the message, or one of its purposes, is –

a) to advertise, promote or offer to supply or provide any of the following:

i. goods or services;[23]

ii. land or an interest in land; or

[23] The terms "goods" and "services" are defined in section 36(1) of the PDPA, as follows:

"goods" means any personal property, whether tangible or intangible, and shall be deemed to include (a) chattels that are attached or intended to be attached to real property on or after delivery; (b) financial products and credit, including credit extended solely on the security of land; (c) any residential property; or (d) a voucher;

"services" includes (a) a service offered or provided that involves the addition to or maintenance, repair or alteration of goods or any residential property; (b) a membership in any club or organisation if the club or organisation is a business formed to make a profit for its owners; (d) the right to use time share accommodation (as defined in section 36(1)) under a time share contract(as defined in section 36(1)); and (e) financial services (as defined in section 2 of the Consumer Protection (Fair Trading) Act (Cap. 52A).

iii. a business opportunity or an investment opportunity;

b) to advertise or promote a supplier/provider (or a prospective supplier/provider) of the items listed in sub-paragraphs (I) to (III) above; or

c) any other prescribed purpose related to obtaining or providing information.[24]

26.2 In most instances, a marketing message of a commercial nature would be a specified message within the meaning of the PDPA. Section 37(1) is subject to certain exceptions under section 37(5) (noted below).

26.3 Messages sent for a purpose which is not specified in paragraphs (a) to (c) above would not be a specified message for the purposes of the PDPA. For example, a message sent solely to promote an employment opportunity, to solicit donations for a charitable cause or to promote a political cause would not be regarded as a specified message.

26.4 In order to determine whether the purpose (or one of the purposes) of a message falls within the meaning of a specified message, section 37(1) specifies that the following would be taken into consideration:

a) the content and presentation of the message; and

b) the content that may be obtained through the message, that is, by using the numbers, URLs or contact information (if any) included in the message or by calling the telephone number from which the message was sent.

26.5 Section 37(1) does not refer to other matters relating to the goods, services or other items specified in that section. Hence, matters such as the quality of the goods, the terms and conditions under which the items would be supplied or whether the items are offered to the recipient at an attractive price or free of charge would not affect whether a message is a specified message.

26.6 It should be noted that under section 37(2), it is immaterial whether the goods, services, land, interest or opportunity exist, or if it's lawful to acquire the goods, services, land or interest or take up the opportunity. Hence an organisation cannot cite as a defence the fact that, for example, the goods if had offered in a specified message were actually not available for purchase.

[24] There are presently no such other prescribed purposes.

27 Exclusions from the meaning of "specified message"

27.1 Section 37(5) provides that a specified message will not include any of the messages referred to in the Eighth Schedule to the PDPA. The types of message referred to in the Eighth Schedule are therefore not specified messages for the purpose of the Do Not Call Provisions and are not subject to the application of those provisions. The types of message excluded under the Eighth Schedule include the following:

a) any message sent by a public agency under, or to promote, any programme carried out by any public agency which is not for a commercial purpose;[25]

b) any message sent by an individual acting in a personal or domestic capacity;

c) any message which is necessary to respond to an emergency that threatens the life, health or safety of any individual;

d) any message sent to an organisation other than an individual acting in a personal or domestic capacity, for any purpose of the receiving organisation;

e) any message the sole purpose of which is –

i. to facilitate, complete or confirm a transaction that the recipient of the message has previously agreed to enter into with the sender;

ii. to provide warranty information, product recall information or safety or security information with respect to a product or service purchased or used by the recipient of the message; or

iii. to deliver goods or services, including product updates or upgrades, that the recipient of the message is entitled to receive under the terms of a transaction that the recipient has previously agreed to enter into with the sender;

f) any message the sole purpose of which is to provide –

i. notification concerning a change in the terms or features of;

[25] The term "public agency" is defined in section 2(1) of the PDPA.

ii. notification of a change in the standing or status of the recipient of the message with respect to; or

iii. at regular periodic intervals, account balance information or other type of account statement with respect to, a subscription, membership, account, loan or comparable ongoing commercial relationship involving the ongoing purchase or use by the recipient of goods or services offered by the sender; or

g) any message the sole purpose of which is to conduct market research or market survey.

27.2 An organisation sending a message that falls within one of the excluded purposes specified in Eighth Schedule (or which is not listed in section 37(1)) should note that it should not use that message for other purposes listed in section 37(1) of the PDPA which are not separately excluded under the Eighth Schedule. Should it do so, the message will still be a specified message and the organisation will be required to comply with the Do Not Call Provisions in relation to the sending of that message.

Example:
An organisation, ABC, is a market research firm that has been engaged to produce a report which illustrates the correlation between investment habits and income, profession and marital status of working Singaporeans aged 25-40. ABC calls Sarah for the sole purpose of gathering information for the report. As the sole purpose of ABC's call is to conduct market research or a market survey, the call falls within an exclusion in the Eighth Schedule and ABC is not considered to have sent a specified message.

ABC also calls John to gather information for the report. After John finishes answering all the questions related to the report, ABC asks if John would consider purchasing one of ABC's market reports. In this case, ABC's call is not for the sole purpose of market research or market survey as one of the purposes of the call is to offer goods or services to John. Hence, ABC would be considered to have sent a specified message to John.

28 Business to Business ("B2B") marketing messages

28.1 As noted above, one of the types of excluded messages specified in the Eighth Schedule relates to messages sent by an organisation to another organisation other than an individual acting in a personal or domestic capacity, for any purpose of the receiving organisation. This exclusion addresses B2B marketing messages and purposes, for example, where a company wishes to market its goods or services to another company for the purposes of the other company.

Example:
John calls an employee of ABCD Childcare Pte Ltd ("ABCD"), Mary, through her business contact number (which John obtained from ABCD's website) to promote a product which he thinks ABCD would purchase for use at its childcare centres. Such a call is not a specified message for the purposes of the Do Not Call Provisions.

However, while talking to Mary, John asks her if she has children and whether she would be interested to buy another product for her personal use. In such a situation, John would not be able to rely on this exception, and will need to ensure that he complies with the Do Not Call Provisions.

29 Meaning of "sender"

29.1 As noted above, the Do Not Call Provisions contain obligations in relation to the sending of a specified message. Hence the party who sends a specified message, referred to in the PDPA as the "sender", is responsible to comply with the Do Not Call Provisions. The term "sender" is defined in section 36(1) of the PDPA as follows:

"sender", in relation to a message, means a person –

a) *who sends the message, causes the message to be sent, or authorises the sending of the message; or*

b) *who makes a voice call containing the message, causes a voice call containing the message to be made, or authorises the making of a voice call containing the message;*

29.2 The definition of a "sender" includes the following persons:

a) the person who actually sends the message or makes a voice call containing the message;

b) the person who caused the message to be sent or the voice call to be made; and

c) the person who authorised the sending of the message or the making of the call;

29.3 Hence it is important to note that in addition to the person who actually sent the message or made a call containing the message, persons who caused or authorised the sending of the message or the making of the call are also senders for the purposes of the Do Not Call Provisions and must comply with these provisions. This means that if Person A authorises the sending of the message by Person B, Person A would be considered the sender regardless of Person's A instructions to Person B.

29.4 Section 37 (3) and (4) of the PDPA clarifies when a person is considered to have authorised another to send a message. These provisions state:

Subject to subsection (4), a person who authorises another person to offer, advertise or promote the first person's goods, services, land, interest or opportunity shall be deemed to have authorised the sending of any message sent by the second person that offers, advertises or promotes that first person's goods, services, land, interest or opportunity.

For the purposes of subsection (3), a person who takes reasonable steps to stop the sending of any message referred to in that subsection shall be deemed not to have authorised the sending of the message.

29.5 Under section 37(3) and (4), if Person A authorises Person B to promote his goods, services, land, interest or opportunity, Person A would be deemed to have authorised the sending of any message for that purpose, unless Person A had taken reasonable steps to prevent Person B from doing so. The determination of whether reasonable steps had been taken would depend on the specific facts in question. For example, reasonable steps may include requiring, as a condition of the authorisation given, that Person B shall not promote Person A's goods by sending specified messages addressed to Singapore telephone numbers.

Example:
Charles wishes to offer his services as a real estate agent. He engages Mary to promote his services. In the contract between Charles and Mary, it is stated that, "Mary shall not send any message, whether in sound, text, visual or other form, to a Singapore telephone number to offer, advertise or promote Charles' services unless expressly permitted in writing by Charles". If Mary sends SMS messages to a Singapore telephone number to promote Charles' services without Charles written permission, Charles would not be

deemed to have authorised that, as he had taken reasonable steps to prevent Mary from doing so.

John also wishes to offer his services as a real estate agent and engages Mary to market his services. John does not specify the manner of marketing to Mary. John and Mary will both be considered the sender of any SMS messages sent to promote John's services, and will both be subject to the Do Not Call Provisions.

30 Exclusions

30.1 The PDPA excludes certain categories of organisations from the scope of a "sender" to the extent that the sending of the message does not involve active intervention on their part. Specifically, under section 36 (2) and (3) of the PDPA, the following organisations are presumed not to have sent or authorised the sending of a message unless the contrary is proved:

a) a telecommunications service provider who merely provides a service that enables the sending of a specified message; and

b) the owners or authorised users of a telecommunication device, service or network that was used to send a specified message if, at the relevant time, that device, service or network was controlled by a person without the knowledge of the owner or authorised users.[26]

30.2 As the Do Not Call Provisions impose obligations on individuals as well as corporate entities such as companies, the PDPA recognises that there are certain situations in which it would not be appropriate to require individuals to comply with the Do Not Call Provisions. Apart from the exclusion for messages sent by an individual acting in his personal or domestic capacity (noted above), the PDPA includes a specific defence for individuals acting as employees.

[26] Section 36(4) clarifies that such control may include physical control or control through the use of software or other means.

30.3 Under section 48, an employee who did an act or engaged in conduct that would be a contravention of one of the Do Not Call Provisions has a defence to any proceedings that may be brought against him for an offence under the Do Not Call Provisions if he can prove that he did the act or engaged in the conduct in good faith in the course of his employment or in accordance with instructions given to him by or on behalf of his employer in the course of his employment.[27]

31 Sending a specified message to a Singapore telephone number

31.1 As the Do Not Call Provisions apply in relation to the sending of a specified message to a Singapore telephone number, it is important to note what constitutes the sending of a message to a Singapore telephone number. Section 36(1) of the PDPA defines the term "send" as referring to:

a) the sending of the message;

b) causing or authorising the sending of the message; or

c) the making of a voice call containing the message, or causing or authorising the making of such a voice call.[28]

31.2 Related to the above, the PDPA recognises that a message may be sent in a number of different forms. Hence, section 36(1) of the PDPA defines "message" to include a message in sound, text, visual or other form.

31.3 From the above definitions, it is important to note that the Do Not Call Provisions apply equally to all means by which a sender may send a specified message to a Singapore telephone number. These include, for example, voice calls, SMS, or any data applications which use a Singapore Telephone Number such as 'Whatsapp', 'iMessage' or 'Viber'.

---

[27] Under section 48 (2) and (3), the defence in section 48(1) is not available to an officer of an organisation that may have committed an offence under the Do Not Call Provisions and who is liable to be proceeded against under section 52 of the PDPA.

[28] The term "voice call" is defined in section 36(1) of the PDPA to include (a) a call that involves a recorded or synthetic voice and (b) in the case of a recipient with a disability (for example, a hearing impairment), a call that is equivalent to a voice call, whether or not the recipient responds by way of pressing buttons on a telephone handset or similar telecommunications device.

31.4 However, the Do Not Call Provisions do not apply to specified messages which are not sent to a Singapore telephone number, e.g. location-based broadcasts that are pushed to mobile phones through data-enabled smart phone applications or data applications that do not use a Singapore telephone number to send messages.

32 Duty to check the Do Not Call Register

32.1 Section 43 of the PDPA sets out the obligation of organisations to check with the Do Not Call Registry. In particular, under section 43(1) and (3), organisations shall not, with effect from the prescribed date, send a specified message addressed to a Singapore telephone number unless they had:

a) checked the relevant Do Not Call Register within the "prescribed duration"[29] before sending the message and received confirmation that the telephone number is not listed in the register;[30] or

b) obtained the clear and unambiguous consent of the user of subscriber of the telephone number (evidenced in written or other form accessible for future reference) to the sending of the message to that Singapore telephone number.

32.2 If consent obtained by an organisation for the purposes of the Do Not Call Provisions is withdrawn by the individual, the organisation will need to check with the Do Not Call Registry as noted above. The requirements of the PDPA relating to obtaining consent for the purposes of the Do Not Call provisions are discussed below.

32.3 Under section 45(2), contravention of section 43(1) is an offence and offenders are liable upon conviction to a fine not exceeding $10,000. The Commission also has the discretion, under S55(2), to compound any offences under Part IX prescribed as a compoundable offence by collecting from a person reasonably suspected of having committed the offence a sum of not exceeding $1,000.

---

[29] Refers to the period within which organisations must check the Do Not Call Registry, which will be prescribed in regulations to be issued under the PDPA.

[30] Section 43(4) clarifies that as there will be 3 Do Not Call Registers established by the Commission, the relevant Do Not Call Register shall depend on the particular type of specified message. For example, if a specified message will be sent through a voice call only, the organisation must check the Do Not Call Register relating to voice calls but need not check the other Do Not Call Registers relating to text messages and faxes.

32.4 As the Commission is currently in the process of developing the Do Not Call Registry, various matters relating to the operation of the Do Not Call Registry will be made known by the Commission in due course. The date from which organisations must comply with the obligation to check the Do Not Call Registry, referred to in the PDPA and above as the "prescribed date", will be specified in due course in regulations made under the PDPA.

32.5 The period within which organisations must check the Do Not Call Registry (the "prescribed duration" referred to in the PDPA and noted above) will similarly be prescribed in regulations. It is expected that this duration will initially be 60 days, which will be reduced to 30 days. That is, organisations may send specified message to Singapore telephone numbers not listed in the relevant Do Not Call Register for 60 (and later 30) days after they have received confirmation from the Commission that the Singapore telephone numbers are not listed on the Do Not Call Register, before they are required to check the register again. As noted earlier, there will initially be three Do Not Call Registers covering voice calls, text messages and fax messages.

33 Obtaining consent for sending messages to Singapore telephone numbers

33.1 As noted in the previous section, an organisation is not required to check with the Do Not Call Registry before sending a specified message to a Singapore telephone number if they have obtained a clear and unambiguous consent of the subscriber or user of the number for the sending of the message to that number.

Clear and unambiguous consent

33.2 The PDPA does not define the terms 'clear' and 'unambiguous' as the determination of whether consent was clear and unambiguous will depend on the specific facts in question. This may include, for example, whether the organisation notified the user or subscriber in a clear manner that specified messages would be sent to his or her Singapore telephone number or whether the individual gave a clear statement that he or she agreed to receive specified messages through their Singapore telephone number. There is presently no standard form for the manner or form of giving consent.

Example:
Sarah signs up for a spa membership over the Internet. She is directed to the terms and conditions page. There is a check box on the first page next to a line which says "click here if you wish to receive information about our products and services, including special offers we may have from time to time, by SMS". Sarah checks the box. Sarah has given clear and unambiguous consent to receive such messages by SMS.

Alice signs up for a different spa membership over the Internet. She is also directed to the terms and conditions page but it has a check box on the first page next to a line which says "click here if you agree to the use of your personal data for marketing purposes". Alice checks the box. Alice would not be considered to have given clear and unambiguous consent to receive specified messages through her Singapore telephone number.

Consent evidenced in written or other form

33.3 Section 43(3) requires consent obtained for the purposes of section 43 to be evidenced in written or other form so as to be accessible for subsequent reference. Written form may include physical documents or documents in electronic form.

33.4 If the consent required under section 43 is not evidenced in written form, it must be recorded in a form which is accessible for subsequent reference. This means that the consent must be captured in a form which can be retrieved and reproduced at a later time in order to confirm that such consent was obtained. Possible forms include an audio or video recording of the consent given.

Consent given before the prescribed day

33.5 As an individual may have consented to receive specified messages sent to his or her Singapore telephone number before the Do Not Call Provisions take effect, the PDPA recognises such consent for the purposes of the Do Not Call Provisions. In particular, section 47(4) provides that for the purposes of the Do Not Call Provisions, a subscriber or user of a Singapore telephone number is deemed to have given his or her consent to an organisation to send a specified message to that number if –

a) the subscriber or user had consented to the sending of the message before the Do Not Call Provisions come into operation; and

b) such consent had not been withdrawn on or after the date on which the Do Not Call Provisions come into operation.

Withdrawal of consent

33.6 As mentioned previously, any consent given by the subscriber or user of a Singapore telephone number for the purposes of the Do Not Call Provisions may be withdrawn by the user of subscriber. In particular, section 47(1) of the PDPA provides that a subscriber or user of a Singapore telephone number may withdraw any consent given to an organisation for the sending of any specified message to that number by giving notice to the organisation. Section 47(3) provides that an organisation that receives such a notice must cease (and cause its agents to cease) sending any specified messages to that number after the expiry of the "prescribed duration", which will be prescribed in Regulations.

33.7 As the user of a Singapore telephone number may not be the subscriber of that number, section 47(6) the PDPA allows a subscriber to withdraw any consent given for the sending of a specified message to that number.[31] This includes any consent given by other previous or current users of that number.

No withdrawal by subsequent registration with the Do Not Call Registry

33.8 A subscriber or user of a Singapore telephone number who has given consent (which meets the requirements specified in the PDPA) to an organisation may subsequently register his or her number with the Do Not Call Registry as she does not want to receive marketing messages from other organisations. In such a situation, the PDPA recognises that the consent given before registration with the Do Not Call Registry will continue to be effective for the purposes of the Do Not Call Provisions.

33.9 In particular, section 47(5) of the PDPA provides that where a subscriber or user of a Singapore telephone number consents to an organisation sending a specified message to that number on or after the commencement of the Do Not Call Provisions and subsequently adds that number to a Do Not Call Register, the addition of the number shall not be regarded as a withdrawal of consent for the purposes of the Do Not Call Provisions.

[31] "Subscriber", in relation to a Singapore telephone number, means the subscriber of the telecommunications service to which the Singapore telephone number is allocated. (S36(1)).

33.10 Reading section 47 (4) and (5) together, the addition of a Singapore telephone number on a Do Not Call Register does not amount to withdrawal of consent given before the commencement of the Do Not Call Provisions. Individuals wishing to withdraw consent to the sending of specified messages to their Singapore telephone number should withdraw consent by giving reasonable notice to the organisation under section 16 of the PDPA.

Other obligations relating to consent

33.11 The Do Not Call Provisions includes a few additional obligations which organisations are required to comply with in connection with obtaining consent. First, section 46 prohibits organisations from:

a) requiring, as a condition for supplying goods, services, land, interest or opportunity, a subscriber or user of a Singapore telephone number to give consent for the sending of a specified message to that number or any other Singapore telephone number beyond what is reasonable to provide the goods, services, land, interest or opportunity to that subscriber or user; and

b) obtaining or attempting to obtain consent for sending a specified message to a Singapore telephone number by providing false or misleading information with respect to the sending of the message or by using deceptive or misleading practices.

33.12 Section 46 provides that any consent given in such circumstances is not validly given.

33.13 Secondly, section 47(2) provides that an organisation shall not prohibit a subscriber or user of a Singapore telephone number from withdrawing consent to the sending of a specified message to that Singapore telephone number. However, this provision does not affect any legal consequences arising from such withdrawal.

33.14 As the requirements of sections 46 and 47(2) are similar to those provided in the Data Protection Provisions please refer to the section on the “Consent Obligation” in these Guidelines for more information.

34 Duty to identify the sender of a message

34.1 In addition to the duty to check the Do Not Call Registry under section 43 of the PDPA, organisations have a duty to identify the sender of a message. This comprises 2 separate obligations under sections 44 and 45 of the PDPA.

34.2 Section 44(1) prohibits an organisation from sending a specified message addressed to a Singapore telephone number on or after the date the Do Not Call Provisions take effect unless the message includes clear and accurate information on the following:

a) information identifying the organisation who sent or authorised the sending of the specified message (the "sender"); and

b) information about how the recipient can readily contact the sender.

34.3 The above information must be reasonably likely to be valid for at least 30 days after the message is sent. The message must also include such other information and comply with any conditions specified in regulations made under the PDPA.[32]

34.4 Section 45(1) of the PDPA prohibits an organisation who makes a voice call containing a specified message (or causes or authorises the making of such a call) addressed to a Singapore telephone number from a telephone number or facsimile number from concealing or withholding from the recipient the calling line identify of the sender.[33]

34.5 Contravention of section 44(1) or 45(1) is an offence under sections 44(2) and 45(2) respectively and, in either case, the offender is liable on conviction to a fine not exceeding $10,000. The Commission also has the discretion, under S55(2), to compound any offences under Part IX prescribed as a compoundable offence by collecting from a person reasonably suspected of having committed the offence a sum of not exceeding $1,000.

END OF DOCUMENT

[32] There are no such conditions or other information specified at present.

[33] The term "calling line identity" is defined in section 36(1) as the telephone number or information identifying the sender.