ADVISORY GUIDELINES ON KEY CONCEPTS IN THE PERSONAL DATA PROTECTION ACT

Issued 23 September 2013
Revised 2 June 2020

TABLE OF CONTENTS

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 Guidelines should be read in conjunction with the document titled "Introduction to the Guidelines" and are subject to the disclaimers set out therein.

1.3 It should be noted that the examples in these Guidelines serve to illustrate particular aspects of the PDPA, and are not meant to exhaustively address every obligation in the PDPA that would apply in that scenario.

2 Overview of the PDPA

2.1 The PDPA governs the collection, use and disclosure of individuals' personal data by organisations in a manner that recognises both the right of individuals to protect their personal data and the need of organisations to collect, use and disclose personal data for purposes that a reasonable person would consider appropriate in the circumstances. The PDPA contains two (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 three (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 faxes.

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. In addition, certain organisations that are in an ongoing relationship with individuals may be exempted from the obligation to check the Do Not Call Registry before sending certain messages related to the subject of the ongoing relationship. Please refer to the Advisory Guidelines on the Do Not Call Provisions for more information.

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

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

PART II: IMPORTANT TERMS USED IN THE PDPA

3 Definitions and related matters

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

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

"The purpose of this Act is to govern the collection, use and disclosure of personal data by organisations in a manner that recognises both the right of individuals to protect their personal data and the need of organisations to collect, use or disclose personal data for purposes that a reasonable person would consider appropriate in the circumstances." (emphasis added)

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

a) "individuals"

b) "personal data"

c) "organisations"

d) "collection, use and disclosure"

e) "purposes"

f) "reasonable"

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

4 Individuals

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

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

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

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

[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 may cover different types of data about an individual and from which an individual can be identified, regardless of such data being true or false or whether the data exists in electronic or other form.

5.3 The PDPA does not apply in relation to certain categories of personal data which are expressly excluded from the application of the PDPA. These are highlighted in the sections later. Please also refer to the chapter on "Anonymisation" in the Advisory Guidelines on the PDPA for Selected Topics, which describes the considerations and conditions under which personal data may be anonymised and no longer considered personal data for the purposes of the PDPA.

Data about an individual

5.4 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. Some examples of data that is about an individual include information about an individual's health, educational and employment background, as well as an individual's activities such as spending patterns.

5.5 Not all data that relates to an individual may identify the individual. For example, a residential address, on its own, relates to a particular place and there could be several individuals 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 The content of individuals' communications, such as email messages and text messages, in and of themselves may not be considered personal data, unless they

contain information about an individual that can identify the individual[2].

Individual who can be identified

5.7 Data constitutes personal data if it is data about an individual who can be identified from that data on its own, or from that data and other information to which the organisation has or is likely to have access.

Individual can be identified from that data on its own

5.8 Certain types of data can, on its own, identify an individual, for instance biometric identifiers which are inherently distinctive to an individual, such as the face geometry or fingerprint of an individual.

5.9 Similarly, data that has been assigned to an individual for the purposes of identifying the individual (e.g. NRIC or passport number of an individual) would be able to identify the individual from that data alone.

5.10 Such data which, on its own, constitutes personal data, is referred to as "unique identifier" in these guidelines. Data that the Commission generally considers unique identifiers include:

- Full name[3]
- NRIC Number or FIN (Foreign Identification Number)
- Passport number
- Personal mobile telephone number
- Facial image of an individual (e.g. in a photograph or video recording)
- Voice of an individual (e.g. in a voice recording)[4]
- Fingerprint
- Iris image
- DNA profile

---

[2] Please refer to the following:
a) *Re Executive Coach International Pte. Ltd.* [2017] SGPDPC 3, in relation to personal history of an individual disclosed to participants in a WhatsApp Group;
b) *Re Interflour Group Pte Ltd* [2017] PDP Digest, in relation to emails downloaded from a Hotmail account; and
c) *Re Black Peony* [2017] PDP Digest, in relation to screenshots of WhatsApp messages disclosed on the Internet.

[3] *Re Full House Communications Pte Ltd* [2016] SGPDPC 8, where it was found that a person's full name in the drop down box alone would enable identification of the individual.

[4] An individual may be identified from his voice, for example, where a voice clip is sufficiently clear and of a sufficient duration.

5.11 The above is not an exhaustive list of unique identifiers.

> Example: Data that is personal data on its own
>
> John picks up a passport photograph which clearly shows the facial image of an identifiable individual. The photograph is considered to constitute personal data of the individual, even though John does not know who the individual is.

Individual can be identified from that data and other information to which the organisation has or is likely to have access

5.12 Generic information, such as gender, nationality, age or blood group, alone is not usually able to identify a particular individual (e.g. gender alone cannot identify the individual). Nevertheless, such information may constitute part of the individual's personal data if it is combined with a unique identifier[5] or other information such that it can be associated with, or made to relate to, an identifiable individual.

5.13 Whether any data or dataset constitutes personal data would depend on the specific facts of each case. Data or datasets that may identify an individual in a certain situation may not identify an individual in another situation. An organisation should consider the availability of other information it has or is likely to have access to, among other considerations.

> Example: Dataset that is a combination of a unique identifier and other information
>
> Organisation ABC conducts a street intercept survey to collect information from passers-by on the average amount spent on household items per month, their full name, gender, and age range.
>
> The combination of data collected generally constitutes personal data of the individuals as it includes their full names.
>
> If Organisation ABC only collects information on the average amount spent on household items, gender, and age range, the dataset may not constitute personal data as it is unlikely to identify the individuals.

[5] The Commission notes that so long as any combination of data contains a unique identifier of an individual, that combination of data will constitute personal data of the individual.

Example: Dataset comprising data points which, individually, cannot identify a particular person

Organisation DEF conducts a street intercept survey and collects the following information from passers-by:

- Age range
- Gender
- Occupation
- Place of work

Although each of these data points, on its own, would not be able to identify an individual, Organisation DEF should be mindful that the dataset, comprising a respondent's age range, gender, occupation and place of work may be able to identify the respondent.

Respondent A is a female individual who is between 20 and 30 years of age, and works as a retail salesperson at Orchard Road. This dataset may not be able to identify Respondent A since there could be many female salespersons in their 20s working in retail outlets at Orchard Road.

Respondent B is a male individual who is between 20 and 30 years of age, and works as a security officer at Bencoolen Street. This dataset may be able to identify respondent B if there are no other male security officers in their 20s working at Bencoolen Street.

Given that some of the respondents' datasets are likely to identify the respondents, Organisation DEF should treat the datasets as personal data and ensure they comply with the Data Protection Provisions.

True and false personal data

5.14 It should be noted that the PDPA's definition of personal data does not depend on whether the data is true or false. If organisations collect personal data which is false, or if the data collected has changed such that it is no longer true, such data will still be personal data, and organisations are required to comply with the Data Protection Provisions under the PDPA.

5.15 As explained in greater detail 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 (the "Accuracy Obligation").

Personal data relating to more than one individual

5.16 Information about one individual may contain information about another individual.

In that circumstance, the same information could be personal data of both individuals.

5.17 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

5.18 The PDPA does not apply to, or applies to a limited extent to, certain categories of personal data.

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

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

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

5.20 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

5.21 The Data Protection Provisions do 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".

5.22 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 the card 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.

5.23 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.

5.24 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 salesperson, Tom, to assist him in searching for a suitable property unit as a second branch. Damien passes his contact details to Tom so that Tom can update him from time to time on property units which he might like. Tom shares Damien's contact details with his colleagues, so that more salespersons 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 Tom 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

5.25 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.

5.26 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).

5.27 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.

5.28 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.

5.29 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

5.30 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.

5.31 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.

5.32 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, organisations 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. An organisation 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*[6].

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.

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

[6] 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.

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.

<u>Considerations for organisations using data intermediaries</u>

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.

6.21 When engaging a data intermediary, an organisation should make clear in its contract the scope of work that the data intermediary is to perform on its behalf and for its purposes. For instance, if the organisation requires the data intermediary to process personal data on its behalf to respond to access or correction requests by individuals, the organisation should include contractual clauses to ensure that the data intermediary's scope of work and level of responsibilities are clear. The data

intermediary has independent obligations to protect and cease retention of personal data that it has received for processing under the contract. The organisation remains liable for any breach of the Data Protection Provisions for any processing by a data intermediary on its behalf and for its purposes.

Overseas transfers of personal data

6.22 Where an organisation engages a data intermediary to process personal data on its behalf and for its purposes, the organisation is responsible for complying with the Transfer Limitation Obligation in respect of any overseas transfer of personal data. This is regardless of whether the personal data is transferred by the organisation to an overseas data intermediary, or transferred overseas by the data intermediary in Singapore as part of its processing on behalf and for the purposes of the organisation.

6.23 The Transfer Limitation Obligation requires that an organisation ensures that personal data transferred overseas is protected to a standard comparable with the Data Protection Provisions. The onus is on the transferring organisation to undertake appropriate due diligence and obtain assurances when engaging a data intermediary to ensure it is capable of doing so. In undertaking its due diligence, transferring organisations may rely on data intermediaries' extant protection policies and practices, including their assurances of compliance with relevant industry standards or certification.

Example: Company A uses a Customer Relationship Management (CRM) cloud service that is offered by a service provider from the US. In using this service, Company A has to transfer personal data to the US. Company A must comply with the Transfer Limitation Obligation by ensuring that the service provider is able to afford adequate protection to the personal data transferred.
Example: Company B uses a cloud storage solution (CSS) offered by a service provider in Singapore. In providing this service, CSS has to transfer personal data to its other servers in London and Hong Kong. As CSS is carrying out this transfer on behalf of and for the purposes of Company B, Company B must comply with the Transfer Limitation Obligation. CSS will nonetheless remain responsible for compliance with the Protection and Retention Obligations in respect of the personal data that it transfers on behalf of and for the purposes of Company B.

Determination of who the data intermediary is

6.24 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 provisions 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.

6.25 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. Since B has exercised its own judgement in determining the purpose and manner of such use and disclosure of the personal data, B will be required to comply with all Data Protection Provisions.

6.26 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.

6.27 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 are 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.

6.28 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 that 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.

6.29 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

6.30 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

6.31 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"").

6.32 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.

6.33 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.

6.34 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 products 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[7]. 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[8].

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 Obligations (PDPA sections 21 and 22): An organisation must, upon request, (i) provide an individual with his or her personal data in the possession or under the control of the organisation and information about the ways in which the personal data may have been used or disclosed during the past year; and (ii) correct an error or omission in an individual's personal data that is in the possession or under the control of

[7] See PDPA section 11(2).

[8] See PDPA section 4(3).

the organisation.

e) The Accuracy Obligation (PDPA section 23): An organisation must make a reasonable effort to ensure that personal data collected by or on behalf of the organisation is accurate and complete if the personal data is likely to be 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 (PDPA section 26): An organisation must not transfer personal data to a country or territory outside Singapore except in accordance with the requirements prescribed under the PDPA.

i) The Accountability Obligation (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 Applicability to Inbound Data Transfers

11.1 The Data Protection Provisions apply to organisations carrying out activities involving personal data in Singapore. Where personal data is collected overseas and subsequently transferred into Singapore, the Data Protection Provisions will apply in respect of the activities involving the personal data in Singapore[9].

> Example:
>
> ABC, an organisation based overseas, has a contractual agreement with JKL, a data hosting company based in Singapore, for JKL to host ABC's client database. The Data Protection Provisions apply in respect of the personal data in the client database when it is in Singapore. Since JKL is acting as ABC's data intermediary in relation to the hosting of the client database pursuant to their contractual agreement, JKL is subject to the Protection and Retention Limitation Obligations in respect of such hosting.
>
> ABC discloses personal data of its clients to DEF, a company based in Singapore, for DEF to conduct its own market research. Since DEF is not a data intermediary, DEF is subject to all the Data Protection Provisions in respect of its collection, use and disclosure of personal data for its purposes.

11.2 Where personal data originating from outside Singapore is collected by an organisation in Singapore for use or disclosure for its own purposes in Singapore (that is, not as a data intermediary of another organisation), the organisation is required to comply with all Data Protection Provisions from the time it seeks to collect the personal data (if such collection occurs in Singapore) or from the time it brings the personal data into Singapore. This includes obtaining consent for the collection, use and disclosure of the personal data (where such activities will be conducted in Singapore) unless the personal data may be collected, used or disclosed without consent under the PDPA or consent may be deemed. The Commission notes that where personal data is collected outside Singapore, such collection may be subject to the data protection laws of the country or territory in which it was collected (if any). In determining whether an organisation has complied with the Notification Obligation and the Consent Obligation before collecting, using or disclosing the personal data in Singapore, the Commission will take into account the manner in which the personal data was collected in compliance with such data protection laws.

[9] The organisation will separately have to determine the applicable laws in respect of the data activities involving personal data overseas.

11.3 Where personal data collected from outside Singapore is transferred to an organisation in Singapore, the Transfer Limitation Obligation could apply to the latter organisation if it transfers the personal data outside Singapore, although the avenues for compliance depend on whether the personal data is data in transit. Please refer to the section on the Transfer Limitation Obligation for more details.

12 The Consent Obligation

12.1 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.

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

12.3 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

12.4 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".

12.5 Consent can be obtained in a number of different ways. As 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.

12.6 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

12.7 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.

12.8 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).

12.9 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 requires 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. Please refer to Chapters 7 and 8 of the Advisory Guidelines on the Do Not Call Provisions for more details.

Failure to opt out

12.10 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.

12.11 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.

12.12 In relation to the Do Not Call 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

12.13 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.

12.14 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

12.15 Section 14(2) 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.

12.16 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.

12.17 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.

12.18 Section 14(2)(a) may not prohibit certain situations in which an organisation may seek to require consent. For example, organisations may provide offers, discounts or lucky draw opportunities to individuals that are conditional on the collection, use or disclosure of their personal data for specified purposes. In any event, organisations are reminded that their 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.

12.19 When collecting personal data through a form, it is 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.

12.20 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. For more information on requiring consent for the collection, use or disclosure of personal data for marketing purposes, please refer to the Advisory Guidelines on Requiring Consent for Marketing Purposes.

12.21 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.

12.22 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

12.23 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.

12.24 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.

12.25 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.

12.26 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.

12.27 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.

12.28 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.

12.29 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.

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

12.30 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).

12.31 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.

12.32 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.

12.33 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

12.34 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.

12.35 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[10].

Example:

Sarah provides the personal data of her friend Jane to the sales consultant at her spa as part of a member's 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 indeed provided her consent.

[10] 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.

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 good 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.

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

12.36 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.

12.37 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 to 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.

12.38 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)[11] 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.

Withdrawal of consent

12.39 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.

12.40 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 likely 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

12.41 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 the individual has given reasonable notice would include the amount of time needed to give effect to the

[11] 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 and the manner in which notice was given.

12.42 The Commission considers that it would be difficult to take a one-size-fits-all approach and prescribe a specific time frame for reasonable notice to be given. However, as a general rule of thumb, the Commission would consider a withdrawal notice of at least ten (10) business days from the day the organisation receives the withdrawal notice, to be reasonable notice. Should an organisation require more time to give effect to a withdrawal notice, it is good practice for the organisation to inform the individual of the time frame by which the withdrawal of consent will take effect.

12.43 In order to enable and facilitate withdrawal, organisations are advised to make an appropriate consent withdrawal policy that is clear and 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 provision of the products/services (that may include 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.

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

12.45 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 provide 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 of 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 types of personal data by the organisation for the purpose of supplying the subscribed services. Such types 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 types 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.

12.46 If an individual has withdrawn his earlier consent to the collection, use or disclosure of his personal data by an organisation, but subsequently provides fresh consent to the organisation, the organisation may collect, use or disclose his personal data within the scope of the fresh consent that he subsequently provided.

Example:

Peter withdraws his consent to Organisation ABC to send him marketing messages via e-mail, and accordingly, ABC ceases to do so.

A few months later, Peter decides that he now wishes to receive marketing messages via e-mail from ABC and provides his consent for ABC to send him marketing messages via e-mail. ABC may now rely on the consent provided by Peter to send him marketing messages via e-mail again, notwithstanding that Peter had previously withdrawn his consent.

Effect of a withdrawal notice

12.47 In determining the effect of any notice to withdraw consent, the Commission will consider all relevant facts of the situation. This could include but is not limited to matters like:

a) the actual content of the notice of withdrawal;

b) whether the intent to withdraw consent was clearly expressed; and

c) the channel through which the notice was sent.

12.48 In cases where an organisation provides a facility for individuals to withdraw consent (e.g. by clicking on an "unsubscribe" link within an e-mail), the organisation should clearly indicate the scope of such withdrawal. The organisation is also encouraged to inform individuals of how they may withdraw consent for matters outside the scope of such withdrawal. In facilitating any notice to withdraw consent, an organisation should act reasonably and in good faith.

> Example:
>
> Organisation ABC has obtained consent from Joan to send her marketing messages via e-mail and fax.
>
> ABC sends Joan an e-mail informing her of the latest in-store promotion, and included a link for her to unsubscribe:
>
> "*If you wish to stop receiving marketing messages from ABC via e-mail, please click on the link 'unsubscribe'. If you wish to stop receiving marketing messages from ABC via other channels, please send us an e-mail at dpo@abc.org.*"
>
> Joan clicks on the 'unsubscribe' link and is directed to a website which states:
>
> "*You have unsubscribed successfully from e-mail marketing messages from ABC.*"
>
> Joan would be considered to have withdrawn consent to receive marketing messages sent by e-mail only. If Joan writes to ABC stating her intention to withdraw consent from receiving marketing messages via fax, ABC must facilitate the withdrawal of consent.

Where a withdrawal notice for marketing is kept general

12.49 Typically, where the withdrawal notice for marketing contains a general withdrawal message, i.e. it is not clear as to the channel of receiving marketing messages for which consent is withdrawn, the Commission will consider any withdrawal of consent for marketing sent via a particular channel to only apply to all messages relating to the withdrawal sent via that channel. Please see the example below for more details.

> Example:
>
> Organisation ABC has obtained consent from Sally to send her marketing messages via e-mail and fax.

ABC sends Sally an e-mail informing her of the latest in-store promotion, and included a link for her to unsubscribe:

"*If you wish to stop receiving marketing messages from ABC, please click on the link 'unsubscribe'.*"

Sally clicks on the 'unsubscribe' link and is directed to a website which states:

"*You have unsubscribed successfully.*"

As the withdrawal notice is general and does not specify the channel of receiving marketing messages for which consent is withdrawn, Sally would be considered to have withdrawn consent to receive marketing messages sent by e-mail only.

12.50 Where relevant, organisations should consider how the withdrawal notice impacts both consent obtained under the Data Protection Provisions and the Do Not Call Provisions. Please refer to Chapter 8 of the Advisory Guidelines on the Do Not Call Provisions for more details on withdrawal of consent under the Do Not Call Provisions.

Actions organisations must take upon receiving a notice of withdrawal

12.51 Once an organisation has received from an individual a notice to withdraw consent, the organisation should inform the individual concerned of the likely consequences of withdrawing his consent, even if these consequences are set out somewhere else, e.g. in the service contract between the organisation and the individual.

12.52 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. In other cases, the organisation may not be able to continue providing services to the individual or there may be legal consequences.

12.53 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 cease to collect, use or disclose the individual's personal data, and inform its data intermediaries and agents about the withdrawal and ensure that they cease collecting, using or disclosing the personal data for the various purposes.

12.54 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 give notice to withdraw consent to those other organisations directly.

12.55 Although an individual may withdraw consent for the collection, use, or disclosure of his personal data, the PDPA does not require an organisation to delete or destroy the individual's personal data upon request. Organisations may retain personal data in their 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

12.56 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

12.57 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.

12.58 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.

12.59 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[12]. His membership profile which is publicly searchable lists his name, date of birth and the university at which he is currently enrolled. Alan also regularly updates his profile picture. The data (including pictures of him) which Alan has shared on this online social network is very likely to be personal data that is publicly available, since any other user of the social network would be able to gain access to the data, even if they accessed his profile page by accident and any member of public may join the online social network.

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

12.60 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.

12.61 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.

12.62 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

[12] 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.

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.

12.63 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 by the mall 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 good practice, Store ABC should put up relevant notices to inform its 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 its 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 good 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.

12.64 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.

12.65 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.

12.66 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)[13].

12.67 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 of whether the personal data is publicly available. Please refer to the PDPA for full definitions of "news organisation" and "news activity".

[13] 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.

Example:

Charles wishes to organise a birthday party for his son David. Charles books a private room within a fast food restaurant for the occasion and invites twenty of David's friends and their parents. The private room is right by the general dining area and the interior can be seen by other patrons through the glass windows. The fast food restaurant management puts up a sign at the entrance of the private room which says "Reserved for Private Event: David's 8th birthday party". Charles keeps the door closed at all times and keeps an eye on it to ensure that only invited guests enter. The birthday party would not be considered open to the public because members of the public (who are not invited to attend) are unlikely to be able to gain access to the event.

Mary similarly wishes to organise a birthday party for her daughter Jane. She invites twenty of Jane's friends and their 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.

13 The Purpose Limitation Obligation

13.1 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).

13.2 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.

13.3 The main objective of the Purpose Limitation Obligation is to ensure that organisations collect, use and disclose personal data that are relevant for the purposes, and 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).

13.4 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.)

14 The Notification Obligation

14.1 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.

14.2 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.

14.3 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.

14.4 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).

14.5 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.

14.6 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

14.7 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.

14.8 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

14.9 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.

14.10 Relevant factors affecting an organisation's determination of the appropriate manner and form of notification to an individual of its purposes may include the following:

a) the circumstances and manner 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 channel through which the notification is provided (e.g. face-to-face or through a telephone conversation).

14.11 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

14.12 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[14]. An organisation may choose to notify individuals of the purposes for which it collects, uses and discloses personal data through its Data Protection Policy.

14.13 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.

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

[14] Please see the section on "The Accountability Obligation" more information.

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.

14.14 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 Accountability Obligation is met. Please refer to the section on "The Accountability 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.

Information to be included when stating purposes

14.15 An organisation should state its purposes at an appropriate level of detail for the individual to determine the reasons and manner in 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.

14.16 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.

Good practice considerations relating to the Notification Obligation

14.17 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.

14.18 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 channel(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 surveys a group 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.

An estate agent 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 estate agent'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

14.19 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.

14.20 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").

14.21 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.

14.22 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.

15 The Access and Correction Obligations

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

15.2 The Access and Correction Obligations relate to personal data in an organisation's possession as well as personal data that is under its control (which may not be in its possession). For example, if an organisation has transferred personal data to a data intermediary that is processing the personal data under the control of the organisation, the organisation's response to an access or correction request must take into account the personal data which is in the possession of the data intermediary. The PDPA does not directly impose the Access and Correction Obligations on a data intermediary in relation to personal data that it is processing only on behalf of and for the purposes of another organisation pursuant to a contract which is evidenced or made in writing[15]. A data intermediary may (but is not obligated under the PDPA to) forward the individual's access or correction request to the organisation that controls the personal data. The Commission understands that, in some cases, an organisation may wish to enter into a contract with its data intermediary for the data intermediary to assist with responding to access or correction requests on its behalf. In this connection, the Commission would remind organisations that engage the data intermediary, that they remain responsible for ensuring compliance with the Access and Correction Obligations under the PDPA. Please refer to the sections on data intermediaries and their obligations for more information.

<u>Obligation to provide access to personal data</u>

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

a) personal data about the individual that is in the possession or under the

[15] Section 4(2) of the PDPA states that Parts III to VI (except for section 24 (protection of personal data) and section 25 (retention of personal data)) shall not impose any obligation on a data intermediary in respect of its 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.

control of the organisation; and

b) information about the ways in which that personal data has been or may have been used or disclosed by the organisation within a year before the date of the individual's request.

15.4 Section 21(1) allows an individual to submit a request to an organisation for access to personal data about him that is in the possession or under the control of the organisation (an "access request"). Such a request may be for:

a) some or all of the individual's personal data; and

b) information about the ways the personal data has been or may have been used or disclosed by the organisation within a year before the date of the individual's request.

15.5 An organisation's obligation in responding to an access request is to provide the individual access to the complete set of personal data requested by the individual which is in the organisation's possession or under its control, unless any relevant exception in section 21 or the Fifth Schedule to the PDPA applies.

15.6 To be clear, an organisation is not required to provide access to the documents (or systems) which do not comprise or contain the personal data in question, as long as the organisation provides the individual with the personal data that the individual requested and is entitled to have access to under section 21 of the PDPA. In the case of a document containing the personal data in question, the organisation may provide only the personal data (or the sections of the document containing the personal data) if it is feasible for it to do so.

15.7 An organisation does not need to provide access to information which is no longer within its possession or under its control when the access request is received. The organisation should generally inform the requesting individual that it no longer possesses the personal data and is thus unable to meet the individual's access request. Organisations are also not required to provide information on the source of the personal data.

15.8 In certain circumstances, the individual making the access request may ask for a copy of his personal data in documentary form. Organisations should provide the copy and have the option of charging the individual a reasonable fee for producing the copy (please see the section on "fees chargeable for access to personal data" for more details). If the requested personal data resides in a form that cannot practicably be provided to the individual in documentary form, whether as physical or electronic copies (for example, the data cannot be extracted from a special

machine owned by the organisation), then the organisation may provide the individual a reasonable opportunity to examine the requested data in person.

15.9 Organisations should note that the obligation to provide access applies equally to personal data captured in unstructured forms such as personal data embedded in emails. Organisations are generally required to implement processes to keep track of the collection, use, and disclosure of all personal data under their control, including unstructured data. Organisations should note that they are not required to provide access if the burden or expense of providing access would be unreasonable to the organisation or disproportionate to the individual's interest or if the request is otherwise frivolous or vexatious. Please see the sections on exceptions to the obligation to provide access to personal data for more details (including on mandatory exceptions relating to situations where an organisation must not provide access).

15.10 If the personal data requested by the individual can be retrieved by the individual himself (e.g. resides in online portals in which access has been granted by the organisation), the organisation may inform the individual how he may retrieve the data requested.

> Example:
>
> Organisation ABC receives a request from John seeking to know what personal data relating to him was disclosed in Organisation ABC's correspondence with Organisation DEF in a specified month within the last one year. Assuming that the request does not fall under any relevant exception (for example, it is not opinion data kept solely for an evaluative purpose), Organisation ABC is required to provide John with his personal data even if its correspondence with Organisation DEF had not been archived in a formalised system such as a database.
>
> To be clear, Organisation ABC's obligation is limited to providing John with the full set of his personal data that he requested which is in their possession or control, and it is not necessarily required to provide John with copies of the actual correspondence with Organisation DEF.

15.11 The PDPA does not expressly state that an access request be accompanied by a reason for making the request. However, an organisation should ask the applicant to be more specific as to what type of personal data he requires, the time and date the personal data was collected, to facilitate processing of the access request, or to determine whether the request falls within one of the prohibitions under section

21(3) of the PDPA or any exception in the Fifth Schedule[16]. When assessing an access request, the organisation should consider the purpose of the applicant's access request, so as to determine the appropriate manner and form in which access to the personal data should be provided. For instance, the organisation may determine that it will provide the individual a print-out from a video instead of a masked video clip as the most cost effective and efficient way to allow an individual to show that he was present at a particular location at a specific date and time. If the individual is unable or unwilling to provide more details, the organisation should make an attempt to respond to the access request as accurately and completely as reasonably possible.

15.12 Before responding to an access request, organisations should exercise due diligence and adopt appropriate measures to verify an individual's identity. While the Commission does not prescribe the manner in which organisations are to obtain verification from the individual making an access request, organisations are encouraged to have documentary evidence to demonstrate that it is in compliance with the PDPA, and minimise any potential disputes. Organisations may implement policies setting out the standard operating procedures on conducting verification when processing access requests (e.g. this may include the questions that an employee handling the access request may ask the applicant in order to verify his identity)[17].

15.13 In a situation where a third party is making an access request on behalf of an individual, organisations receiving the access request should ensure that the third party has the legal authority to validly act on behalf of the individual.

15.14 In some cases, there may be two or more individuals (e.g. husband and wife) making an access request at the same time for their respective personal data captured in the same set of records. The organisation may obtain consent[18] from the respective individuals to disclose their personal data to each other, so that it may provide the individuals access to a common data set containing their personal data, without

[16] The Commission notes that an access request may be more easily fulfilled if sufficient information is provided by the applicant to enable an organisation to process the request.

[17] Among other things, an organisation must implement policies and practices that are necessary for it to meet its obligations under the PDPA under section 12 of the PDPA.

[18] The organisation may also consider if deemed consent may apply. 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. When it is unclear whether consent may be deemed, organisations should obtain consent from the individual to collect, use or disclose his personal data (as the case may be) for the relevant purposes in order to avoid any dispute over whether consent was given.

having to exclude the personal data of the other individuals[19]. If such consent cannot be obtained, an organisation receiving such requests may provide access to the personal data to the individuals separately, for example, by masking the personal data of the other individuals before providing the individual access to his own personal data (i.e. the individual will be provided access to only his own personal data).

Information relating to ways which personal data has been used or disclosed

15.15 As stated in section 21(1) of the PDPA, if an individual requests for information relating to the use or disclosure of his personal data by the organisation, the organisation is required to provide information relating to how the personal data has been or may have been used or disclosed within the past year. In this regard, an organisation may develop a standard list of all possible third parties to whom personal data may have been disclosed by the organisation. In many cases, an organisation may provide this standard list as an alternative to providing the specific set of third parties to whom the personal data has been disclosed, as part of its response to access requests that ask for information relating to how the personal data has been or may have been disclosed within the past year. The organisation should also update the standard list regularly and ensure that the information is accurate before providing the list to the individual. Generally, in responding to a request for information on third parties to which personal data has been disclosed, the organisation should individually identify each possible third party (e.g. 'pharmaceutical company ABC'), instead of simply providing general categories of organisations (e.g. 'pharmaceutical companies') to which personal data has been disclosed. This would allow individuals to directly approach the third party organisation to which his personal data has been disclosed.

15.16 In specifying how the personal data has been or may have been used or disclosed within the past year, organisations may provide information on the purposes rather than the specific activities for which the personal data had been or may have been used or disclosed. For example, an organisation may have disclosed personal data to external auditors on multiple occasions in the year before the access request. In responding to an access request, the organisation may state that the personal data was disclosed for audit purposes rather than describing all the instances when the personal data was disclosed.

15.17 Generally, the organisation's actual response would depend on the specific request,

[19] Obtaining consent from the respective parties may address the prohibition against revealing their personal data under section 21(3)(c) of the PDPA. However, organisations are reminded to also consider if there are other prohibitions or exceptions to providing access that would apply.

and organisations are reminded that in meeting their responsibilities under the PDPA, they are to consider what a reasonable person would consider appropriate in the circumstances.

> Example:
>
> Sarah makes an access request to her spa, requesting for information relating to how her personal data has been used or disclosed. The request was made on 5 December 2015. The spa is only required to provide information on how her personal data has been used or disclosed within the past year – that is, the period from 6 December 2014 to the date of the request, 5 December 2015.

Response time frame for an access request

15.18 Subject to the PDPA and the Personal Data Protection Regulations[20], an organisation is required to comply with section 21(1) of the PDPA and must respond to an access request as soon as reasonably possible from the time the access request is received. If an organisation is unable to respond to an access request within 30 days[21] after receiving the request, the organisation shall inform the individual in writing within 30 days of the time by which it will be able to respond to the request.

When not to accede to an access request

15.19 An organisation must respond to an access request by providing access to the personal data requested, or by informing the individual of a rejection of the access request where it has valid grounds not to provide access.

15.20 Organisations are not required to accede to a request if an exception[22] from the access requirement applies.

15.21 Additionally, an organisation shall not inform any individual or organisation that it has disclosed personal data to a prescribed law enforcement agency if the disclosure is necessary for any investigation or proceedings and the personal data is disclosed

[20] Please refer to sections 21(2), 21(3), 21(4) and 21(5) of the PDPA and Personal Data Protection Regulations 2014, Part II.

[21] Generally, this refers to 30 calendar days. This may however be extended in accordance with rules on computation of time under the law, e.g. where the last day of the period falls on a Sunday or public holiday, the period shall include the next day not being a Sunday or public holiday.

[22] The Fifth Schedule of the PDPA specifies the exceptions which apply.

to an authorised[23] officer of the agency. In this regard, an organisation may refuse to confirm or deny the existence of personal data, or the use of personal data without consent for any investigation or proceedings, if the investigation or proceedings and related appeals have not been completed.

15.22 It also does not have to respond to a request unless the applicant agrees to pay the fee for services provided to the applicant to enable the organisation to respond to the applicant's request. This is provided the organisation has provided the applicant a written estimate of the fee. Where applicable, the Commission may review the fee by confirming, reducing or disallowing the fee, or directing the organisation to make a refund to the applicant.

15.23 An organisation shall not accede to an access request if any of the grounds in section 21(3) are applicable, for instance, where the provision of the personal data or other information could reasonably be expected to threaten the safety or physical or mental health of an individual other than the requesting individual, or to cause immediate or grave harm to the safety or physical or mental health of the requesting individual.

15.24 If the organisation searches for the requested personal data but is unable to respond to the access request within the 30-day timeframe (e.g. technical processing of personal data residing in a specific format requires more time), the organisation must inform the applicant within the 30-day timeframe of the date when it will be able to respond to the request, and must still respond to the request as soon as reasonably possible.

Fees chargeable to comply with the access obligation

15.25 An organisation may charge an individual a reasonable fee to process an access request by the individual[24]. The purpose of the fee is to allow organisations to recover the incremental costs of responding to the access request. This may include the time and costs incurred to search for the personal data requested. An example of such incremental costs is the cost of producing a physical copy of the personal data for the individual requesting it. As organisations are required to make the necessary arrangements to provide for standard types of access requests, costs incurred in capital purchases (e.g. purchasing new equipment in order to provide access to the requested personal data) should not be transferred to individuals.

[23] Paragraph 1(n) of the Fourth Schedule of the PDPA specifies the circumstances under which an officer is authorised.

[24] Regardless of whether or not access to the personal data requested is eventually provided by the organisation.

15.26 The Commission is of the view that it would be difficult to prescribe a standard fee or range of fees at the outset to apply across all industries or all types of access requests. Organisations should exercise proper judgement in deriving the reasonable fee they charge based on their incremental costs of providing access. The Commission may, upon the application of an individual, review a fee charged by an organisation under section 28 of the PDPA (among other matters). In reviewing a fee, the Commission may consider the relevant circumstances, including the absolute amount of the fee, the incremental cost of providing access which may include the time and costs incurred to search for the personal data requested, and similar fees charged in the industry.

15.27 If an organisation wishes to charge an individual a fee to process an access request, the organisation must give the individual a written estimate of the fee[25]. If the organisation wishes to charge a fee higher than the original written estimate, it must inform the individual in writing of the increased fee. The organisation may refuse to process or provide access to the individual's personal data until the individual agrees to pay the relevant fee.

Example: Company ZYX receives an access request from a customer to view his personal data stored in a format that is readable only by a special machine. The company owns two such machines but both are faulty. In order to respond to the customer's request in a timely manner, Company ZYX purchases another machine and transfers its cost to the customer as part of the access fee. Because of this, the access fee amounted to $50,000. Under the PDPA, this would not be considered a reasonable fee as Company ZYX is expected to have the general means to comply with its customers' access requests.
Example: An individual requests from Company TUV a paper copy of his personal data. Company TUV charges a fee of $50 for the information printed out on 50 pages of paper, based on the incremental cost of producing the copy. The fee is reasonable as it reflects the incremental cost of providing the personal data.

<u>Exceptions to the obligation to provide access to personal data</u>

15.28 The obligation in section 21(1) is subject to a number of exceptions in sections 21(2) to 21(4) including some mandatory exceptions relating to situations where an

[25] If the Commission has reviewed a fee under section 28(1)(b) of the PDPA, then the final fee charged should not exceed the amount of the fee allowed by the Commission under section 28(2)(b) of the PDPA.

organisation must not provide access. These exceptions are listed below.

15.29 Section 21(2) of the PDPA provides that an organisation is not required to provide individuals with the personal data or other information specified in section 21(1) in respect of the matters specified in the Fifth Schedule to the PDPA. An organisation is not prohibited from providing information in respect of the matters specified in the Fifth Schedule and may do so if it decides to.

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

a) opinion data kept solely for an evaluative purpose[26];

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

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

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

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

f) personal data which is subject to legal privilege;

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

h) personal data collected, used or disclosed without consent for the purposes of an investigation if the investigation and associated proceedings and appeals have not been completed[27];

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

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

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

[27] The terms "investigation" and "proceedings" are defined in section 2(1) of the PDPA.

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

iii. under any written law; or

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

j) any request —

i. that would unreasonably interfere with the operations of the organisation because of the repetitious or systematic nature of the requests;

ii. if the burden or expense of providing access would be unreasonable to the organisation or disproportionate to the individual's interests;

iii. for information that does not exist or cannot be found;

iv. for information that is trivial; or

v. that is otherwise frivolous or vexatious.

Example:

A shopping centre receives a request from an individual to view all CCTV footage of him recorded at the shopping centre over the past year. In this scenario, reviewing all CCTV footage from the past year to find records of the individual making the request would require considerable time and effort. To the extent that the burden of providing access would be unreasonable to the shopping centre and disproportionate to the individual's interests as the individual is making a general request for all CCTV footage, the shopping centre is unlikely to have to provide the requested personal data under the Access and Correction Obligations.

Example:

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

Example: An individual sends an email providing feedback to Organisation XYZ. The form contains his personal data including his full name and contact number. A day later, he requests access to the personal data in the form while having full knowledge of the information he is requesting. Such a request is likely to be considered frivolous or vexatious, unless it can be shown otherwise.
Example: An individual submits an access request every fortnight for the same set of personal data in Organisation ABC's possession. Such requests are likely to be considered to unreasonably interfere with the operations of the organisation because of the repetitious or systematic nature of the requests.

15.31 In addition to the matters specified in the Fifth Schedule to the PDPA, section 21(3) specifies a number of situations in which an organisation must not provide the personal data or other information specified in section 21(1).

15.32 The situations specified in section 21(3) are where the provision of personal data or other information under section 21(1) could reasonably be expected to:

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

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

c) reveal personal data about another individual;

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

e) be contrary to the national interest[28].

<u>Providing personal data of an individual without the personal data of other individuals</u>

15.33 Section 21(5) of the PDPA provides that if an organisation is able to provide the individual with his personal data and other information requested under 21(1)

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

without the personal data of other information excluded under 21(2), 21(3) and 21(4), the organisation must provide the individual access to the requested personal data and other information without the personal data or other information excluded. For example, if the personal data requested by the individual also contains personal data of other individual(s), an organisation should consider if it is able to provide the requested personal data without the personal data of the other individuals, such as by masking out the personal data of other individual(s) before providing the personal data requested by the individual.

> Example:
>
> Mary makes an access request with Organisation ABC for footage of herself captured by Organisation ABC's CCTV system on a particular date and time.
>
> Organisation ABC looks for the requested CCTV footage, and finds that the requested footage captured personal data of Mary and two other individuals. Organisation ABC then assesses that it is possible to provide Mary access to her personal data without revealing the other individuals' personal data by masking the images of the other individuals in the same footage.

Access that may reveal personal data about another individual

15.34 One of the prohibitions, section 21(3)(c), requires that an organisation must not provide access to the personal data or other information under section 21(1) where the provision of personal data or other information could reasonably be expected to reveal personal data about another individual. The Commission is of the view that this prohibition does not apply in circumstances where:

a) the other individual has given consent to the disclosure of his personal data; or

b) any of the exceptions listed under the Fourth Schedule[29] to the PDPA apply to the extent that the organisation may disclose the personal data of the other individual without consent.

[29] Disclosure of personal data without consent

Example:

John applies to School ABC for access to CCTV footage of himself in a classroom when he was having a discussion with another classmate, Peter. Peter provides consent to the school disclosing his personal data (that is part of the CCTV footage requested by John) to John. School ABC is able to provide John access to the requested CCTV footage without masking Peter's image.

Example:

Betty applies to Shopping Centre ABC for access to CCTV footage of herself walking through the aisles of the shopping centre on a specific day and time. The CCTV footage contains images of other individuals.

Since the images of the other shoppers are recorded in a public area, the data is considered to be publicly available. Shopping Centre ABC does not need to obtain consent of the other shoppers in the CCTV footage or mask their images before providing access to Betty.

Access request relating to disclosure to prescribed law enforcement agency

15.35 Section 21(4) of the PDPA contains an additional obligation of organisations in relation to the Access and Correction Obligations. That subsection provides that where an organisation has disclosed personal data to a prescribed law enforcement agency without the consent of the individual pursuant to paragraph 1(f) or (n) of the Fourth Schedule[30] or under any other written law, the organisation must not inform the individual that personal data has been disclosed.

Access request relating to legal proceedings

15.36 Where personal data has been collected for the purpose of prosecution, investigation, civil proceedings and associated proceedings and appeals, Section 1(h) of the Fifth Schedule may apply to exempt such personal data from the access request. Organisations are thus not required to provide the requested information. Further, under Section 1(e) of the Fifth Schedule, access need not be provided in respect of a document related to a prosecution if all proceedings related to the prosecution have not been completed.

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

15.37 Where personal data has been collected prior to the commencement of prosecution and investigations but is nonetheless relevant to the proceedings, an individual should obtain access through criminal and civil discovery avenues rather than through the access obligation under the PDPA. The intent of an access obligation is to ensure that organisations remain accountable for the personal data of individuals in their possession or under their control, including ensuring the accuracy and proper use of the personal data. The Data Protection Provisions of the PDPA do not affect discovery obligations under law that parties to a legal dispute may have (e.g. pursuant to any order of court). For instance, if criminal disclosure of civil discovery regimes are applicable, section 4(6) of the PDPA applies, and any request for access to the personal data should be made pursuant to any other written laws providing for such disclosure or discovery applications. A possible advantage of obtaining access to personal data through the discovery process is that it allows the requestor to obtain un-redacted and complete documents, while and access request would grant the requestor only his personal data, with other content redacted.

Rejecting an access request

15.38 Subject to the PDPA and the Personal Data Protection Regulations[31], an organisation is to provide a reply to the individual even if the organisation is not providing access to the requested personal data or other requested information. In such a situation, and where appropriate, organisations should, as good practice, inform the individual of the relevant reason(s), so that the individual is aware of and understands the organisation's reason(s) for its decision.

Preservation of personal data when processing an access request

15.39 If an organisation has scheduled periodic disposal or deletion of personal data (e.g. the CCTV system deletes the footage every X days, or physical documents containing personal data are shredded every X days), the organisation is to identify the requested personal data, as soon as reasonably possible after receiving the access request, and ensure the personal data requested is preserved while the organisation is processing the access request.

15.40 However, organisations should generally be mindful not to unnecessarily preserve personal data "just in case" to meet possible access requests, and should not retain personal data indefinitely when there is no business or legal purpose to do so.

[31] In particular, see PDPA section 21(2), 21(3), 21(4) and 21(5) and Personal Data Protection Regulations 2014, Part II.

Preservation of personal data after rejecting an access request

15.41 If an organisation determines that it is appropriate under section 21 of the PDPA and Part II of the Personal Data Protection Regulations 2014[32] to not provide some or all of the personal data requested in the individual's access request ("withheld personal data"), the organisation should, as good practice, preserve a copy of the withheld personal data for a period of at least 30 calendar days after rejecting the access request – as the individual may seek a review of the organisation's decision. In the event the individual submits an application for review to the PDPC and the PDPC determines that it will take up the review application, as soon as the organisation receives a Notice of Review Application from the PDPC, it should, as good practice, preserve the withheld personal data until the review by PDPC is concluded and any right of the individual to apply for reconsideration and appeal is exhausted.

15.42 Notwithstanding the foregoing, in the event it is determined by the Commission or any appellate body that the organisation did not have appropriate grounds under the PDPA to refuse to provide access to the personal data in question and had therefore contravened its obligations under the PDPA, it may face enforcement action under section 29 of the PDPA.

15.43 As good practice, the organisation should keep a record of all access requests received and processed, documenting clearly whether the requested access was provided or rejected.

Example:

Mary makes an access request with Organisation ABC for CCTV footage of herself at a particular date and time. Organisation ABC has a CCTV recording system which typically keeps the CCTV footage for 30 days before the footage is overwritten.

As Mary submitted her access request before the scheduled deletion of the specific CCTV footage, the organisation should search for the requested CCTV footage as soon as reasonably possible before the footage is overwritten by the CCTV system.

a) If Organisation ABC assesses the access request and provides Mary access to the requested personal data captured in the CCTV footage, Organisation ABC must delete the footage thereafter if the purpose for collecting the personal data is no longer served by retention and it has no

[32] Requests for access to and correction of personal data.

other business or legal purpose to retain the footage in accordance with the PDPA[33].

b) If, however, Organisation ABC determines that it is to reject Mary's request to access the personal data captured in the CCTV footage, Organisation ABC should preserve the footage for a reasonable period of at least 30 calendar days after rejecting the request, to allow Mary the opportunity to exhaust any recourse under the PDPA.

Obligation to correct personal data

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

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

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

15.45 An organisation is not entitled to impose a charge for the correction of personal data required under section 22.

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

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

15.48 The other organisations which are notified of a correction made by an organisation responding to a correction request are required under section 22(4) to similarly correct the personal data in their possession or under their control unless they are

[33] Please refer to Chapter 18 on the Retention Limitation Obligation for more information.

satisfied on reasonable grounds that the correction should not be made.

> Example:
>
> An online retailer receives a request from a customer to update his address (which forms part of the customer's personal data). The retailer decides that there are no reasonable grounds to reject the customer's request and proceeds to correct the customer's address in its database.
>
> The retailer also sends the corrected address to its affiliate which is responsible for servicing the customer's warranty as the affiliate may require such information for its own legal or business purposes. The affiliate determines that it does not require the corrected address for any legal or business purpose as the customer's warranty has expired. The affiliate therefore decides that a correction should not be made to all its records relating to the customer and makes a note that it has not made the correction.
>
> The retailer need not send the corrected address to a courier company which had previously delivered certain products purchased from the retailer by the customer as the courier company was engaged to make the particular delivery and does not require an updated address of the customer for its own legal or business purposes.

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

Exceptions to the obligation to correct personal data

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

a) opinion data kept solely for an evaluative purpose[34];

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

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

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

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

Example:

An individual disputes his performance evaluation records kept by his ex-employer, Organisation ABC. In anticipation of background checks to be conducted by his new employer, an individual requests that Organisation ABC amend his performance track record to something he considers to be more favourable and accurate compared to the one kept by Organisation ABC. Organisation ABC is not obligated to make the correction to the extent that the individual's performance evaluation records constitute or contain an opinion.

Response time for a correction request

15.51 Subject to exceptions as described above, an organisation is required to correct the personal data as soon as practicable from the time the correction request is made.

[34] The term "evaluative purpose" is defined in section 2(1) of the PDPA to mean:
(a) for the purpose of determining the suitability, eligibility or qualifications of the individual to whom the data relates – (i) for employment or for appointment to office; (ii) for promotion in employment or office or for continuance in employment or office; (iii) for removal from employment or office; (iv) for admission to an education institution; (v) for the awarding of contracts, awards, bursaries, scholarships, honours or other similar benefits; (vi) for selection for an athletic or artistic purposes; or (vii) for grant of financial or social assistance, or the delivery of appropriate health services, under any scheme administered by a public agency;
(b) for the purpose of determining whether any contract, award, bursary, scholarship, honour or other similar benefit should be continued, modified or cancelled;
(c) for the purpose of deciding whether to insure any individual or property or to continue or renew the insurance of any individual or property; or
(d) for such other similar purposes as may be prescribed by the Minister.
No other such purposes have been prescribed to date.

If an organisation is unable to correct the personal data within 30 days[35] from the time the request is made, the organisation shall inform the individual in writing within 30 days of the time by which it will be able to correct the personal data.

Form of access and correction requests

15.52 While organisations may provide standard forms or procedures for individuals to submit access and/or correction requests, organisations should accept all requests made in writing and sent to the business contact information of its Data Protection Officer or in the case of a body corporate, left at or sent by pre-paid post to the registered office or principal office of the body corporate in Singapore, where sufficient information has been provided for the organisation to meet the requests (among others).

15.53 Notwithstanding the foregoing, organisations remain responsible under section 21(1) of the PDPA to provide access as soon as reasonably possible and under section 22(2) of the PDPA to correct the personal data as soon as practicable.

[35] Generally, this refers to 30 calendar days. This may however be extended in accordance with rules on computation of time under the law, e.g. where the last day of the period falls on a Sunday or public holiday, the period shall include the next day not being a Sunday or public holiday.

16 The Accuracy Obligation

16.1 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.

16.2 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.

16.3 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>

16.4 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).

16.5 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

16.6 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 the application. 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

16.7 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.

16.8 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.

17 The Protection Obligation

17.1 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.

17.2 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.

17.3 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.

17.4 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

17.5 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.

18 The Retention Limitation Obligation

18.1 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

18.2 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.

18.3 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.

18.4 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.

18.5 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.

18.6 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 be subject to the requirements of the Retention Limitation Obligation.

18.7 Organisations should develop or adjust 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.

18.8 As good 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

18.9 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).

18.10 An organisation ceases to retain documents containing personal data when it, its agents and its data intermediaries no longer have 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.

18.11 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(s) which are archived or to which access is limited will still be considered to be retained for the purposes of the Retention Limitation Obligation.

18.12 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.

Factors relevant to whether an organisation has ceased to retain personal data

18.13 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

18.14 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 the PDPA for Selected Topics.

19 The Transfer Limitation Obligation

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

Conditions for transfer of personal data overseas

19.2 Regulations issued under the PDPA specify the conditions under which an organisation may transfer personal data overseas. In essence, an organisation may transfer personal data overseas if it has taken appropriate steps to ensure that the overseas recipient is bound by legally enforceable obligations to provide the transferred personal data a standard of protection that is comparable to that under the PDPA.

19.3 Legally enforceable obligations may be imposed in two ways. First, it may be imposed on the recipient organisation under:

a) any law;

b) any contract that imposes a standard of protection that is comparable to that under the PDPA, and which specifies the countries and territories to which the personal data may be transferred under the contract;

c) any binding corporate rules that[36] require every recipient of the transferred personal data to provide a standard of protection for the transferred personal data that is comparable to that of the PDPA, and which specify (i) the recipients of the transferred personal data to which the binding corporate rules apply; (ii) the countries and territories to which the personal data may be transferred under the binding corporate rules; and (iii) the

[36] Such binding corporate rules may be adopted in instances where a recipient is an organisation related to the transferring organisation and is not already subject to other legally enforceable obligations (as described in those Regulations) in relation to the transfer. The Regulations further provide that the recipient is related to the transferring organisation if:

a) the recipient, directly or indirectly, controls the transferring organisation;
b) the recipient is, directly or indirectly, controlled by the transferring organisation; or
c) the recipient and the transferring organisation are, directly or indirectly, under the control of a common person.

rights and obligations provided by the binding corporate rules; or

d) any other legally binding instrument.

19.4 Second, if the recipient organisation holds a "specified certification" that is granted or recognised under the law of that country or territory to which the personal data is transferred, the recipient organisation is taken to be bound by such legally enforceable obligations. Under the Regulations, "specified certification" refers to certifications under the Asia Pacific Economic Cooperation Cross Border Privacy Rules (APEC CBPR) System, and the Asia Pacific Economic Cooperation Privacy Recognition for Processors (APEC PRP) System. The recipient is taken to satisfy the requirements under the Transfer Limitation Obligation if:

a) it is receiving the personal data as an organisation[37] and it holds a valid APEC CBPR certification; or

b) it is receiving the personal data as a data intermediary and it holds either a valid APEC PRP or CBPR certification, or both.

19.5 Under the Regulations, a transferring organisation is taken, without more, to have satisfied the Transfer Limitation Obligation in the following circumstances:

a) subject to conditions, the individual whose personal data is to be transferred gives his consent to the transfer of his personal data[38];

b) the transfer is necessary for the performance of a contract between the organisation and the individual (for example, if the organisation is a data intermediary of the individual pursuant to a contract between them in relation to the transfer), or to do anything at the individual's request with a view to his entering a contract with the organisation;

c) the transfer is necessary for the conclusion or performance of a contract between the organisation and a third party which is entered into at the individual's request, or which a reasonable person would consider to be in the individual's interest;

d) the transfer is necessary for a use or disclosure in certain situations where the consent of the individual is not required under the PDPA, such as use or disclosure necessary to respond to an emergency that threatens the life,

[37] As defined under the PDPA.

[38] In order to rely on consent given by the individual, the organisation should (among other things) provide the individual with a reasonable summary in writing of the extent to which the personal data transferred to those countries and territories will be protected to a standard comparable to the protection under the PDPA.

health or safety of an individual[39]. In such cases, the organisation may only transfer personal data if it has taken reasonable steps to ensure that the personal data will not be used or disclosed by the recipient for any other purpose;

e) the personal data is data in transit; or

f) the personal data is publicly available in Singapore.

19.6 The examples below illustrate certain situations in which organisations may transfer personal data overseas in compliance with the Transfer Limitation Obligation.

Example: Organisation ABC is transferring personal data of its customers to its parent company overseas via the group's centralised customer management system. The conditions of the transfer, including the protections that will be accorded to the personal data transferred, are set out in binding corporate rules that apply to both Organisation ABC and its head office. Organisation ABC has reviewed these binding corporate rules and assessed that they comply with the conditions prescribed under the regulations and would provide protection that is comparable to the standard under the PDPA. In this case, Organisation ABC's transfer of the personal data overseas would be in compliance with the Transfer Limitation Obligation.
Example: Karen purchases an overseas tour with travel agency DEF. In order to perform its obligation under its contract with Karen to make the necessary hotel reservations, travel agency DEF is required to transfer her personal data (such as her name, nationality and passport number) overseas to the hotels that Karen will be staying at during the tour. Travel agency DEF's transfer of Karen's personal data in this case would be in compliance with the Transfer Limitation Obligation as it is necessary for the performance of the contract between travel agency DEF and Karen.

[39] The specific situations are if the transfer is necessary for the personal data to be used under paragraph 1(a), (b) or (d) of the Third Schedule to the PDPA or disclosed under paragraph 1(a), (b), (c), (e) or (o) of the Fourth Schedule to the PDPA.

Example:

Cedric is a client of Organisation GHI. Organisation GHI notifies Cedric in writing that it is adopting a cloud-based solution to store and analyse its client data, which includes personal data such as clients' identification details, address, contact details and income range, and asks for Cedric's consent to move his client data to the cloud-based solution. Organisation GHI also provides Cedric with a written summary of the extent to which Cedric's personal data will be protected to a standard comparable to that under the PDPA, in the countries and territories that it will be transferred to. Should Cedric provide his consent, Organisation GHI would be able to transfer his personal data in compliance with the Transfer Limitation Obligation.

Example:

John is injured in an accident while travelling overseas. To aid John's treatment, his family doctor in Singapore transfers some of his medical records (including personal data such as his identification details, blood type, allergies, and existing medical conditions) to the overseas hospital so that John can receive medical treatment. In this case, the transfer of John's personal data would be in compliance with the Transfer Limitation Obligation as the disclosure to the overseas hospital is necessary to respond to an emergency that threatens John's life, health or safety, and John's family doctor has taken reasonable steps to ensure that the personal data transferred will not be used or disclosed by the recipient for any other purpose.

Example:

Company JKL films a commercial at a location open to the public in Singapore. The commercial captures images of individuals who pass by the filming location. Company JKL wishes to transfer the commercial to its overseas partners for use in an advertising campaign. In this instance, Company JKL's transfer of the commercial would be in compliance with the Transfer Limitation Obligation as the personal data in the commercial would be publicly available to the extent that the filming of images would be reasonably expected at that location[40].

[40] While in this case the personal data may be publicly available, as noted in the sections on 'publicly available data', Company JKL should, as good practice, put up notices at appropriate spots (e.g. at the entrances to the location) to inform passers-by that filming is taking place.

Example:

Alpha.com, a travel website that is based in Singapore, is launching a joint travel promotion offer with Japanese airline company, Air Bravo. Both organisations determine the specific categories of personal data to be collected from customers for the purpose of the joint promotion offer. Alpha.com will need to transfer the customers' personal data to Air Bravo, which is located in Japan, for the joint promotion offer.

Air Bravo informs Alpha.com that it is certified under the APEC CBPR System in Japan. Alpha.com carries out due diligence and determines that Air Bravo is indeed certified under the APEC CBPR System by referring to the list of certified organisations on the APEC website (www.cbprs.org).

In this case, Alpha.com is taken to have satisfied the requirement under the Transfer Limitation Obligation to ensure that Air Bravo is bound by legally enforceable obligations to provide to the transferred personal data a standard of protection that is at least comparable to that under the PDPA.

Example:

Organisation MNO engages a firm based in the U.S., Company PQR, as a data intermediary to use its customer relationship management (CRM) system to process and store customers' information. Organisation MNO will need to transfer its customers' personal data to Company PQR in the U.S. to use its CRM system.

Company PQR informs Organisation MNO that it is certified under the APEC CBPR System but not under the APEC PRP System. Organisation MNO carries out due diligence and determines that Company PQR is indeed certified under the APEC CBPR System by referring to the list of certified organisations on the APEC website (www.cbprs.org).

In this case, Organisation MNO is taken to have satisfied the requirement under the Transfer Limitation Obligation to ensure its data intermediary, Company PQR, is bound by legally enforceable obligations to provide to the transferred personal data a standard of protection that is at least comparable to that under the PDPA.

Example:

Organisation STU, an e-commerce retailer, engages the services of a data analytics firm based in the U.S., Company XYZ, as its data intermediary to conduct analyses on its consumers' preferences on its behalf. Organisation STU will need to transfer its customers' personal data to Company XYZ in the U.S. to conduct the analyses.

Company XYZ informs Organisation STU that it is certified under the APEC PRP System. Organisation STU carries out due diligence and determines that Company XYZ is indeed certified under the APEC PRP System by referring to the list of certified organisations on the APEC website (www.cbprs.org).

In this case, Organisation STU is taken to have satisfied the requirement under the Transfer Limitation Obligation to ensure its data intermediary, Company XYZ, is bound by legally enforceable obligations to provide to the transferred personal data a standard of protection that is at least comparable to that under the PDPA.

Example:

Company Charlie, a travel agent in Singapore, offers U.S. travel packages with resort stays at Resort Delta, a resort and travel services provider based in the U.S. Resort Delta determines the specific categories of personal data of customers to be provided for making room reservations for customers. Company Charlie will need to transfer customers' personal data to Resort Delta in the U.S. for their room reservations.

Resort Delta informs Company Charlie that it is certified under the APEC PRP System in the U.S. Company Charlie carries out due diligence and determines that Resort Delta is only certified under the APEC PRP System and not the APEC CBPR System. As Resort Delta is not receiving the personal data as a data intermediary of Company Charlie, Company Charlie may not rely on Resort Delta's APEC PRP certification to transfer personal data to Resort Delta. Company Charlie should consider whether it can rely on any other avenue as set out at paragraph 19.3 above, such as consent given by the customers for the transfer of their personal data or where it is necessary for the performance of a contract between the customers and Company Charlie.

Scope of contractual clauses

19.7 In setting out contractual clauses that require the recipient to comply with a standard of protection in relation to the personal data transferred to him that is at least comparable to the protection under the PDPA, a transferring organisation should minimally set out protections with regard to the following:

S/N	Area of protection	Recipient is:	
		Data Intermediary[41]	Organisation (except data intermediary)
1	Purpose of collection, use and disclosure by recipient		✓
2	Accuracy		✓
3	Protection	✓	✓
4	Retention limitation	✓	✓
5	Policies on personal data protection		✓
6	Access		✓
7	Correction		✓

19.8 The above table reflects the position under the PDPA that certain Data Protection Provisions are not imposed on a data intermediary in respect of its processing of personal data on behalf of and for the purposes of another organisation pursuant to a contract that is evidenced or made in writing. However, it is expected that organisations engaging such data intermediaries would generally have imposed obligations that ensure adequate protection in the relevant areas in their processing contract.

Data in transit

19.9 Data in transit refers to personal data transferred through Singapore in the course of onward transportation to a country or territory outside Singapore, without the personal data being accessed or used by, or disclosed to, any organisation (other than the transferring organisation or an employee of the transferring organisation acting in the course of his employment with the transferring organisation) while the personal data is in Singapore, except for the purpose of such transportation. An example of data in transit would be data from overseas passing through servers within Singapore enroute to its destination overseas. An organisation transferring personal data overseas will be deemed to comply with the Transfer Limitation Obligation in respect of data in transit.

[41] For the purposes of this table, the term 'data intermediary' refers to a data intermediary processing the personal data on behalf of and for the purposes of the transferring organisation pursuant to a contract evidenced or made in writing.

20 The Accountability Obligation[42]

20.1 In data protection, the concept of accountability refers to how an organisation discharges its responsibility for personal data which it has collected or obtained for processing, or which it has control over[43]. This may include situations where the organisation can determine the purposes for which the personal data is collected, used or disclosed, or the manner and means by which the data is processed. This general concept of accountability is premised on section 11(2) of the PDPA, which states, "An organisation is responsible for personal data in its possession or under its control."

20.2 Accountability under the PDPA requires organisations to undertake measures in order to ensure that they meet their obligations under the PDPA and, importantly, demonstrate that they can do so when required. Some of these measures are specifically required under the PDPA. For example, designating one or more individuals to be responsible for ensuring the organisation's compliance with the PDPA, developing and implementing policies and practices that are necessary for the organisation to meet its obligations under the PDPA ("data protection policies and practices"), and making information about their data protection policies and practices available. Other measures as described at para 20.15 are not mandatory but are good practices to help organisations in meeting their obligations under the PDPA.

Appointing a Data Protection Officer

20.3 Section 11(3) of the PDPA requires an organisation to designate one or more individuals to be responsible for ensuring that the organisation complies with the PDPA. This individual is typically referred to as a data protection officer ("DPO"). Section 11(4) further provides that an individual so designated by an organisation may delegate the responsibility conferred by that designation to another individual. Section 11(6) clarifies that the designation of an individual by an organisation under section 11(3) 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 is not transferred to the designated individual(s). On the whole, these provisions require organisations to designate the appropriate individuals, who may in turn delegate certain responsibilities to other officers, so that collectively,

[42] Previously known as the "Openness Obligation". This section has been updated to reflect developments in data protection relating to the concept of accountability as it applies to organisations which collect, use, disclose or process personal data, or control such collection, use, disclosure or processing.

[43] For more information, please refer to the PDPC's Guide to Accountability under the Personal Data Protection Act on the PDPC's website.

they co-operate to ensure that the organisation complies with the PDPA.

20.4 An organisation's DPO plays an essential role in how the organisation meets its obligations under the PDPA. The responsibilities of the DPO often include working with senior management and the organisation's business units to develop and implement appropriate data protection policies and practices for the organisation. In addition, the DPO would undertake a wide range of activities, which may include producing (or guiding the production of) a personal data inventory, conducting data protection impact assessments, monitoring and reporting data protection risks, providing internal training on data protection compliance, engaging with stakeholders on data protection matters and generally acting as the primary internal expert on data protection. Depending on the organisation's needs, the DPO may also work with (or have additional responsibilities relating to) the organisation's data governance and cybersecurity functions. The DPO can also play a role in supporting an organisation's innovation.

20.5 Individual(s) designated by an organisation under section 11(3) should be: (a) sufficiently skilled and knowledgeable; and (b) amply empowered, to discharge their duties as a DPO, although they need not be an employee of the organisation. Organisations should ensure that individuals appointed as a DPO are trained and certified[44]. The individual(s) should ideally be a member of the organisation's senior management team or have a direct reporting line to the senior management to ensure the effective development and implementation of the organisation's data protection policies and practices. As part of corporate governance, the commitment and involvement of senior management is key to ensure that there is accountability and oversight over the management of personal data in the organisation.

20.6 The DPO (or someone working with him) may also be the primary contact point for the organisation's data protection matters. Section 11(5) of the PDPA 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 20(4)(b) 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.[45] These

[44] For example, the Practitioner Certificate for Personal Data Protection (Singapore) co-issued by the PDPC and the International Association for Privacy Professionals ("IAPP").

[45] 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 (e.g. the office address) or an electronic mailing address.

individuals and persons may be the same individual or the organisation may have different persons undertaking such roles.

20.7 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.

Developing and implementing data protection policies and practices

20.8 Section 12 of the PDPA sets out four additional key requirements which form part of the Accountability Obligation.

20.9 Firstly, an organisation is required to develop and implement data protection policies and practices to meet its obligations under the PDPA[46]. As part of this, organisations should develop both internal and external policies and practices (as required), taking into account matters such as the types and amount of personal data it collects, and the purposes for such collection.[47] This entails ensuring that policies and practices are easily accessible to the intended reader. The organisation should also put in place monitoring mechanisms and process controls to ensure the effective implementation of these policies and practices.

20.10 Secondly, an organisation must develop a process to receive and respond to complaints that may arise with respect to the application of the PDPA[48]. This is to ensure that the organisation can effectively address individuals' complaints and concerns with its data protection policies and practices and aid in its overall compliance efforts.

20.11 Thirdly, an organisation is required to communicate to its staff information about its policies and practices[49]. Such communication efforts could be incorporated in organisations' training and awareness programmes and should include any additional information which may be necessary for the organisation's staff to effectively implement its data protection policies and practices. An effective training

[46] See section 12(a) of the PDPA.

[47] See para. 20.15 for other measures an organisation may wish to adopt when developing its data protection policies and practices.

[48] See section 12(b) of the PDPA.

[49] See section 12(c) of the PDPA.

and awareness programme builds a staff culture that is sensitive and alert to data protection issues and concerns.

20.12 Finally, an organisation is required to make information available on request concerning its data protection policies and practices and its complaint process[50]. This is to ensure that individuals are able to find the necessary information and, if necessary, have the means of raising any concerns or complaints to the organisation directly.

20.13 In general, an organisation's personal data protection policies and practices set the tone for the organisation's treatment of personal data, and provide clarity on the direction and manner in which an organisation manages personal data protection risks. These should be developed to address and suit specific business or organisational needs.

Other provisions related to the Accountability Obligation

20.14 The Data Protection Provisions also provide for specific circumstances where organisations have to be answerable to individuals and the PDPC, and be prepared to address these parties in an accountable manner. For example:

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[51];

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

[50] See section 12(d) of the PDPA.

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

proceedings against the organisation[52].

Other measures relating to accountability

20.15 Although not expressly provided for in the PDPA, organisations may wish to consider conducting Data Protection Impact Assessments ("DPIA") in appropriate circumstances, and implementing a Data Protection Management Programme ("DPMP") to ensure that their handling of personal data is in compliance with the PDPA.[53] Although failing to undertake such measures is not itself a breach of the PDPA, it could, in certain circumstances, result in the organisation failing to meet other obligations under the PDPA. For example, an organisation that does not conduct a DPIA may not fully recognise risks to the personal data it is handling within its IT infrastructure. This, in turn, may result in the organisation failing to implement reasonable security measures to protect such data and hence committing a breach of section 24 of the PDPA.

Example:

In its effort to comply with the PDPA and demonstrate accountability, Organisation ABC undertakes a proactive and comprehensive approach by developing a DPMP. The DPMP incorporates data protection policies to provide transparency in the manner ABC handles personal data, processes as well as roles and responsibilities of the people in the organisation. As part of its corporate risk management framework, ABC also has in place a process to conduct DPIAs to identify, assess and address personal data protection risks.

Having implemented robust personal data protection policies and practices, ABC decides to certify its data protection policies and practices under the Data Protection Trustmark ("DPTM") Certification to enhance consumer trust and provide greater assurance for its stakeholders.

[52] 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).

[53] For more information, please refer to the Guide to Data Protection Impact Assessments and Guide to Developing a Data Protection Management Programme on the PDPC's website.

PART IV: OTHER RIGHTS, OBLIGATIONS AND USES

21 Overview

21.1 The Data Protection Provisions came 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.

21.2 Since the Data Protection Provisions took effect on the appointed day, organisations are required to comply with the Data Protection Provisions and some of the existing rights, obligations and legal relationships have hence been 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.

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

22 Rights and obligations, etc. under other laws

22.1 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.

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

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

22.3 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[54].

22.4 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

[54] 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".

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 in the Third Schedule to the Banking Act, for example, in relation to obtaining consent for disclosure of personal data for a purpose specified in the Third Schedule to the Banking Act, the provisions in the Third Schedule shall prevail. However, the Data Protection Provisions will continue to apply in respect of other purposes which are not specified in the Third Schedule and also to the extent they are not inconsistent with the provisions of the Third Schedule.

23 Use of personal data collected before the appointed day

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

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

a) For collection:

i. the Data Protection Provisions do 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 Data Protection Provisions do 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 Data Protection Provisions do not apply to any disclosure of such personal data before the appointed day; and

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

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

23.4 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. Certain organisations that are in an ongoing relationship with individuals may also be exempted from the obligation to check the Do Not Call Registry in respect of specified text or fax messages related to the subject of the ongoing relationship. Please see the Advisory Guidelines on the Do Not Call Provisions for more information.

23.5 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 IV 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.

23.6 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 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 its customers to send them desktop calendars once every year. This would be considered a reasonable existing use so long as ABC's 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.

END OF DOCUMENT