ADVISORY GUIDELINES ON KEY CONCEPTS IN THE PERSONAL DATA PROTECTION ACT

ISSUED BY THE PERSONAL DATA PROTECTION COMMISSION

24 SEPTEMBER 2013

PART I: INTRODUCTION AND OVERVIEW

1 Introduction

1.1 The Personal Data Protection Act 2012 (the "PDPA") establishes a 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 international 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 The Commission is still in the process of reviewing the matters to be prescribed in the Regulations. As such, advisory guidelines relating to these issues will be issued at a future date:

a) The Access and Correction Obligation

b) The Transfer Limitation Obligation, and

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

2.9 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.

[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 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.

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.

True and false personal data

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 Number or FIN (Foreign Identification Number)
- Passport number
- Photograph or video image of an individual
- Mobile telephone number
- Personal email address
- Thumbprint
- DNA profile
- Name and residential address

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 or method 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.

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. However, in most circumstances, the Commission is likely to consider personal data provided on business/name cards as business contact 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 for his business, 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 organisations should be mindful of.

Ownership of personal data

5.28 Personal data, as used in the PDPA, refers to the information comprised in the personal data and not the physical form or medium in which it is stored, such as a database or a book. The PDPA does not specifically confer any property or ownership rights on personal data per se to individuals or organisations and also does not affect existing property rights in items in which personal data may be captured or stored.

5.29 For example, an individual John Tan lives at Block 123 Ang Mo Kio Avenue 456. The fact that the individual's name is John Tan and that he lives at Block 123 Ang Mo Kio Avenue 456 is personal data of John Tan. However, John Tan does not own the information contained in the name "John Tan" or the information contained in the address "Block 123 Ang Mo Kio Avenue 456". If John Tan's name and address are written on a letter that is intended to be posted to him, the PDPA does not affect ownership rights to the letter which bears John Tan's name and address.

5.30 Similarly, if organisation A takes a photograph of John Tan, the identifiable image of John Tan would constitute his personal data. However, John Tan would not be conferred ownership rights to that photograph under the PDPA. Instead, ownership would depend on existing laws such as property law and copyright law. Regardless of ownership rights, organisation must comply with the PDPA if they intend to collect, use or disclose personal data about an individual.

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. Organisations should ensure that it is able to adduce evidence to establish and demonstrate that it complied with the obligations under the PDPA in the event of an investigation.

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 all the Data Protection Provisions with regard to both Tom and Jane's personal data, unless one or more exceptions apply.
>
> In this case, the travel agency can collect Jane's personal data without her consent as the exception 1(m) in the Second Schedule applies – that is, the travel agency does not need to seek Jane's consent because her personal data was provided by Tom to the travel agency to provide a service for Tom's personal and domestic purposes. However the travel agency must comply with all its other obligations under the Data Protection Provisions, for example, adopting reasonable security arrangements to comply with the Protection Obligation in respect of Tom's and Jane's personal data.

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. Examples of such activities could include opening joint bank accounts between two or more family members, or purchasing life insurance policies on one's child.

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*[2].

6.14 Public agencies are excluded from the application of the Data Protection Provisions. 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 employees' personal data or personal data of other customers.

Data intermediaries

6.15 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.

[2] The gazetted notification(s) of statutory bodies specified by the Minister to be public agencies for the purposes of the PDPA can be accessed through the Commission's website at www.pdpc.gov.sg.

Obligations of data intermediaries

6.16 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 Limitation Obligation") and not any of the other Data Protection Provisions.

6.17 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.

6.18 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."

6.19 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

6.20 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

6.21 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.

6.22 If Organisation A engages Organisation 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.

6.23 In the situation where two or more organisations ("Organisations A and B") engage an organisation ("Organisation C") for the processing of personal data on behalf of and for the purposes of Organisations A and B, then Organisation C may be considered to be both Organisations A and B's data intermediary in relation to such processing. Organisations A and B are both responsible for compliance with the Data Protection Provisions in relation to the personal data processed on their behalf.

6.24 Where Organisation B is a data intermediary of Organisation A, Organisation A is responsible for the personal data collected, used and disclosed by B regardless of whether such personal data was actually transmitted to A, for example, personal data of prospective clients of A that may only reside with B.

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.

Example:

Organisation XYZ provides courier services. Organisation ABC engages XYZ to deliver a parcel and signs a contract with XYZ for delivery of the parcel. ABC provides XYZ with the name and address of the person to whom the parcel is to be delivered. In this case, XYZ will be considered ABC's data intermediary under the PDPA as it is processing personal data on behalf of ABC. Insofar as XYZ is processing the intended recipient's personal data on behalf of and for the purposes of ABC pursuant to the written contract between XYZ and ABC, XYZ will only be subject to the provisions in the PDPA relating to the Protection Obligation and Retention Limitation Obligation in respect of such personal data.

6.25 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.

6.26 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

6.27 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 (ETA) 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. Under the ETA, such access includes the automatic and temporary storage of the third party material for the purpose of providing access.

"Agents" who may be data intermediaries

6.28 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"").

6.29 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.

6.30 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.

6.31 As good practice, organisations should ensure that their agents are made aware of and exercise proper data protection practices in relation to the handling of personal data.

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. The Commission notes that the standard of reasonableness is expected to be evolutionary. Organisations should expect to take some time and exercise reasonable effort to determine what is reasonable in their circumstances. As being reasonable is not a black and white issue, organisations and individuals may find that there will be different expectations about what is reasonable. In assessing what is reasonable, a possible step that an organisation could take is to view the situation from the perspective of the individual and consider what the individual would think as fair.

Part III THE DATA PROTECTION PROVISIONS

10 Overview of the Data Protection Provisions

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.[3] 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.[4]

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.

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

[3] See PDPA section 11(2).

[4] See PDPA section 4(3).

the control of the organisation. (This obligation will be considered in greater detail in advisory guidelines to be issued at a future date)

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 used by the organisation to make a decision that affects the individual concerned or 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 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. (This obligation will be considered in greater detail in advisory guidelines to be issued at a future date)

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.

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 required or authorised to do so under the PDPA or other written 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 good 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, minimally, document the consent in some way, for example,

by noting the fact that oral consent was provided by an individual for certain purposes, together with the date and time of such consent.

Obtaining consent verbally

11.7 In situations where the organisation cannot conveniently obtain consent from an individual in writing, it may choose to obtain verbal consent. However, organisations should note that in cases of dispute it may be more challenging to prove that verbal consent had been given if there is no other supporting evidence.

11.8 As good practice, organisations can consider adopting the following practices in cases when consent is obtained verbally:

a) Confirm the consent in writing with the individual (which may be in electronic form or other form of documentary evidence); or

b) Where appropriate in the circumstances, make a written note (which may be in electronic form or other form of documentary evidence) of the fact that an individual had provided verbal 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).

11.9 Organisations that wish to rely on the individual's consent to send specified messages to Singapore telephone numbers should note that the relevant defence in the Do Not Call Provisions require such consent to be clear and unambiguous consent to the sending of the specified message to that Singapore telephone number, evidenced in written or other accessible form. For this purpose, verbal consent would be insufficient unless it can be recorded in a form which is accessible for subsequent reference.

Failure to opt out

11.10 The Commission notes that there are various means of obtaining an individual's consent to the collection, use and disclosure of his personal data for a specified purpose. In some cases, organisations might adopt the opt out avenue to obtain consent, for example, by deeming that an individual has given his consent through inaction on his part. In general, the Commission notes that failure to opt out may be due to other reasons than the individual's desire to give consent. The Commission's view is that a failure to opt out will not be regarded as consent in all situations. Rather, whether or not a failure to opt out can be regarded as consent will depend on the actual circumstances and facts of the case. The opt out method of obtaining consent also has many variants, and depending on its implementation, could be more or less likely to constitute consent.

> Example:
>
> Retailer A has collected personal data from its customers for the purpose of delivering products purchased by the customers. It subsequently mails a flyer to the customers which states that a customer would have consented to the disclosure of his personal data to Company Z to market the products of Company Z unless the customer writes back to the retailer to opt out by a certain date. Company Z receives no response from the customer. In this case, the customer's inaction is unlikely to 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).
>
> Retailer B puts up a sign informing customers who are interested to join their membership programme to obtain an application form from a shelf next to the counter, fill it out, and drop the completed form into an unmanned box next to the shelf. A line in the form with an accompanying tick box states clearly "tick here if you do not wish your personal data to be provided to Company Z to market Company Z's products". The last field of the form requires the customer to provide his signature. The customer signed the form without putting a tick in the tick box and drops the completed form into the box. In this case, the customer is more likely to have given his consent to the disclosure of his personal data to Company Z for Company Z's marketing purposes.

11.11 The Commission would recommend that organisations obtain consent from an individual through a positive action of the individual to consent to the collection, use and disclosure of his personal data for the stated purposes. If

an organisation intends to adopt the opt out approach in seeking consent, the organisation should consider the risks that it may not have satisfied the Notification Obligation and Consent Obligation.

11.12 In relation to the Do Not Call Registry provisions where an organisation wishes to rely on the clear and unambiguous consent of an individual to the sending of the specified message to a Singapore telephone number to send a specified message to a Singapore telephone number registered on the Do Not Call Registry, the Commission will generally not view the mere failure to opt out as clear and unambiguous consent given by an individual. Organisations that wish to send telemarketing messages to individuals regardless of the registrations on the Do Not Call Registry should obtain a clear indication from the individual that he has opted to receive the telemarketing message, i.e. opt in consent.

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

11.13 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.

11.14 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 elaborate on when consent is not validly given and deemed consent would also apply.

When consent is not validly given

11.15 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.

11.16 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.

11.17 For the avoidance of doubt, organisations 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, so long as organisations do not make it a condition of providing the product or service.

> 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 to 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.

11.18 Section 14(2)(a) does not address other situations in which an organisation may seek to require consent as a condition where this is not tied to the provision of 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.

11.19 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.

11.20 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.

11.21 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 should give due consideration to whether the personal data requested is necessary or integral to providing the 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 subscribed services to the individual. 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.

11.22 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

11.23 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 need not ask for Sarah's consent to collect, use or disclose her credit card number and any other related personal data (e.g. name on credit card) required to process the payment transaction.
>
> Sarah would be deemed to have consented to the collection, use and disclosure of her credit card number and other related personal data for processing of the payment as she voluntarily provided the personal data and it is reasonable that Sarah would provide the personal data to pay for her facial. Sarah's deemed consent would extend to all other parties involved in the payment processing chain who collect or use Sarah's personal data. These parties could include, for example, Sarah's bank, the spa's bank and its processers and the payment system provider.

11.24 For 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.

11.25 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 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.

11.26 Section 15(1) also requires that it be reasonable for the individual to have voluntarily provided his 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.

11.27 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.

11.28 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.

11.29 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 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>

11.30 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).

11.31 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.

11.32 There could also be cases, especially with organisations that operate in a group structure, where one organisation in the group has validly obtained consent to the collection, use and disclosure of an individual's personal data for the purposes of other organisations in the corporate group. For example, when an individual subscribes to a service offered by one organisation in a corporate group, the organisation could have obtained the individual's consent to the collection, use and disclosure of his personal data for the purposes of marketing and promoting the products and services of that organisation and the other companies within the corporate group.

11.33 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". Exercising appropriate due diligence when obtaining personal data from third party sources.

11.34 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)). 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.

11.35 In exercising appropriate due diligence to verify that a third party source ("B") can validly give consent or has obtained consent from the individual concerned, organisations ("A") may adopt one or more of the following measures appropriate to the circumstances at hand:

a) Seek an undertaking from B through a term of contract between A and B that the disclosure to A for A's purposes is within the scope of the consent given by the individual to B;

b) Obtain confirmation in writing from B;

c) Obtain, and document in an appropriate form, verbal confirmation from B; or

d) Obtain a copy of the document(s) containing or evidencing the consent given by the individuals' concerned to B to disclose the personal data[5]

Example:

Sarah provides the personal data of her friend Jane to the sales consultant at her spa as part of a members referral programme the spa is running. Before recording Jane's personal data, the sales consultant asks Sarah a few questions to determine if Jane had been informed of the purposes for which her personal data is being disclosed to and used by the spa, and if Jane had provided her consent. After obtaining verbal confirmation from Sarah in the affirmative to those questions, the sales consultant proceeded to collect Jane's personal data. The sales consultant is likely to have exercised appropriate due diligence in this situation.

As a best practice, when contacting Jane for the first time, the sales consultant should inform Jane that her personal data was disclosed by Sarah and verify that Jane had provided consent to do so.

[5] The Commission notes that this may not always be possible or practical, e.g. in situations where such documents contain personal data which cannot be disclosed to A.

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

11.36 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. These circumstances include, for example, where:

a) the collection 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 collection is necessary for evaluative purposes.

11.37 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.

11.38 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)[6] 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.

[6] 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

11.39 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.

11.40 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));

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)); and

d) 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 (section 16(4)).

Organisations must allow and facilitate the withdrawal of consent

11.41 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.

11.42 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).

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

11.44 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. If the individual subsequently withdraws consent to his personal data in a manner which makes it impossible for the contract to be fulfilled, any legal consequences arising out such withdrawal would not be affected.

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 subscribed 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.

Actions organisations must take upon receiving a notice of withdrawal

11.45 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. Consequences for withdrawal of consent 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.

11.46 Organisations should note that they must highlight the consequences of withdrawal to individuals upon receipt of their notice to withdraw consent even if those consequences are set out somewhere else – e.g. in the service contract between the organisation and the individual.

11.47 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.

11.48 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.

11.49 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 to fulfil that purpose. Andy changes his mind and submits a notice to withdraw the consent he gave to Y Electronics for the purpose of marketing computers and other IT products.

Y Electronics is required to notify Andy of the consequences of his withdrawal, for example, that:

a) Y Electronics and its marketing agents will cease to send information on computer and IT products to Andy;

b) Y Electronics will cease to disclose Andy's personal data to any third party; and

c) Y Electronics will cease using Andy's contact details for marketing computer and IT products and will instruct its outsourced marketing agent likewise (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

11.50 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 other contractual obligations.

Publicly available data

11.51 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.

11.52 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.

11.53 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[7]. 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

[7] 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.

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.

11.54 The Commission recognises that personal data that is publicly available at one point in time may, for various reasons, no longer be publicly available after that time. For example, users of social networking sites may change their privacy settings from time to time, which would have an impact on whether their personal data would be considered publicly available.

11.55 The Commission recognises that it would be excessively burdensome for organisations intending to use or disclose publicly available personal data without consent to constantly verify that the data remains publicly available, especially in situations where the use or disclosure happens some time after the collection of the personal data. Hence, the Commission will take the position that so long as the personal data in question was publicly available at the point of collection, organisations will be able to use and disclose personal data without consent under the corresponding exceptions, notwithstanding that the personal data may no longer be publicly available at the point in time when it is used or disclosed.

11.56 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

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

11.57 Personal data is observed by reasonably expected means if individuals ought to reasonably expect their personal data to be collected in that particular manner at that location or event. It is important to note that this test is an

objective one, considering what individuals ought reasonably to expect instead of what a particular individual actually expects (which would vary from individual to individual).

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 enters Store ABC to make a purchase. It would be reasonably expected that his image would be captured by CCTVs installed by Store ABC for security reasons. However, as best practice, Store ABC should put up relevant notices to inform their customers about the CCTVs in operation.

Jeff subsequently enters Store XYZ, who has engaged a photographer for the day. Generally speaking, photo-taking is reasonably expected in a location like a store that is open to the public. Therefore, it would be reasonably expected for Jeff's personal data to be captured by Store XYZ's photographer (or by other photo-taking equipment, e.g. smart phones of fellow patrons). However, as good practice, Store XYZ should put up relevant notices to inform their customers about the photographer.

Jeff leaves the shopping mall and enters a public park where filming for a TV show is taking place. His image was captured by the film crew in the course of filming the show. In this case, it would be reasonably expected that his image could be captured by the film crew. However, as best practice the film crew should put up notices at appropriate locations (e.g., at the entrances to the park) to inform park users that filming is taking place.

11.58 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. Generally speaking, the more restrictions there are for access to a particular location, the less likely it would be considered "open to the public". Relevant considerations would be factors that affect the ease and ability with which the public can gain access to the place. Examples include the presence or absence of physical barriers, such as fences, walls and gates, around the place; the conditions and effectiveness of these barriers; and the employment of security systems, sentries and patrols aimed at restricting entry.

11.59 However, the mere existence of some restrictions is not sufficient to 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 relevant factors such as whether the event was open to a large number of members.

11.60 The Commission recognises that there can be private spaces within public spaces. 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. In addition, 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. Another example would be the interior of a taxi for the duration when it is hired by a passenger. During the period(s) of hire, the interior of the taxi would not be considered a location that is open to the public, even though the taxi itself may be in a public space. The "publicly available data" exception may not apply to such private spaces within public spaces and an organisation must typically provide appropriate notification and obtain consent before collecting, using or disclosing personal data (e.g., in-vehicle video cameras which collect personal data of the passengers in a taxi.)[8]

11.61 For the avoidance of doubt, the PDPA provides exceptions for news organisations to collect, use and disclose personal data without consent solely for its news activity, regardless whether the personal data is publicly available. Please refer to the PDPA for full definitions of "news organisation" and "news activity".

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

[8] The Commission recognises that organisations may have to collect, use or disclose personal data in private spaces within public spaces for reasonable purposes – e.g. to monitor in-vehicle activities for the safety of the taxi driver and the passenger.

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 Obligation 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 of its purposes; and

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

When an organisation must inform the individual of its purposes

13.7 Under section 20 (1) and (4) of the PDPA, 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.

13.8 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 and form in which an organisation should inform the individual of its purposes

13.9 The PDPA does not specify a specific 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 best way of doing so such that the individual is provided with the required information to understand the purposes for which his personal data is collected, used or disclosed.

13.10 Relevant factors affecting an organisation's determination of the appropriate manner and form to notify an individual of its purposes 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;

c) the frequency at which the personal data will be collected; and

d) the medium through which the notification is provided (e.g. face-to-face or through a telephone conversation).

13.11 It is generally good practice for an organisation to state its purposes in a written form (which may be electronic form or other form of documentary evidence) so that the individual is clear about its purposes and both parties will be able to refer to a clearly documented statement of the organisation's purposes in the event of any dispute. For example, organisations may state their purposes in the service agreement between the organisation and the individual or 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.

Providing Notification through a Data Protection Policy

13.12 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.[9] An organisation may choose to notify individuals of the purposes for which it collects, uses and discloses personal data through its Data Protection Policy.

13.13 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.

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

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.

13.14 For the avoidance of doubt, organisations are not required to make available to individuals information related to the organisation's internal corporate governance matters (e.g. expense policies or corporate rules) unrelated to the organisation's data protection policies and practices as part of their Data Protection Policy, so long as the Openness Obligation is met. Please refer to the section on "the Openness Obligation" for more information on the requirement for organisations to develop and implement policies and practices that are necessary for the organisation to meet its obligations under the PDPA and to make information about those data protection policies and practices available

Example:

Sarah signs up for a membership at a gym. The application form contains an extract of the most relevant portions of the Data Protection Policy in a physical document. For example, it states that Sarah's address details will be used for sending her a gym membership card and other communications related to her gym membership. The sales representative of the gym informs her that the full Data Protection Policy is available on the gym's website and provides her with relevant information to locate it. In this case, the gym has informed Sarah of the purposes for which her personal data will be collected, used or disclosed.

<u>Information to be included when stating purposes</u>

13.15 An organisation should state its purposes at an appropriate level of detail 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 section on "Purposes", an organisation need not specify every activity it will undertake in relation to collecting, using or disclosing personal data when notifying individuals of its purposes. This includes activities that are directly related to the collection, use or disclosure of personal data or activities that are integral to the proper functioning of the overall business operations related to the purpose. For example, if an organisation wishes to obtain consent to

collect or use personal data for the purpose of providing a service to an individual, the organisation does not need to seek consent for: (a) every activity it will undertake to provide that service; and (b) internal corporate governance processes such as allowing auditors to access personal data as part of an audit.

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

d) 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

e) 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 the electronics store's corporate group and outsourced marketing company for the purposes of marketing the products of the various companies in its corporate group 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 would not be considered to have stated a sufficiently specific purpose.

Best practice considerations relating to the Notification Obligation

13.17 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. Hence organisations should endeavour to ensure that their notifications are clear, easily comprehensible, provide appropriate information and are easily accessible.

13.18 In considering how to notify individuals of their purposes, organisations should consider:

a) Drafting notices that are easy to understand and appropriate to the intended audience, providing headings or clear indication of where the individuals should look to determine the purposes for which their personal data would be collected, used or disclosed and avoiding legalistic language or terminology that would confuse or mislead individuals reading it;

b) Using a 'layered notice' where appropriate, by providing the most important (e.g. summary of purposes) or basic information (e.g. contact details of the organisation's Data Protection Officer) more prominently (e.g. on the first page of an agreement) and more detailed information elsewhere (e.g. on the organisation's website). A layered approach is useful when individuals do not want to read all the information at the point of transaction, or when the medium of transaction is not suitable for conveying detailed information (e.g. telephone conversation);

c) Considering if some purposes may be of special concern or be unexpected to the individual given the context of the transaction, and whether those purposes should be highlighted in an appropriate manner;

d) Selecting the most appropriate medium(s) to provide the notification (e.g. in writing through a form, on a website, or orally in person); and

e) Developing processes to regularly review the effectiveness of and relevance of the notification policies and practices.

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 through a survey form which it hands to shoppers. The first line of each survey forms clearly and legibly states that "Your personal data will be used by the supermarket or its appointed survey company for analysis of survey responses to find out ways to improve customer experience at our supermarket, or to contact survey respondents for follow-up queries on the survey responses for such analysis." The supermarket would 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. Individuals who visit the show flat are asked to provide their name, address and income information in the guest book. The receptionist greets every individual who enters the show flat and explains verbally that his personal data is collected for the agency's market research and product planning purposes and that it would not be used to contact individuals after they leave the show flat. The real estate agency would be considered to have provided appropriate notification in this case.

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

13.19 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.

13.20 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").

13.21 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 currently has a membership with a spa. Her spa wants to use her personal data for the purposes of sending her greeting cards and the spa's annual newsletter in the post while her spa membership is still active. 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 spa wants to send her information about an affiliate company's hair salon promotions. The spa would need to obtain Sarah's consent before sending information promoting new services that Sarah has not signed up for, as that is unlikely to fall within sub-paragraphs (a) to (c) above.

14 The Accuracy Obligation

14.1 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.

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

14.3 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.

<u>Requirement of reasonable effort</u>

14.4 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).

14.5 For the avoidance of doubt, an organisation may not be required to check the accuracy and completeness of an individual's personal data each and every time it makes a decision about the individual. An organisation may also not be required to review all the personal data currently in its possession to ensure that they are accurate and complete each and every time it is likely to make a decision about the individual. Organisations should perform their own risk assessment and use reasonable effort to ensure the accuracy and completeness of such personal data that is likely to be used to make a decision that will affect the individual.

Ensuring accuracy when personal data is provided directly by the individual

14.6 Organisations may presume that personal data provided directly by the individual concerned is accurate in most circumstances. When in doubt, organisations can consider requiring the individual to make a verbal or written declaration that the personal data provided is accurate and complete. 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, by requesting a more updated copy of the personal data before making a decision that will significantly impact the individual).

Example:

Nick applies for a credit card 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.

Two years later, Nick applies for a home loan from a bank. The bank has not made any checks during the two years that Nick's personal data is accurate and complete. When the bank received the home loan application, the bank showed Nick their records of his personal data and asked Nick to make a fresh declaration that the record is accurate and complete. In addition, noting that the supporting documents previously obtained for the credit card application are now dated two years back, the bank asked Nick to provide a copy of his most recent payslip and proof of employment. In this scenario, the bank has made a reasonable effort to ensure that the personal data collected from Nick is accurate and complete.

Ensuring accuracy when collecting personal data from a third party source

14.7 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. It may also conduct further independent verification if it deems prudent to do so.

Example:

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 dated eight years

ago, when Nick first joined the company.

In this scenario, the adventure camp company should consider asking Nick for a more recent health record.

14.8 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 new 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 about the qualifications 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.

15 The Protection Obligation

15.1 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.

15.2 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.

15.3 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.

15.4 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.

Examples of security arrangements

15.5 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; and • 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.
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.

16 The Retention Limitation Obligation

16.1 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.

How long personal data can be retained

16.2 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.

16.3 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.

16.4 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 must not be kept by an organisation “just in case” it may be needed for other purposes that have not been notified to the individual concerned.

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.

16.5 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 large quantity of different types of personal data may have to implement varying retention periods for each type of personal data as appropriate.

16.6 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.

16.7 Organisations should start developing or adjusting relevant processes to ensure that personal data is recorded and stored in a manner which facilitates the organisation's compliance with the Retention Limitation Obligation. In this regard, the Commission recognises that organisations may have retention policies which are applied to groups or batches of personal data.

16.8 As a best practice, organisations should prepare an appropriate personal data retention policy which sets out their approach to retention periods for personal data. In particular, where personal data is retained 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 personal data

16.9 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).

16.10 An organisation ceases to retain documents containing personal data when it, its agents and its data intermediaries no longer has access to those documents and the personal data they contain. Examples could include:

a) Returning the documents to the individual concerned;

b) Transferring the document to another person on the instructions of the individual concerned;

c) Destroying the documents – e.g. by shredding them or disposing of them in an appropriate manner; or

d) Anonymising the personal data.

16.11 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. Like physical documents, personal data in electronic form which are archived or to which access is limited will still be considered to be retained for the purposes of the Retention Limitation Obligation.

16.12 As far as possible, an organisation should cease to retain documents containing personal data in a manner which renders those documents completely irretrievable or inaccessible to the organisation. However, the Commission recognises that there are certain circumstances where the personal data still remain within reach of the organisation or within the organisation's systems in some form. Examples would include shredded documents lying in the bin, or deleted personal data in an un-emptied recycling bin on an organisation's computer. In circumstances where there is doubt about whether an organisation has ceased to retain personal data, the Commission will have regard to the factors articulated in the paragraph below.

<u>Factors relevant to whether an organisation has ceased to retain personal data</u>

16.13 In considering whether an organisation has ceased to retain personal data the Commission will consider the following factors in relation to the personal data in question:

a) Whether the organisation has any intention to use or access the personal data;

b) How much effort and resources the organisation would need to expend in order to use or access the personal data again;

c) Whether any third parties have been given access to that personal data; and

d) Whether the organisation has made a reasonable attempt to destroy, dispose of or delete the personal data in a permanent and complete manner.

Anonymising personal data

16.14 An organisation will be considered to have ceased to retain personal data when it no longer has the means to associate the personal data with particular individuals – i.e. the personal data has been 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.

17 The Openness Obligation

17.1 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. Designating an individual responsible for an organisation's compliance with the PDPA

17.2 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. For the avoidance of doubt, the individual(s) designated by an organisation need not be an employee of the organisation.

17.3 For the purpose of responding to access and correction requests in writing, at least one of the business contact information of this designated individual should be a mailing address (for example the office address) or an electronic mailing (email) address.

17.4 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.

17.5 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 section 20(1)(c) and (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.

17.6 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 is especially important if the relevant person is not physically based in Singapore. This would facilitate the organisation's ability to respond promptly to any complaint or query on its data protection policies and practices.

Accountability

17.7 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;[10]

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.[11]

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

[11] 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).

PART IV: OTHER RIGHTS, OBLIGATIONS AND USES

18 Overview

18.1 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.

18.2 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.

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

19 Existing rights, etc under law

19.1 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.[12]

19.2 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.

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

20 Other written law

20.1 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.[13]

20.2 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.

[13] 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".

21 Use of personal data collected before the appointed day

21.1 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.

21.2 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.

21.3 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.

21.4 For the avoidance of doubt, the purpose of telemarketing (i.e. sending a specified message to a Singapore telephone number) could be a reasonable existing use. Organisations must, however, ensure that they also comply with the Do Not Call Provisions in Part IX of the PDPA (which apply concurrently with the Data Protection Provisions). Before sending a specified message to a Singapore telephone number, the organisation must check with the Do Not Call registry to confirm that the number is not listed on a Do Not Call Register, unless it has obtained "clear and unambiguous consent" in evidential form from the individual to the sending of the message. Please see the section below on the "Do Not Call Provisions" for more information.

21.5 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 specific activity falls within the scope of the original purposes for which personal data was collected, an organisation may consider the following:

a) how the activity 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 activity falls within the scope of the original purposes.

21.6 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.

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.

PART V: THE DO NOT CALL PROVISIONS

22 Overview

22.1 In addition to the Data Protection Provisions, the PDPA also contains the Do Not Call Provisions. The Do Not Call Provisions are found in Part IX of the PDPA and apply to persons including individuals as well as companies, associations and other bodies of persons, corporate or unincorporated.[14] The Do Not Call Provisions contain a number of obligations that apply in relation to persons sending specified messages to Singapore telephone numbers.[15] In particular, such persons are required to perform the following obligations (the specific sections of the PDPA under which these obligations arise are cited below for reference):

a) Duty to check the Do Not Call Register – before a person sends a specified message to a Singapore telephone number, the person 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 the person has obtained clear and unambiguous consent in evidential form from the user or subscriber of the number[16] (section 43 of the PDPA); and

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

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

---

[14] As drafted, the Do Not Call Provisions impose obligations on a "person" sending specified messages. However, as may be seen from the definitions of "person" in section 2(1) of the Interpretation Act, the term includes natural persons as well as companies, associations and other bodies of persons, corporate or unincorporated. For the avoidance of doubt, the term "person" as used in this section of the Guidelines shall be construed as including individuals as well as companies, associations and other bodies of person, corporate or unincorporate.

[15] 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).

[16] 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. for voice calls, not conceal or withhold from the recipient the sender's calling line identity[17] (section 45 of the PDPA).

22.2 There will initially be three Do Not Call Registers covering voice calls, text messages and fax messages.

22.3 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 questions, as well as the scope of the above obligations, are addressed in the following sections.

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

23 Locations of sender and recipient

23.1 It should be noted that the locations of the sender and recipient when a specified message is sent and accessed affect 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.

23.2 Under section 38, the Do Not Call Provisions do not apply if both the sender and the recipient are not in Singapore when the specified message is sent and accessed respectively. This may be the situation, for example, when the recipient is travelling in another country and accesses a specified message sent by a sender in that country. However, the Do Not Call Provisions would apply if the recipient is travelling in another country and the sender is in Singapore. The Do Not Call Provisions also apply 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.

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.

24 Meaning of "specified message"

24.1 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;[18]
ii. and or an interest in land; or
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.[19]

24.2 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).

24.3 Messages sent for a purpose which is not specified in section 37(1) 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.

---

[18] 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; (c) 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 (d) financial services (as defined in section 2 of the Consumer Protection (Fair Trading) Act (Cap. 52A).

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

> Example:
>
> Organisation ABC calls Charles for the sole purpose of finding out if he is interested to apply for a vacancy in the organisation. The call from Organisation ABC would not be considered a specified message.

24.4 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 aspects 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.

24.5 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.

24.6 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 a person cannot cite as a defence the fact that, for example, the goods it had offered in a specified message were actually not available for purchase.

25 Exclusions from the meaning of "specified message"

25.1 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 messages 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. A specified message shall not include any of 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;[20]

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 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; or

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;

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

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

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,

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

iv. 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

f) any message the sole purpose of which is to conduct market research or market survey; or

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

25.2 A person sending a message that falls within one of the excluded purposes specified in Eighth Schedule (or which is not listed in section 37(1)) must not use that message for any of the purposes listed in section 37(1) of the PDPA and which is not excluded under the Eighth Schedule. Otherwise, the message will still be a specified message and the sender 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.

26 Business to Business ("B2B") marketing messages

26.1 As noted above, one of the excluded messages specified in the Eighth Schedule relates to messages sent to an 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 first mentioned 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.

27 Meaning of "sender"

27.1 As noted above, the Do Not Call Provisions contain obligations in relation to the sending of a specified message. Hence a person who sends a message, referred to in the PDPA as the "sender", is responsible for complying 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.

27.2 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 causes the message to be sent or the voice call to be made; and

c) the person who authorises the sending of the message or the making of the call.

27.3 Hence it is important to note that in addition to the person who actually sent the message or made the 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 a sender.

27.4 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.

27.5 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 depends 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.

28 Exclusions

28.1 The PDPA excludes certain persons from the scope of the Do Not Call Provisions 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 persons 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.[21]

28.2 As the Do Not Call Provisions impose obligations on individuals as well as corporate entities such as companies, the PDPA provides that there are certain situations in which it would not be appropriate to apply 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.

28.3 Under section 48, an employee who acts 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 acted 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. This defence is not available to an "officer" of an organisation that may have committed an offence under the Do Not Call Provisions.[22]

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

[22] The term "officer" is defined in section 52(5) of the PDPA.

29 Sending a specified message to a Singapore telephone number

29.1 As the sending of a specified message to a Singapore telephone number is relevant in determining the application of the Do Not Call Provisions, it is important to understand 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.[23]

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

29.3 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'.

29.4 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. For the avoidance of doubt, the Data Protection Provisions may still apply to such specified messages which are not sent to a Singapore telephone number.

[23] 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.

30 Duty to check the Do Not Call Register

30.1 The obligation of persons to check with the Do Not Call Registry is set out in section 43 of the PDPA. In particular, under section 43(1) and (3), persons 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" before sending the message and received confirmation that the telephone number is not listed in the register;[24] 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.

30.2 The "prescribed duration" within which a person must check with the Do Not Call Registry before sending a specified message to a Singapore telephone number will be prescribed in the Regulations. This duration will be:

a) 60 days, for messages sent before 1 August 2014, and

b) 30 days, for messages sent on or after 1 August 2014.

30.3 The validity period of the results returned from the Do Not Call Registry reflects the requirement for persons to check with the Do Not Call Registry within the "prescribed duration", and provides for a gradual transition to address the switch in "prescribed duration" from 60 days to 30 days.

[24] Section 43(4) clarifies that as there may be more than one Do Not Call Register 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.

Validity period of results returned from the Do Not Call Registry		
Receipt of Results	**Validity Period**	**Remarks**
Between 2 January 2014 to 31 May 2014 (both dates inclusive)	**60 days** from receipt of results	E.g., If an organisation submits telephone numbers for checking against the Do Not Call Registry and receives the results on 4 March 2014, the results will be valid until 3 May 2014.
Between 1 June 2014 to 1 July 2014 (both dates inclusive)	Until **31 July 2014**	As this is the transition period between the 60/30 days validity period, all results received during this period will be valid until 31 July 2014.
From 2 July 2014 onwards	**30 days** from receipt of results	E.g., If an organisation submits telephone numbers for checking against the Do Not Call Registry and receives the results on 4 July 2014, the results will be valid until 4 August 2014.

30.4 If consent obtained by a person for the purposes of the Do Not Call Provisions is withdrawn, the person 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. The "prescribed period" (as set out in section 47(3)) within which persons must effect a withdrawal of consent is:

i. 60 days, for a notice of withdrawal given by a consumer from 2 January 2014 to 1 July 2014 (inclusive); and

ii. 30 days, for a notice of withdrawal given on or after 2 July 2014.

30.5 Under section 43(2), contravention of section 45(1) is an offence and offenders are liable upon conviction to a fine not exceeding $10,000. The Commission also has the discretion, under section 55(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.

31 Obtaining consent for sending messages to Singapore telephone numbers

31.1 As noted in the previous section, a person is not required to check with the Do Not Call Registry before sending a specified message to a Singapore telephone number if the person has obtained a clear and unambiguous consent evidenced in written or other form from the subscriber or user of the number for the sending of the message to that number.

Clear and unambiguous consent

31.2 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.

31.3 Facts that would determine if consent was clear and unambiguous would include:

a) Whether the person had notified the user or subscriber clearly and specifically that specified messages would be sent to his or her Singapore telephone number; and

b) Whether the user or subscriber gave consent to receive specified messages through some form of positive action. Clear and unambiguous consent is unlikely to be construed to have been obtained from a mere failure to opt out through inaction on the part of the user or subscriber. Please refer to section above on "Failure to opt out" for more information.

Example:

Example Clause A: "you consent to receive information about special offers we may have from time to time, by SMS".

Example Clause B: "you consent to the use of your personal data for marketing purposes".

Clause A clearly and specifically notifies the user or subscriber that specified messages would be sent to his or her Singapore telephone number. Clause B is not sufficiently specific as "marketing purposes" may or may not include the sending of specified messages.

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 Example Clause A above ("you consent to receive information about special offers we may have from time to time, by SMS"). Sarah checks the box.

Sarah would be considered to have given clear and unambiguous consent.

Example:

Retailer A has collected personal data from its customers for the purpose of delivering products purchased by the customers. The retailer subsequently sends an email to all its customers informing them that unless they reply to the email to indicate otherwise, they would be considered to have agreed to Example Clause A above ("you consent to receive information about special offers we may have from time to time, by SMS").

Retailer A's customer, Jane, did not reply to the email. Jane would <u>not</u> be considered to have given clear and unambiguous consent.

Example

Sarah fills up an online form. The following clause is directly above the "Submit" button.

I would like to receive information about promotions and offers by:

a. Phone [ ]

b. SMS [ ]

c. Email [ ]

d. Mail [ ]

Sarah checks the boxes SMS and Email and submits the online form. Sarah would be considered to have given clear and unambiguous consent.

Example:

Sarah fills out a form with a clause with a check box next to it that says "please send me special offers about Org ABC's products by SMS".

This clause is clearly printed directly above where Sarah has to sign the application form.

Sarah ticks the check-box and signs the form. Sarah would be considered to have given clear and unambiguous consent.

Example:

Jane fills out a form. At the end of the form, right before the signature line, this clause is printed: "We would like to send you information about new products and sales promotions. We would call you or send SMSes to your Singapore telephone number." Following this clause there are 3 options with accompanying check boxes for individuals to tick, as follows:

a. I do not agree to receive such information.
b. I agree to receive such information. (regardless of any current or future registration on any DNC Register)

Jane places a tick in the check box next to option b. Jane would be considered to have given clear and unambiguous consent.

Consent evidenced in written or other form

31.4 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, documents or other form of records in electronic form. A person should note that the requirement to obtain consent in evidential form applies to both online and offline situations.

31.5 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 manner or 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

31.6 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 a person 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.

31.7 The Commission is of the view that persons obtaining consent from individuals before the prescribed day to receive specified messages should also fulfil the section 43(3) requirements – i.e. that the consent be clear and unambiguous and evidenced in written or other form. A person must check with the Do Not Call Registry before sending a specified message to a Singapore telephone number if the consent obtained does not fulfil the section 43(3) requirements.

Withdrawal of consent

31.8 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 or 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 a person for the sending of any specified message to that number by giving notice to the person. Section 47(3) provides that a person 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.

31.9 As the user of a Singapore telephone number may not be the subscriber of that number, section 47(6) of the PDPA allows a subscriber to withdraw any consent given for the sending of a specified message to that number.[25] This includes any consent given by other previous or current users of that number.

[25] "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)).

No withdrawal by subsequent registration with the Do Not Call Registry

31.10 A subscriber or user of a Singapore telephone number who has given consent (which meets the requirements specified in the PDPA) to a person may subsequently register his or her number with the Do Not Call Registry as he/she does not want to receive marketing messages from other persons. 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.

31.11 In particular, section 47(5) of the PDPA provides that where a subscriber or user of a Singapore telephone number consents to a person 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.

31.12 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

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

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

31.15 Secondly, section 47(2) provides that a person 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.

31.16 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.

32 Duty to identify the sender of a message

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

32.2 Section 44(1) prohibits a person 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 person who sent or authorised the sending of the specified message (the "sender")[26]; and

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

32.3 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.[27]

32.4 Section 45(1) of the PDPA prohibits a person 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.[28]

32.5 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

---

[26] An organisation may choose to use an abbreviated version of its name or other appropriate abbreviations as part of information identifying the organisation so long as the organisation can be clearly identified from that information. E.g. American Express International Inc may choose to use the abbreviated form of its name, "Amex" to identify itself.

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

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