PERSONAL DATA
PROTECTION COMMISSION
SINGAPORE

ADVISORY GUIDELINES ON KEY CONCEPTS IN THE PERSONAL DATA PROTECTION ACT

Issued 23 September 2013
Revised 16 May 2022

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 PDPA was first enacted in 2012 and revised in 2020. 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 3 to 6A 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;

d) Notifying the Commission and affected individuals of data breaches; and

e) 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 Parts 9 and 9A 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 comprises 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 may 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 would not need to check the Do Not Call Registry before sending certain messages related to the subject of the ongoing relationship.

2.7 Further, organisations are prohibited from sending any messages to any telephone number that is generated or obtained through the use of address-harvesting software, or to use dictionary attacks or similar automated means to send messages indiscriminately. Please refer to the Advisory Guidelines on the Do Not Call Provisions for more information.

2.8 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.

2.9 Part 9B of the PDPA sets out offences that hold individuals accountable for egregious mishandling of personal data. The offences are for knowing or reckless unauthorised (a) disclosure of personal data; (b) use of personal data for a wrongful gain or a wrongful loss to any person; and (c) re-identification of anonymised data.

2.10 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 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 1 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 whether such data is true or accurate, 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.

When is data considered "personal data"?

5.4 The most basic requirement for data to constitute personal data is that it is information about an identifiable individual. There are two principal considerations. First, is the **purpose** of information to be data about an individual or which relates to the individual. Examples include information about an individual's health, educational and employment background, as well as an individual's activities such as spending patterns. There will be situations where the personal data is incidental to the purpose of the information. For example, an internal investigations report that incidentally includes names and appointments of key actors involved in the incident under investigations. The content of individuals' communications, such as email messages and text messages, in and of themselves will generally not be considered personal data, unless they contain information about an individual that can identify the individual.

5.5 Second, the individual should be **identifiable** from the data. However, not all data that relates to an individual may identify the individual. For example, a residential address could also relate to another individual who resides there, and it may not be possible to identify a specific individual from the residential address. 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. For example, a mailing list of email addresses may not be personal data on its own, but if the list contains customer IDs that can be linked to records in the Customer Relationship Management ("CRM") system, then the list may be considered personal data.

5.6 A practical approach is to first identify the set of information under consideration (e.g. information recorded in documents and stored in files, or stored in electronic databases or IT systems). Next, organisations should apply the analysis in the preceding paragraphs and ask: (a) is the purpose of this set of information about individuals; and (b) can individuals be identified from this set of information or other information they have access to. In general, organisations should avoid making assessments in the abstract. The following paragraphs set out a few of the Commission's considerations in determining personal data.

Number of data elements in the dataset and availability of other information

5.7 The rule of thumb is that there should be at least two data elements in the dataset before individuals can be identified. Sometimes, more than two data elements may be required before an individual can be identified. This depends very much on the specificity and nature of the data elements. For example, the combination of name and NRIC number is usually sufficient to identify individuals, but email addresses may need to be combined with customer shopping preferences and purchase history before individuals can be identified from this combination of data elements. In determining whether the dataset is personal data, an organisation should not overlook the availability of other information it has or is likely to have access to. For example, a unique customer ID that can link a mailing list to the CRM system.

5.8 In general, the Commission will apply a "practicability" threshold in determining whether an organisation is likely to have access to other data that will identify an individual. As such, an organisation will not be considered to have access to other information if it is not practicable (e.g. where it requires huge costs, time, resources) even though it is theoretically or technically possible for the organisation to gain access to such information.

Nature of data

5.9 Certain types of data, by their nature or use, are more likely to identify an individual. This includes data that has been assigned exclusively to an individual for the purposes of identifying the individual (e.g. NRIC or passport number of an individual), or data of a biological nature (e.g. DNA, facial image, fingerprint, iris prints). In general, fewer data elements are required for a dataset to constitute personal data if it contains data points or data elements that are more unique to an individual. In contrast, generic information, such as gender, nationality, age or blood group, will

unlikely be able to identify a particular individual. Nevertheless, such information may still constitute part of the individual's personal data if it is combined with other information such that it can be associated with, or made to relate to, an identifiable individual.

Purpose of the dataset or document

5.10 The purpose of the dataset or document is another relevant factor to consider in determining whether it contains personal data. One of the purposes (which need not be the dominant or primary purpose) of the dataset or document should be to record or communicate information about an individual before the collection of information is considered personal data. For example:

a) Content of email messages is not personal data unless the content was intended to convey additional information about an individual (e.g., employment or medical history of an individual): *Re Executive Coach International Pte. Ltd* [2017] SGPDPC 3, *Re Interflour Group Pte Ltd* [2017] PDP Digest;

b) Private communications (e.g. WhatsApp messages and chats) are not necessarily personal data in and of themselves: *Re Black Peony* [2017] PDP Digest, in relation to screenshots of WhatsApp messages disclosed on the Internet;

c) Customer database, including extracts compiled in a document will constitute personal data: *Re K Box Entertainment Group Pte Ltd* [2016]; and

d) Communications content to name/blacklist specific individuals will constitute personal data, but the purpose of the communication may be reasonably acceptable: *Re Jump Rope* [2016].

Example:

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 dataset constitutes personal data of the individuals as they can be identified from the dataset.

If 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.

Example:

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, 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 a particular shopping mall in 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 a specific office building on 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, DEF should treat the datasets as personal data and ensure they comply with the Data Protection Provisions.

Example:

Organisation GHI collects data of its employees (i.e. educational information, blood type, full name). GHI also keeps a record of its minutes of meeting, containing information that was shared by certain employees.

When assessed holistically, the combination of employee records and company data will constitute personal data of the employees. However, the minutes of meeting on its own, will unlikely be deemed as containing personal data of the employees in the meeting as such information is not the objective of the minutes (i.e. to keep official record of actions and decisions made at a meeting).

Truth and accuracy of personal data

5.11 It should be noted that the PDPA's definition of personal data does not depend on whether the data is true or accurate. If organisations collect personal data which is inaccurate, 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.

5.12 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

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

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

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

5.15 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.

5.16 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

5.17 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 or her personal purposes".

5.18 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.

5.19 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.

5.20 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.

Derived personal data

5.21 Derived personal data is defined under the PDPA to refer to personal data about an individual that is derived by an organisation in the course of business from other personal data about the individual or another individual, in the possession or under the control of the organisation. It generally refers to new data elements created through the processing of personal data (e.g. through mathematical, logical, statistical, computational, algorithmic, or analytical methods based on the application of business-specific rules). Derived data is a general term but in the context of data portability, it does not include personal data derived by the organisation using any prescribed means or methods which are commonly known and used by the industry (e.g. simple mathematical averaging or summation).

Personal data of deceased individuals

5.22 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.

5.23 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).

5.24 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.

5.25 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.

5.26 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.

Control, not ownership, of personal data

5.27 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 provides data subjects with some extent of control over personal data, for example controlling the purpose of use through consent and withdrawal of consent, accessing and requesting for a copy of personal data or for corrections to be made. 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.

5.28 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.

5.29 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 generally 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; and

c) Any public agency.

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's 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 in paragraph 8 under Part 3 of the First 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 primarily responsible for the actions of the employees (including volunteers) which result in a contravention of the Data Protection Provisions.

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) a tribunal appointed under any written law; or

c) a statutory body specified by the Minister by notice in the *Gazette*[2].

6.14 Public agencies are excluded from the application of the Data Protection Provisions. Organisations that provide services to public agencies may either have obligations under the PDPA as data controllers or as data intermediaries.

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 (a) protection of personal data (later referred to as the "Protection Obligation"); (b) retention of personal data (later referred to as the "Retention Limitation Obligation"); and (c) notifying the organisation of data breaches as part of notification of data breaches (later referred to as the "Data Breach Notification 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

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

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. Where a data breach is discovered by a data intermediary that is processing personal data on behalf and for the purposes of another organisation, the data intermediary is required to notify the organisation without undue delay from the time it has credible grounds to believe that the data breach has occurred. 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[3].

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 that 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 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, the CSS provider has to transfer

[3] Please refer to the Guide to Managing Data Intermediaries for more information on the considerations when outsourcing data processing to data intermediaries.

personal data to its other servers in London and Hong Kong. As the CSS provider is carrying out this transfer on behalf of and for the purposes of Company B, Company B must comply with the Transfer Limitation Obligation. The CSS provider will nonetheless remain responsible for compliance with the Protection, Retention and Data Breach Notification (in relation to notifying Company B of data breaches without undue delay) 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's 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 1,000 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 telephone 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, XYZ 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, address and telephone number 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, Retention Limitation and Data Breach Notification (in relation to notifying ABC of data breaches without undue delay) Obligations 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 4 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 are 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 the 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, residential address and contact number 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 must, 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 circumstance 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 circumstance. 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 3 to 6A 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[4]. 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[5].

10.2 Broadly speaking, the Data Protection Provisions contain ten 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, 22 and 22A): An organisation must, upon request, (i) provide an individual with his or her personal data in the possession or under the control of the organisation and information about the ways in which the personal data may have been used or disclosed during the past year; and (ii) correct an error or omission in an individual's personal data that is in the possession or under the control of the organisation.

[4] See PDPA section 11(2).
[5] See PDPA section 4(3).

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 (i) unauthorised access, collection, use, disclosure, copying, modification or disposal, or similar risks; and (ii) the loss of any storage medium or device on which personal data is stored.

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 Data Breach Notification Obligation (PDPA sections 26A to 26E): An organisation must assess whether a data breach is notifiable and notify the affected individuals and/or the Commission where it is assessed to be notifiable.

j) 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 ten obligations mentioned above may have other related requirements which organisations must comply with. In addition, some of the ten 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[6].

> **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, Retention Limitation and Data Breach Notification (in relation to notifying ABC of data breaches without undue delay) 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 Consent and Notification Obligations 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.

[6] 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 Chapter 19 on the Transfer Limitation Obligation for more details.

12 The Consent Obligation

12.1 The PDPA recognises that organisations need to collect, use and disclose personal data for reasonable purposes[7] that are articulated in the PDPA through deemed consent and exceptions to the consent obligation. For all other purposes, section 13 of the PDPA provides that organisations are allowed to collect, use or disclose an individual's personal data if the individual gives his consent for the collection, use or disclosure of his personal data. This obligation to obtain the individual's consent is referred to in these Guidelines as the Consent Obligation.

12.2 This obligation does not apply where the collection, use or disclosure of an individual's personal data is required or authorised under the PDPA or any other written law. However, organisations may still need to comply with other requirements of the Data Protection Provisions. Please refer to **Annex A** for further information on the framework for the collection, use or disclosure of personal data, to obtain consent in a way that is meaningful to individuals.

Obtaining consent from an individual

12.3 Section 14(1) of the PDPA states how an individual gives consent under the PDPA. 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 do so, any consent obtained from the individual would be invalid.

12.4 Consent can be obtained in several ways. Consent that is obtained in writing or recorded in a manner that is accessible is referred to in these Guidelines as 'express consent'. Such consent provides the clearest indication that the individual has consented to notified purposes of the collection, use or disclosure of his personal data.

12.5 In situations where it may be impractical for the organisation to obtain express consent in writing, it may choose to obtain verbal consent. As good practice, organisations can consider adopting the following practices in cases when consent is obtained verbally, to prove that verbal consent had been given, in the event of disputes:

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

[7] Refer to (a) section 3 of the PDPA and Minister for Communications and Information's speech on the Personal Data Protection (Amendment) Bill on 2 November 2020 available at www.parliament.gov.sg; and (b) section 18 of the PDPA regarding the Purpose Limitation Obligation.

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: Written consent after signing up for services over the telephone

An individual wishes to sign up for certain services with a service provider over the telephone. The service provider may request the individual's consent for 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 description of the personal data provided by the individual, and recording his consent to the 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).

12.6 Depending on the facts in some cases, the Commission may consider that consent is inferred or implied from the circumstances or the conduct of the individual in question. This is a form of consent where the individual does, in fact, consent to the collection, use and disclosure of his personal data (as the case may be) by his conduct, although he has not expressly stated his consent in written or verbal form[8].

12.7 Organisations that wish to rely on the individual's consent to send specified messages to Singapore telephone numbers should ensure that the individual has given clear and unambiguous consent beforehand. Consent for the sending of specified messages to Singapore telephone numbers should be evidenced in written or other accessible form. For this purpose, verbal consent alone would be insufficient.

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

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

[8] Please refer to *Re German European School Singapore* [2019] SGPDPC 8, in relation to implied consent inferred from the parents' decision to enrol their child and to continue his enrolment in the school, after having the school's by-laws made available to them.

give consent on behalf of another.

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

When consent is not validly given

12.10 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.

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

12.12 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 sign 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.

12.13 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.

12.14 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.

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

12.16 In particular, where an organisation would be unable to provide the product or service to the individual if the individual did not consent (or withdrew consent) to the collection, use or disclosure of his personal data for that purpose, the organisation 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.

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

Deemed consent

12.18 Sections 15 and 15A of the PDPA provide for different forms of deemed consent, namely (a) deemed consent by conduct; (b) deemed consent by contractual necessity; and (c) deemed consent by notification.

12.19 Further, where an individual gives or is deemed to have given consent for disclosure of his personal data by one organisation ("A") to another organisation ("B") for a purpose, the individual is deemed to consent to the collection of his personal data by B for that purpose.

Deemed consent by conduct

12.20 Deemed consent by conduct applies to situations where the individual voluntarily provides his personal data to the organisation. The purposes are limited to those that are objectively obvious and reasonably appropriate from the surrounding circumstances. Pursuant to section 15(1), consent is deemed to have been given by

the individual's act of providing his personal data.

12.21 An individual may be regarded as voluntarily providing personal data where the individual takes certain actions that allow the data to be collected, without actually giving consent. Consent is deemed to be given to the extent that the individual intended to provide his personal data and took the action required for the data to be collected by the organisation.

Example: Deemed consent for processing of payment

Sarah makes a visit to a spa for a facial treatment. After the treatment is complete, the cashier tells her that the facial would cost her $49.99. She hands over her credit card to the cashier to make 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 is 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.

Example: Deemed consent for health check-up

Eva goes for a health check-up at a clinic and is given information on the tests that will be conducted, which involves the collection of her blood pressure, height and weight. By proceeding with the tests, Eva is deemed to consent to the collection of her personal data by the clinic for the purposes of the health check-up.

Example: Deemed consent for taxi booking

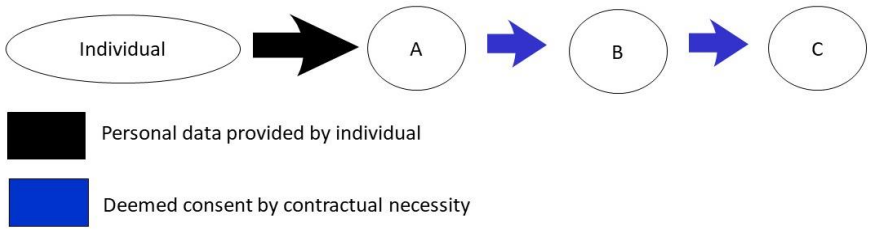
Tina calls a taxi operator's hotline to book a taxi. The customer service officer asks for her name and number to inform her of the taxi number, which Tina provides voluntarily. Tina is deemed to have consented to the taxi company using her name and number to call or text her when her taxi arrives.

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

Deemed consent by contractual necessity

12.22 The second situation in which consent may be deemed is where an individual provides his personal data to one organisation ("A") for the purpose of a transaction and it is reasonably necessary for A to disclose the personal data to another organisation ("B") for the necessary conclusion or performance of the transaction between the individual and A. Deemed consent by contractual necessity under section 15(3) extends to disclosure by B to another downstream organisation ("C") where the disclosure (and collection) is reasonably necessary to fulfil the contract between the individual and A. To be clear, deemed consent by contractual necessity allows further use or disclosure of personal data by C and other organisations downstream (refer to Diagram 1 below) where the use or disclosure is reasonably necessary to conclude or perform the contract between the individual and A.

Diagram 1:



Example: Deemed consent for processing of payment

In an example above, Sarah is deemed to consent to a spa 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 spa's bank which handles the payment. Since Sarah is deemed to consent to the disclosure of her credit card details by the spa to its bank, deemed consent by contractual necessity would apply to all other parties involved in the payment processing chain who collects or uses Sarah's personal data, where the collection, use or disclosure is reasonably necessary to fulfil the contract between Sarah and the spa. These parties include, for example, Sarah's bank, the spa's bank, the banks' processers and the credit card scheme's payment system providers.

Example: Deemed consent for processing of GIRO deduction and tax relief

Benjamin donates $5,000 to a charity organisation and provides his personal data (i.e. NRIC number, residential address, bank account details) through an online donation form on the charity organisation's website. The form clearly states the purposes of collection, use or disclosure of donors' personal data – for the charity organisation to process the donation (e.g. through GIRO deduction from the bank) and for tax relief purposes. Since Benjamin consents to the collection, use and disclosure of his personal data by the charity organisation for the notified purposes, deemed consent by contractual necessity would apply to all other parties involved in the GIRO and tax relief processing chain who collects, uses or discloses Benjamin's personal data, where the collection, use or disclosure is reasonably necessary to fulfil the transaction between Benjamin and the charity organisation. These parties include, for example, Benjamin's bank, the charity organisation's bank, the banks' processers, and the tax authority.

Example: Deemed consent for processing of payment and delivery

Bella orders furniture from a retailer through an e-commerce platform and provides her personal data (e.g. credit card details, contact number and residential address) for the purchase and delivery of goods. She also selects the option to have her furniture delivered to her home by a delivery company.

The retailer can rely on deemed consent by contractual necessity to disclose Bella's personal data to the delivery company as the disclosure is reasonably necessary to fulfil the transaction between Bella and the retailer. The delivery company and all other parties involved in Bella's transaction with the retailer would also be able to rely on deemed consent by contractual necessity to collect, use or further disclose personal data where reasonably necessary to fulfil the transaction between Bella and the retailer. These parties include, for instance, the e-commerce company, the online payment gateway in which payment for the transaction is processed, the relevant banks and logistics service partners (e.g. sub-contractors in the entire delivery chain, including the last mile delivery to Bella's home).

Deemed consent by notification

12.23 Section 15A of the PDPA provides that an individual may be deemed to have consented to the collection, use or disclosure of personal data for a purpose that he had been notified of, and he has not taken any action to opt out of the collection, use or disclosure of his personal data. Deemed consent by notification is useful

where the organisation wishes to use or disclose existing data for secondary purposes that are different from the primary purposes for which it had originally collected the personal data for, and it is unable to rely on any of the exceptions to consent (e.g. business improvement, research) for the intended secondary use. This is subject to the organisation assessing and determining that the following conditions are met, taking into consideration the types of personal data involved and the method of collection, use or disclosure of the personal data in the manner set out below:

a) **Conduct an assessment to eliminate or mitigate adverse effects**: Section 15A(4)(a) of the PDPA provides that an organisation must, before collecting, using or disclosing any personal data about an individual, conduct an assessment to determine that the proposed collection, use or disclosure of personal data is not likely to have an adverse effect on the individual. The assessment for relying on deemed consent by notification will also have to take into consideration the method of notification and opt-out period (see paragraphs 12.23(b) and (c)). Apart from identifying the likely adverse effects, the organisation's assessment should consider any measures to be taken by the organisation to eliminate, reduce the likelihood of or mitigate the adverse effects identified. Organisations may wish to use the **Assessment Checklist for Deemed Consent by Notification** (at **Annex B**) to conduct the assessment. Please refer to the Personal Data Protection Regulations 2021 and paragraphs 12.64 – 12.69 below on conducting the assessment.

b) **Organisation must take reasonable steps to ensure that notification provided to individuals is adequate**: Section 15A(4)(b) of the PDPA provides that an organisation must take reasonable steps to bring the following matters to the attention of the individual: (i) the organisation's intention to collect, use or disclose the personal data; (ii) the purpose of such collection, use or disclosure; and (iii) a reasonable period within which, and a reasonable manner by which, an individual can opt out of the collection, use or disclosure of his personal data for this purpose. The Commission does not prescribe the method by which the individual should be notified, but the organisation must ensure the notification is adequate and effective in making the individual aware of the proposed collection, use or disclosure of his personal data[9]. Organisations may choose to rely on a single mode or multiple modes of communication in notifying individuals adequately. Some considerations for determining the appropriate mode(s) of communication

[9] Refer to Chapter 14 on the Notification Obligation in these Guidelines, and PDPC's Guide to Notifications.

include:

(i) The **usual mode of communication** between the individual and the organisation.

(ii) **Whether direct communication channels such as mail, email messages, telephone calls or SMS[10] are available**. Notification provided through **interactive portals and applications** may also be considered. These could include push notifications sent through mobile applications. These also include dashboards or consent portals where individuals can keep track of their interactions with the organisation, including their preferences on purposes for which they consent to the collection, use or disclosure of their personal data. However, organisations should note that these channels may not always be effective (e.g. contact information may not be updated).

(iii) **Number of individuals to be notified**. In particular, where the organisation intends to reach out to a large number of individuals, and assesses that direct communication channels are not effective, other forms of **mass communication channels** may be considered. These include a micro-site on the organisation's corporate website, notification through the organisation's social media channels, and notifications through printed or other news media.

Example: Providing appropriate notification to users of mobile application

A health app company provides a mobile application that collects, uses and discloses personal data relating to individuals' lifestyle and wellness (e.g. number of steps walked, height, weight, age and gender). Users are able to view their activity data (e.g. sleep patterns, periods of activity, number of calories lost) through the mobile application.

The health app company intends to use the lifestyle and wellness data collected from its users to provide a personalised weight loss programme for its users. It intends to use the users' personal data to provide the personalised programme through the application installed on their devices. It assesses that there is no likely adverse effect to users in using their personal data for this purpose. Thereafter, each user can decide whether to participate after viewing the personalised programme (in which case express consent will be obtained).

[10] Where the notification constitutes a "specified message", the organisation must comply with the Do Not Call Provisions of the PDPA in sending the message via voice call, text or fax.

The health app company decides that the best way to notify users is through the mobile application as it is a direct and effective way to communicate with users who are monitoring their activity through the application. To ensure inactive users of the application are notified, it notifies users by email and through its social media channels.

c) **Organisation must provide a reasonable opt-out period**: The organisation must provide a reasonable period for the individual to opt out before it proceeds to collect, use or disclose the personal data. Consent for the collection, use or disclosure of personal data is deemed to be given only after the opt-out period has lapsed. Any collection, use or disclosure of personal data for the purposes that have been notified should commence only after the expiry of the opt-out period. Deemed consent by notification should not be relied on where individuals would not have a reasonable opportunity and period to opt out (e.g. security monitoring of premises using video cameras). The Commission does not prescribe a specific opt-out period, and organisations shall assess and determine a reasonable period for individuals to opt out of the collection, use or disclosure of personal data. Some considerations for determining the reasonableness of the opt-out period include:

(i) **The nature and frequency of interaction with the individual**. For instance, where an organisation sends push notifications through a mobile application used by individuals to track and update monthly medical check-up information, the opt-out period should not be shorter than one month.

(ii) **The communications and opt-out channels used**. Direct communications channels, particularly those that have a track record of being effective in reaching the intended customer base, may justify a shorter opt-out period than mass communications channels. Opt-out methods that are easily accessible and easy to use may also justify a shorter opt-out period (e.g. providing for opt-out via email or hyperlink).

12.24 After the opt-out period has lapsed and the individual no longer wishes to consent to the purpose, the individual can withdraw his consent for the collection, use or disclosure of personal data.

12.25 Under the Personal Data Protection Regulations 2021, the organisation must retain a copy of its assessment throughout the period that the organisation collects, uses or discloses personal data based on deemed consent by notification. When

requested by the Commission, the organisation must provide to the Commission its assessment for collecting, using or disclosing personal data based on deemed consent by notification. The organisation is not required to provide its assessment to individuals who request for it as it may contain commercially sensitive information.

Example: Hotel's sharing of personal data with partners

A hotel chain wishes to rely on deemed consent by notification to disclose personal data of its members (e.g. frequency and length of hotel stays, type of rooms, preferences and reviews) to travel website company to develop online travel resources and customised travel packages. The personal data it shares will not be used to obtain consent for sending direct marketing messages to members.

The hotel chain assesses that there is no likely adverse effect to its members in disclosing their personal data for this purpose. The hotel chain also assesses that emailing members on the intended sharing of their personal data is an appropriate and effective method of notification, as it regularly sends emails to its members regarding membership points, rewards and offers. It also assesses that 10 days is a reasonable period for individuals to opt out.

The hotel chain sends an email to its members which notifies them of the intended disclosure of their personal data to the travel website company for the purpose and provides a contact number for any queries on the intended disclosure. A hyperlink is provided in the email for members to opt out of it, and the hotel chain requests that members who wish to opt out do so within 10 days from the date of the email.

Members who do not opt out within the 10-day opt-out period are deemed to have consented to the collection, use and disclosure of their personal data for this purpose. The hotel chain will need to allow and facilitate any withdrawal of consent from members after the 10-day opt-out period.

Example: Banks' use of voice data for customer authentication

A bank collects voice data of customers when they call the bank's contact centre for managing disputes. Customers are informed that their voice data is collected for this purpose.

The bank intends to use the collected voice data (i.e. voiceprint) as an alternate means of authentication to complement existing verification methods (e.g. where the customer misplaces his credentials or where his mobile number is tagged to his bank account).

The bank assesses that its authentication of customers using voiceprint is sufficiently reliable and secure, and there is no likely adverse effect to its

customers in using their personal data for this purpose. It also assesses that emailing customers on the intended use of their personal data would be an appropriate and effective method of notification, as the bank regularly sends emails to its customers regarding the changes in its business operations and privacy policy. It also assesses that 14 days is a reasonable period for customers to opt out.

The bank sends an email to its customers to notify them of the intended use of their voice data for authentication purposes and provides a contact number for customer queries. A hyperlink is provided in the email for customers who wish to opt out of the use of their voice data for this purpose within 14 days from the date of the email.

Customers who do not opt-out within the 14-day opt-out period are deemed to consent to the use of their voice data for this purpose. After the expiry of the opt-out period, the bank may commence using voice data of customers who have not opted out to develop the biometric signatures that would be used for authentication. The bank must also allow and facilitate any requests from customers to withdraw their consent to use their voice data for this purpose after the 14-day opt-out period.

Example: Event company's use of sensors to collect visitors' personal data

An association is organising an exhibition for its members and intends to deploy sensors at the exhibition venue to collect facial images and movement data of those who visit the exhibition. The data collected would be used to analyse the exhibits visited and duration spent by each visitor. The exhibition is only open to members of the association and is not open to the public.

The association may not rely on deemed consent by notification by putting up notifications at the exhibition venue to inform visitors that facial images and movement data collected by sensors deployed at the exhibition venue would be used for analysing the exhibits visited and duration spent, as it would not be able to provide a reasonable period for them to opt out from the use of their data for this purpose.

12.26 The Commission recognises that there are various ways of implementing the opt-out method. The Commission will consider the circumstances and facts of each case in assessing whether the conditions for relying on deemed consent by notification have been met.

Consent for sending of directing marketing messages

12.27 The Personal Data Protection Regulations 2021 prescribes that deemed consent by notification does not apply to the purpose of sending **direct marketing messages**.

12.28 Organisations should generally obtain express consent for the purpose of sending direct marketing messages to individuals. Such consent should be obtained through the opt-in method (e.g. requiring action to check an unchecked box in order to give consent); the Commission does not consider the opt-out method (e.g. providing a pre-checked box and requiring action to opt-out) as appropriate for obtaining consent for the receipt of direct marketing messages. Similarly, consent obtained using the opt-out method will not constitute clear and unambiguous consent under the Do Not Call Provisions for sending a specified message to a Singapore telephone number registered on the Do Not Call Registry.

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

12.29 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 of the PDPA).

12.30 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.

12.31 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.

12.32 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 Chapter 14 on the "Notification Obligation".

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

12.33 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). 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.

12.34 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[11].

[11] 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.

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. 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

12.35 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 First Schedule and Part 1 of 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.

12.36 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 First Schedule and Part 3 of the Second 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.

12.37 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)[12] 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

12.38 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.

12.39 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)).

[12] Section 20(2) states that – "An organisation, on or before collecting personal data about an individual from another organisation without the individual's consent, must 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."

Organisations must allow and facilitate the withdrawal of consent

12.40 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 withdrawal of consent and the manner in which notice was given.

12.41 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.

12.42 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.

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

12.44 An organisation must not prohibit an individual from withdrawing his consent to the collection, use or disclosure of personal data about the individual himself. For example, if an organisation requires certain personal data from an individual in order to fulfil a contract with the individual to 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 Operator X 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 Operator X 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 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.

12.45 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

12.46 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.

12.47 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

12.48 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.

12.49 Where relevant, organisations should consider how the withdrawal notice impacts both consents 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.

<u>Actions organisations must take upon receiving a notice of withdrawal</u>

12.50 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.

12.51 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.

12.52 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.

12.53 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.

12.54 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 Chapter 18 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

12.55 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) and enumerates the permitted purposes in the First and Second Schedules to the PDPA. 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.

Legitimate interests exception

12.56 "Legitimate interests" generally refer to any lawful interests of an organisation or other person (including other organisations). Paragraphs 2 to 10 under Part 3 of the First Schedule to the PDPA relate to specific purposes that would generally be considered "legitimate interests", for instance, for evaluative purposes, for any investigation or proceedings, or for recovery or payment of debt owed. Legitimate interests exceptions in paragraphs 2 to 10 under Part 3 of the First Schedule are specific exceptions which organisations can rely on if these are applicable. The general legitimate interests exception ("legitimate interests exception") in paragraph 1 under Part 3 of the First Schedule is a broad exception that can be relied on for any other purposes that meet the definition of "legitimate interests", when other specific exceptions do not apply. To rely on this general exception,

organisations will need to assess the adverse effect and ensure the legitimate interests outweigh any adverse effect.

12.57 As the legitimate interests exception allows the collection, use or disclosure of personal data without consent for a wide range of circumstances and purposes, the onus is on the organisation seeking to rely on this exception to comply with additional safeguards to ensure that the interests of individuals are protected. Organisations must assess that they satisfy the following requirements before relying on the legitimate interests exception:

a) **Identify and articulate the legitimate interests**. Organisations must identify and be able to clearly articulate the situation or purpose that qualifies as a legitimate interest.

b) **Conduct an assessment**. Paragraph 1(2)(a) read with paragraph 1(3) under Part 3 of the First Schedule, provides that an organisation must conduct an assessment before collecting, using or disclosing personal data (as the case may be) to (i) identify any adverse effect that the proposed collection, use or disclosure is likely to have on the individual; and (ii) identify and implement reasonable measures to eliminate, reduce the likelihood of or mitigate the adverse effect on the individual. Where it is assessed that there is likely residual adverse effect to the individual after implementing the measures, organisations are required to conduct a balancing test as part of the assessment to determine that the legitimate interests of the organisation or other person (including other organisations) outweigh any likely residual adverse effect to the individual. Organisations may wish to use the **Assessment Checklist for Legitimate Interests Exception** (at **Annex C**) to conduct the assessment. Please refer to the Personal Data Protection Regulations 2021 and paragraphs 12.64 – 12.69 below for the considerations when conducting the assessment.

c) **Disclose reliance on the legitimate interests exception**. Paragraph 1(2)(b) under Part 3 of the First Schedule provides that organisations relying on the legitimate interests exception to collect, use or disclose personal data without consent must take reasonable steps to provide the individual with reasonable access to information that they are relying on the exception. This may be through any means that is reasonably effective (e.g. disclosure as part of the organisation's public data protection policy).

Identify and articulate the legitimate interests

12.58 In identifying the legitimate interests of collecting, using or disclosing the personal data for a purpose, organisations should be able to articulate the following:

a) ***What the benefits and who the beneficiaries are***: Organisations should identify the benefits arising from the collection, use or disclosure of the personal data, and who the beneficiaries are. The benefits identified should focus primarily on direct benefits of the collection, use or disclosure of the personal data. Examples of benefits include security of business assets and individuals at premises, prevention of fraud and misuse of services, etc. Organisations should also consider whether there could be any negative impact on individuals, or a particular group of individuals should the organisation not be able to collect, use or disclose the personal data without consent for the purpose. Apart from benefits to the organisation, beneficiaries could also include other organisations, the wider public or a segment of the public such as customers, employees, sectors or industries of the economy.

b) ***Whether the benefits are real and present***: In general, the identified benefits should not be purely speculative, and should include both tangible (e.g. increased business efficiency and cost savings) and intangible benefits (e.g. improved customer experience). The presence of related commercial or business interests do not subtract from the public benefits which may be derived, and all the benefits to each identified beneficiary should be considered.

12.59 Organisations cannot rely on the legitimate interests exception to send direct marketing messages. In general, organisations must obtain express consent to send direct marketing messages to individuals. In addition, where direct marketing messages are sent to Singapore telephone numbers via voice call, text or fax, the organisation must comply with the Do Not Call Provisions of the PDPA[13].

Disclose reliance on legitimate interests exception

12.60 Organisations that rely on the legitimate interests exception to collect, use or disclose personal data must make it known to individuals that they are relying on this exception to collect, use and disclose personal data without consent. For example, an organisation could state in its public data protection policy that it is relying on the legitimate interests exception to collect, use or disclose personal data for purposes of security and prevention of misuse of services. To be clear, organisations are not required to make available their assessments of legitimate interests to the public or to individuals as part of disclosing reliance on the exception.

12.61 Organisations must also provide the business contact information of a person who is able to address individuals' queries about the organisations' reliance on the

[13] Refer to PDPC's Advisory Guidelines on the Do Not Call Provisions.

legitimate interests exception. This person may be the Data Protection Officer ("DPO") or someone charged with the responsibility to handle such queries. This is similar to the requirement under the PDPA where an organisation needs to inform an individual of the purpose of the collection, use or disclosure of his personal data when it enters into an employment relationship or appoints the individual to any office; or manages or terminates an employment relationship[14], except that the information relating to the reliance on the legitimate interests exception will have to be provided through channels that are external-facing (e.g. general notification in the company's data protection policy on its publicly-accessible website).

Justify reliance on legitimate interests upon the Commission's request

12.62 Organisations that rely on the legitimate interests exception to collect, use or disclose personal data are to document their assessments and steps taken to mitigate residual risks. Under the Personal Data Protection Regulations 2021, the organisation must retain a copy of its assessment throughout the period that the organisation collects, uses or discloses personal data based on the legitimate interests exception. Upon the Commission's request, organisations are required to provide justification to the Commission on their reliance on the legitimate interests exception, including their assessments of legitimate interests (which includes balancing tests), and other related documents. Given the potential commercial sensitivity of organisations' assessments, the assessments need not be made available to the public or to individuals.

Examples of legitimate interests

12.63 Examples of legitimate interests include the purposes of detecting or preventing illegal activities (e.g. fraud, money laundering) or threats to physical safety and security, IT and network security; preventing misuse of services; and carrying out other necessary corporate due diligence[15]. Subjecting such purposes to consent is not viable as individuals may choose not to give consent or to withdraw any consent earlier given (e.g. individuals who intend to or who had engaged in illegal activities), impeding the organisations' ability to carry out such functions.

[14] Section 20(4) and (5) of the PDPA provides that, despite subsection (3), an organisation, on or before collecting, using or disclosing the personal data about an individual for the purpose of entering into an employment relationship with the individual or appointing the individual to any office; or managing or terminating the employment relationship with or appointment of the individual, shall inform the individual of (a) that purpose; and (b) on request by the individual, the business contact information of a person who is able to answer the individual's questions about that collection, use or disclosure on behalf of the organisation.

[15] This would apply to organisations that intend to conduct further and necessary corporate due diligence on customers, potential customers and business partners in addition to existing statutory requirements. For instance, the collection, use and disclosure of personal data for the consolidation of official watch lists.

Example: Fraud detection and prevention purposes by a company

An insurance company intends to collect, use and disclose personal data about its customers' past insurance claims for fraud detection and prevention.

The insurance company conducts an assessment of legitimate interests, and assesses that the benefits of the collection, use and disclosure of personal data outweigh any adverse effect to the individual. Insurance company states in its data protection policy on its website that it is relying on the legitimate interests exception to collect, use and disclose personal data for fraud detection and prevention purposes.

In this case, the insurance company may rely on the legitimate interests exception to collect, use or disclose personal data for detecting and preventing fraud.

Example: Fraud detection by multiple companies

A healthcare service provider and multiple insurance companies intend to share personal data (i.e. medical records, payment information, patient's health insurance policies, claim records) to detect and prevent healthcare fraud and abuse (e.g. duplicated claims) by creating a fraud detection model.

The companies conduct a joint assessment of legitimate interests, and assess that the benefits of the collection, use and disclosure of personal data outweighs any adverse effect to the individual. These companies also include in their respective data protection policies on their websites that they are relying on the legitimate interests exception to collect, use and disclose personal data for detecting and preventing misuse of services.

The companies may rely on the legitimate interests exception to collect, use and disclose the personal data of their customers to detect and prevent misuse of their services.

Example: Hotels' detection and prevention of misuse of services by guests

Several hotels intend to compile and share a blacklist of hotel skippers (i.e. hotel guests with track record of not fulfilling their payments for use of hotel services) to prevent further misuse of their services. The blacklist would contain the personal data of hotel skippers (i.e. full name, NRIC/passport number, amount owed and details of non-payment) who have two or more occurrences of non-payment for the use of hotel services.

These hotels conduct a joint assessment of legitimate interests, and assess that the benefits of the collection, use and disclosure of the personal data outweigh any adverse effect to the individuals. These hotels also include in their respective data protection policies on their websites that they are relying on legitimate interests exception to collect, use and disclose personal data for detecting and preventing misuse of services.

The hotels may rely on the legitimate interests exception to collect, use and disclose the personal data of customers to detect and prevent misuse of their services.

Example: Bank's network analysis to prevent fraud and financial crime, and perform credit analysis

A bank intends to integrate data across individuals and their associated organisations and businesses to build further profiles about them. The use of personal data allows the bank to identify individuals who may have committed a financial crime or received funds in relation to a crime; and to identify individuals and organisations with credit inter-dependencies to form better assessments of their actual credit standings and sources of funds for repayment.

In addition to comply with the Monetary Authority of Singapore's ("MAS") requirements[16], the bank conducts an assessment of legitimate interests and assesses that the benefits of using the data (i.e. detection and deterrence of flow of illicit funds through Singapore's financial system, understanding prospects' or customers' financial standing) outweigh any likely adverse effect to the individuals (e.g. identification of individuals with potential nefarious intentions, enforcement actions by authorities, and impact on credit facilities to individuals assessed to be of poorer credit standing).

The bank includes in its privacy policy that it is relying on the legitimate interests exception to collect, use and disclose personal data for conducting credit checks, analyses and due diligence checks as required under applicable laws.

In this case, the bank may rely on the legitimate interests exception to collect, use and disclose personal data to prevent fraud and financial crime, and perform credit analysis.

[16] Banks in Singapore are required to ensure their collection, use and disclosure of personal data are in accordance with the MAS requirements to prevent money laundering and countering the finance of terrorism.

Example: Collection and use of personal data on company-issued devices to prevent data loss

As part of its internal security defence and data loss prevention strategy, a technology company intends to install a data loss prevention software on the laptops, desktops and mobile devices which it issues to its employees so that it can effectively detect any unauthorised data leakage, disclosure or loss of its information. The tool collects a variety of personal data about its users (e.g. user log-in details, device information, files, device communications and content).

The technology company conducts an assessment of legitimate interests and assesses that the benefits of the collection of personal data to protect its commercial and proprietary interests outweigh any likely adverse effect on its employees.

The technology company includes in its privacy policy and employee handbook to inform its employees that it is relying on the legitimate interests exception for the collection and use of personal data through the software installed on company-issued devices.

Assessments for relying on deemed consent by notification[17] and legitimate interests exception[18]

12.64 Organisations are required to conduct assessments of any likely adverse effect to the individual when relying on deemed consent by notification or the legitimate interests exception.

12.65 In general, the Commission considers adverse effect to include any physical harm, harassment, serious alarm or distress to the individual. There may be circumstances where individuals may be affected by businesses' decisions resulting from the use of personal data (e.g. differential pricing for customers of differing purchase history or payment track records). To be clear, while the collection, use or disclosure of an individual's personal data could result in differentiated treatment of individuals, not all instances of differential charges (e.g. insurers charging persons with pre-existing health conditions a higher insurance premium) or refusal to provide services (e.g. rejecting loan application from an individual with poor credit rating) will be considered "adverse effect". The Commission generally considers prevailing social norms, including practices that a reasonable person would consider appropriate, when determining whether there is likely adverse effect to the individual.

[17] Refer to section 15A(4)(a) of the PDPA.
[18] Refer to paragraphs 1(2)(a) and (3) under Part 3 of the First Schedule to the PDPA.

12.66 As part of the assessment, organisations are also required to identify and put in place reasonable measures to eliminate, reduce the likelihood of or mitigate any adverse effect to the individual. In determining whether the measures implemented to eliminate or mitigate the likely adverse effects identified are appropriate, the Commission adopts a commercially reasonable standard. Examples of reasonable measures and safeguards include minimising the amount of personal data collected, encrypting or immediate deletion of personal data after use, functional separation, access controls, and other technical or organisational measures that lower the risks of personal data being used in ways that may adversely impact the individual.

12.67 Where it is assessed that there are likely **residual adverse** effects to the individual after implementing the measures, **organisations will not be able to rely on deemed consent by notification** to collect, use or disclose personal data for the purpose. Whereas for the legitimate interests exception, organisations are required to conduct a balancing test as an additional step in the assessment to determine whether the legitimate interests of the organisation or other person (including other organisations) outweigh any likely residual adverse effect on the individual. **Organisations may rely on the legitimate interests exception if the legitimate interests outweigh any likely residual adverse effect** to the individual.

12.68 **Joint assessments** may also be conducted by the disclosing and receiving organisations when relying on deemed consent by notification or legitimate interests exception to collect and disclose the personal data. In such cases, the assessment will factor in the considerations of the organisations involved. Alternatively, the disclosing and receiving organisations may conduct their assessments separately and provide their own justifications for the collection or disclosure of personal data for the identified purposes.

12.69 In determining the likely adverse effect on the individual, the organisation should consider the following:

a) ***The impact of the collection, use or disclosure of the personal data on the individual****:* Organisations are required to assess both the **severity and likelihood** of any adverse effect that may arise from the collection, use or disclosure of personal data. The assessment referred to in these Guidelines requires an assessment of **all reasonably foreseeable risks and adverse effect to the individual** resulting from the intended collection, use or disclosure. In general, the more severe the adverse effect of the collection, use or disclosure to the individual, the more unlikely the benefits of the collection, use or disclosure would outweigh the likely adverse effect. Please refer to paragraph 12.65 on adverse effect.

b) ***The nature and type of personal data and whether the individuals belong to a vulnerable segment of the population****:* In general, the potential adverse effect to individuals will be higher if the personal data is sensitive in nature. Organisations should also consider the individuals to whom the personal data relate, and whether they belong to a vulnerable group such as minors[19], individuals with physical or mental disabilities, or other special needs. The adverse effect may be more severe if the individuals belong to a vulnerable segment of the population.

c) ***The extent of the collection, use or disclosure of personal data and how the personal data will be processed and protected****:* Organisations should consider how extensive the collection, use or disclosure of an individual's personal data will be, and how the personal data will be collected, used or disclosed (e.g. whether collection is one-off or on a continuous basis). Organisations shall ensure that they do not collect, use or disclose more personal data than is reasonably necessary in order to achieve the purpose. For instance, collection of more types of data about an individual is likely to have a higher risk and adverse effect than collection of only specific types of personal data. How the personal data is protected, such as the implementation of access controls to prevent any unauthorised access, use or disclosure, may also affect the likelihood of adverse effect to the individuals.

d) ***Reasonableness[20] of the purpose of collection, use or disclosure of personal data****:* Organisations should ensure that the purpose of the collection, use and disclosure of personal data is proportionate and appropriate in the circumstances. In general, the context should be considered when assessing the reasonableness of purpose. For example, when using or disclosing personal data for a secondary purpose, organisations may wish to consider the primary purpose and how the personal data was collected, and whether it affects the reasonableness of using or disclosing the personal data for the new purpose.

e) ***Whether the predictions or decisions that may arise from the collection, use or disclosure of the personal data are likely to cause physical harm, harassment, serious alarm or distress to the individual***: Where the collection, use or disclosure of personal data is to make predictions or decisions about individuals, organisations should also consider prevailing social norms and practices that a reasonable person would consider appropriate in determining if the decisions are likely to result in unfair

[19] Refer to Chapter 7 of PDPC's Advisory Guidelines on the PDPA for Selected Topics.
[20] Refer to section 18 of the PDPA on Purpose Limitation Obligation.

discrimination, physical harm, harassment, alarm or distress to the individual.

12.70 Please refer to **Annex B** for the Assessment Checklist for Deemed Consent by Notification, and **Annex C** for the Assessment Checklist for Legitimate Interests Exception.

Business improvement exception

12.71 Part 5 of the First Schedule and Division 2 under Part 2 of the Second Schedule ("business improvement exception") enable organisations to use, without consent, personal data that they had collected in accordance with the Data Protection Provisions of the PDPA, where the use of the personal data falls within the scope of any of the following business improvement purposes[21]:

a) Improving, enhancing or developing new goods or services;

b) Improving, enhancing or developing new methods or processes for business operations in relation to the organisations' goods and services;

c) Learning or understanding behaviour and preferences of individuals (including groups of individuals segmented by profile); or

d) Identifying goods or services that may be suitable for individuals (including groups of individuals segmented by profile) or personalising or customising any such goods or services for individuals.

12.72 In order to rely on the business improvement exception, organisations will need to ensure the following:

a) The business improvement purpose cannot reasonably be achieved without using the personal data in an individually identifiable form; and

b) The organisation's use of personal data for the business improvement purpose is one that a reasonable person would consider appropriate in the circumstances.

12.73 The business improvement exception also applies to the sharing of personal data (i.e. collection and disclosure) between entities belonging to a group of companies[22], without consent, for the following business improvement purposes:

[21] "Relevant purposes" are defined in paragraph 1(2) under Part 5 of the First Schedule to the PDPA.
[22] "Group of companies" refers to related corporations within the meaning of the Companies Act (Cap. 50).

a) Improving, enhancing or developing new goods or services;

b) Improving, enhancing or developing new methods or processes for business operations in relation to the organisations' goods and services;

c) Learning or understanding behaviour and preferences of **existing or prospective customers** (including groups of individuals segmented by profile); or

d) Identifying goods or services that may be suitable for **existing or prospective customers** (including groups of individuals segmented by profile) or personalising or customising any such goods or services for individuals.

12.74 Business insights relating to individuals will be considered personal data if an individual can be identified from that data, including other information that the organisation has or is likely to have access (e.g. insights and predictions generated about a specific individual). The Commission recognises that it may be necessary for organisations to share data regarding customer behaviour and preferences to improve products as part of the feedback loop in product development. In such cases, organisations may rely on the business improvement exception as the sharing of personal data is relevant to the eventual aim of improving, enhancing or developing new goods or services.

12.75 **"Existing customers"** refer to individuals who have a history of purchasing or hiring any goods or using any services provided by the organisation. "**Prospective customer"** generally refers to an individual who:

a) informs or has informed the organisation of his interest in its goods or services. The level of interest includes subscription to a mailing list and extends to requests for information concerning specific goods or services.

b) conducts or is conducting negotiations to purchase or hire or use any goods or use of services provided by the organisation. Negotiations can range from exploratory discussions to negotiations with a view to conclude an agreement.

12.76 Organisations relying on the business improvement exception to share personal data within the group will need to ensure the following:

a) The business improvement purpose cannot reasonably be achieved without sharing the personal data in an individually identifiable form;

b) The organisations' sharing of personal data for the business improvement

purpose is one that a reasonable person would consider appropriate in the circumstances; and

c) The organisations involved in the sharing are bound by any contract or other agreement or binding corporate rules requiring the recipient(s) of personal data to implement and maintain appropriate safeguards for the personal data.

12.77 Organisations cannot rely on the business improvement exception to send direct marketing messages[23]. In general, organisations must obtain express consent to send direct marketing messages to individuals. In addition, where direct marketing messages are sent to Singapore telephone numbers via voice call, text or fax, the organisation must comply with the Do Not Call Provisions of the PDPA[24].

Example: Use of personal data to create credit risk model for operational efficiency

A bank intends to use personal data it has of its customers (i.e. income and transaction history with the bank) to create a credit risk model to reduce the time taken for it to assess and approve loan applications.

The bank assesses that it requires the use of data in individually identifiable form for this purpose, and that its use of personal data to create the credit risk model or loan application approvals is considered appropriate to a reasonable person. The bank considers the use of credit risks models for loan application approvals to be a common industry practice.

The bank may rely on the business improvement exception to use personal data without consent to create a credit risk model to improve operational efficiency and service improvement (i.e. reduced time for loan applications).

[23] Refer to paragraph 1(6) under Part 5 of the First Schedule to the PDPA.
[24] Refer to PDPC's Advisory Guidelines on the Do Not Call Provisions.

Example: Use of personal data to understand spending habits and develop new credit services

A credit card company wants to use its customers' personal data (i.e. credit payment history) to derive insights on spending habits of its customers, to develop its new line of credit card and design new credit card reward schemes. The credit card company assesses that (a) it requires the use of data in individually identifiable form for the purpose; and (b) its use of personal data is considered appropriate to a reasonable person.

The credit card company may rely on the business improvement exception to use its customers' personal data without consent to understand its customers better and to develop new products and services.

Example: Use of personal data to train machine learning models

A wearables company intends to develop and provide a new functionality in its health tracking mobile application to provide its customers with timely reminders based on changes to individuals' vital signs. The company intends to use the personal data of its customers (i.e. heart rate, steps count) to train its machine learning model for the monitoring of vital signs and develop the new functionality.

The wearables company assesses that the use of anonymised data is enough for model training to develop and provide the new functionality. However, it assesses that the historical personal data of each customer is necessary when personalising the new product feature for that customer, and that its use of personal data for this purpose is considered appropriate to a reasonable person.

The wearables company may rely on the business improvement exception to use its customers' personal data without consent to improve or enhance its products or services and personalise services or goods for its customers.

Example: Sharing of personal data within a group of related corporations to learn or understand behaviour and preferences of prospective customers

A supermarket and a seafood restaurant belong to a group of companies. The supermarket intends to share the personal data of its customers (e.g. customers' shopping propensity) with the seafood restaurant so the seafood restaurant can learn and understand its prospective customers better (e.g. to offer dining privileges for seafood lovers).

In order to rely on the business improvement exception to share personal data with the seafood restaurant, the supermarket must ensure that the personal data discloses relates to individuals who are (i) the supermarket's customers and (ii) the seafood restaurant's customers or prospective customers. The supermarket should not disclose the shopping propensity of all its customers without first doing the check on overlaps of customers between itself and the seafood restaurant. In this case, the supermarket will only be sharing personal data of its customers who are also customers of the seafood restaurant or who signs up to receive the seafood restaurant's marketing information.

The supermarket should also ensure that the seafood restaurant is bound by an agreement (e.g. contract, binding corporate rules) that requires the seafood restaurant to implement and maintain appropriate safeguards for the personal data shared.

Example: Sharing of personal data to automate claim approvals to improve operational efficiency and develop new insurance products

A healthcare service provider and an insurance company belong to a group of companies. The insurance company intends to collect personal data from the healthcare service provider (i.e. medical records, payment information) to create an automated claim assessment system to improve the insurance company's efficiency and to develop new insurance products.

The healthcare service provider assesses that the sharing of individually identifiable data may not be necessary as the insurance company can use non-individually identifiable data (e.g. aggregated patient profile data) to develop an automated claim assessment system. Furthermore, the sharing of medical information for this purpose is unlikely to be considered appropriate to a reasonable person.

The healthcare service provider and the insurance company may not rely on the business improvement exception to share personal data without consent for this purpose.

Sending of direct marketing messages and preparatory activities to marketing

12.78 To be clear, organisations cannot rely on the exceptions for legitimate interests or business improvement for the purpose of **sending direct marketing messages**.

12.79 Notwithstanding this, organisations may rely on the business improvement exception to use existing customers' personal data for data analytics and market research to derive insights and understand their existing customers prior to their business marketing activities. The Commission considers these to be **preparatory**

activities for marketing purposes and are to be distinguished from the sending of direct marketing messages to individuals.

Research exception for the use and disclosure of personal data without consent

12.80 While the business improvement exception is intended to enable organisations to use personal data to improve their products, services, business operations and customer experience, the research exception is intended to enable organisations to conduct broader research and development that may not have any immediate application to their products, services, business operations or market. Commercial laboratories that carry out research for the development of science, institutes of higher learning that conduct research into the arts and social sciences, and organisations that carry out market research are examples of organisations that can continue to rely on the research exception. The research exception provides that organisations may **use** personal data for a research purpose, including historical and statistical research, subject to the following conditions:

a) The research purpose cannot reasonably be accomplished unless the personal data is provided in an individually identifiable form;

b) There is a clear public benefit to using the personal data for the research purpose;

c) The results of the research will not be used to make any decision that affects the individual; and

d) In the event the results of the research are published, the organisation must publish the results in the form that does not identify the individual.

12.81 Similarly, organisations may rely on the research exception to disclose personal data for a research purpose, including historical and statistical research. All the conditions for use of personal data for a research purpose are applicable together with the following **additional condition**:

a) It is impracticable for the organisation to seek the consent of the individual for the disclosure.

12.82 When assessing whether it would be "impracticable" for the organisation to seek consent of the individual, the specific facts of the case will have to be considered. Factors that the Commission considers relevant in assessing whether it is "impracticable" to seek consent may include, but are not limited to:

a) Organisation does not have current contact information of the potential research subject or sufficient information to seek up-to-date contact

information. The organisation should be able to demonstrate that the potential research subject cannot be reached using the contact information, such as by attempting to contact the potential research subject.

b) Given the target population required for meaningful conclusions to be drawn from the research, the quantum of the research grant and the period allotted for the research, the costs of attempting to seek consent from each potential research subject would impose disproportionate resource demands and burden on the organisation or take up so much time that carrying out the research is no longer viable. In this regard, there is no fixed number of subjects that would be determined as "impracticable" to seek consent from. Such an assessment would be based on all relevant circumstances of the case, which may include the nature and extent of the personal data required, whether or not there is an existing relationship with the individuals, and other factors affecting the difficulty of contacting the required research subjects.

c) Exceptional circumstances where seeking the research subject's consent would affect the validity or defeat the purposes of the research, in particular, where seeking consent would skew the research or introduce bias into the research such that no meaningful conclusions can be drawn. Organisations should nevertheless consider whether it is possible to seek consent in a manner that would not introduce such bias.

12.83 The Commission considers the degree of practicability. Mere inconvenience, such as to the organisation or the potential research subject, would not amount to "impracticability". Organisations relying on this exception have to demonstrate that the additional costs or time delays resulting from having to contact individuals for consent is so onerous such that the research is no longer viable. Organisations may use convenient and practical means for individuals to provide consent, for instance through an online form or replying to a letter, email, text message or recording of voice call, instead of requiring the individual to make a trip to the organisation for the purpose of giving consent.

Publicly available data

12.84 Another significant exception in paragraph 1 under Part 2 of the First Schedule 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.

12.85 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.

12.86 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[25]. 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.

12.87 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.

[25] 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.

12.88 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 takes 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.

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

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

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

12.90 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.

12.91 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.

12.92 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.

12.93 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)[26].

12.94 For the avoidance of doubt, the PDPA provides an exception 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".

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.

[26] 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.

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 Chapter 14 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 chapters 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 or 15A 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 First and Second 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), (4) and (5) 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[27]. 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

[27] Please see Chapter 211 on "The Accountability Obligation" more information.

provide a more specific description of its purposes to a particular individual who will be providing his personal data in a particular situation (such as when subscribing for a particular service), to provide clarity to the individual on how his personal data would be collected, used or disclosed.

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 Chapter 21 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 DPO) 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 form clearly and legibly states that "Your personal data will be used by the supermarket and 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 real estate agency's market research and product planning purposes, and that it would not be used to contact individuals after they leave the show flat. The real estate agency would be considered to have provided appropriate notification in this case.

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

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 in accordance with Section 15 or 15A of the PDPA; and

c) whether the purpose falls within the exceptions from consent in the First and Second 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, 22 and 22A 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[28]. 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.

Obligation to provide access to personal data

15.3 Section 21(1) of the PDPA provides that, upon request by an individual, an organisation must 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

[28] Section 4(2) of the PDPA states that Parts 3, 4, 5, 6 (except sections 24 and 25), and 6A (except sections 26C(3)(a) and 26E) do 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 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, so 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 should, where feasible, provide only the personal data (or relevant sections of the document containing the personal data) without providing access to the entire document in its original form.

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 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), ABC is required to provide John with his personal data even if its correspondence with DEF had not been archived in a formalised system such as a database.
>
> To be clear, ABC's obligation is limited to providing John with the full set of his personal data that he requested which is in its possession or control, and it is not necessarily required to provide John with copies of the actual correspondence with 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[29]. 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 snapshot from a video recording, 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 they are 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)[30].

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[31] 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 having to exclude the personal data of the other individuals[32]. If such consent cannot be obtained, an organisation receiving such requests may provide access to the

[29] 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.

[30] 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.

[31] The organisation may also consider if deemed consent may apply (see sections 15 and 15A of the PDPA). 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.

[32] 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.

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 their 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, 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 2021[33], 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[34] 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[35] 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 to an authorised[36] 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.

[33] Please refer to sections 21(2) to 21(7) of the PDPA and Part 2 of the Personal Data Protection Regulations 2021.

[34] 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.

[35] The Fifth Schedule of the PDPA specifies the exceptions from access requirement.

[36] Paragraph 4 under Part 3 of the Second Schedule to the PDPA specifies the circumstances under which an officer is authorised.

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[37]. 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.

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 48H of the PDPA (among other matters). In reviewing a

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

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[38]. 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, ZYX purchases another machine and transfers its cost to the customer as part of the access fee. Because of this, the access fee amounts to $50,000. This would not be considered a reasonable fee as 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 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

[38] If the Commission has reviewed a fee under section 48H(1)(d) of the PDPA, then the final fee charged should not exceed the amount of the fee allowed by the Commission under section 48H(2)(d) of the PDPA.

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[39];

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[40];

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

i. under a collective agreement under the Industrial Relations Act 1960;

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

[39] The term "evaluative purpose" is defined in section 2(1) of the PDPA.
[40] The terms "investigation" and "proceedings" are defined in section 2(1) of the PDPA.

j) any request —

i. that would unreasonably interfere with the operations of the organisation because of the repetitious or systematic nature of the requests (i.e. considering the number and frequency of requests received);

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 Obligation.

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 photograph 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[41];

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 or her identity; or

e) be contrary to the national interest[42].

Providing personal data of an individual without the personal data of other individuals

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 section 21(1) without the personal data of other information excluded under sections 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

[41] Paragraphs (c) and (d) do not apply to any user activity data about, or any user-provided data from, the individual who made the request despite such data containing personal data about another individual.
[42] 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.

excluded. Organisations may request information about the purpose of the access request so that it can 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 requested Travel Agency ABC to furnish formal documentation confirming the cancellation of her transit flight to process her insurance claims.

As the letter from the airline also contains the personal data of 36 other passengers who signed up for the same tour package, e.g. name, nationality, date of birth and passport number, ABC assesses that it is possible to provide Mary access to her personal data without revealing the other individuals' personal data by redacting the personal data of the other passengers from the letter.

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 prohibition does not apply to any user activity data[43] about, or any user-provided data from, the individual who made the request despite such data containing personal data about another individual. Although organisations do not need to mask or remove personal data of these other individuals in user-activity or provided data, organisations should still consider if the other harmful situations in 21(3) may arise. In addition, the Commission is of the view that this prohibition does not apply in circumstances where:

a) any of the exceptions relating to disclosure of personal data without consent listed under the First and Second Schedules to the PDPA apply to the extent that the organisation may disclose the personal data of the other individual without consent (e.g. if the personal data of the individual is publicly available or if the organisation can rely on the legitimate interests exception);

b) as permitted or required by any other law and regulation (e.g. exercise of police investigatory powers, compliance with discovery directions in civil

[43] User activity data is defined in the PDPA as personal data about an individual that is created in the course or as a result of the individual's use of any product or service provided by the organization.

proceedings or regulations governing building maintenance and strata management); or

c) the other individual has given consent to the disclosure of his personal data.

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 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.

Example:

John applies to Organisation DEF for records of his transactions and purchases made on DEF's platform. Some of the transactions and purchases made by John on DEF's platform contain personal data of a third-party (e.g. name of third-party whom John had sent an item to after purchasing that item on the platform). As the personal data of the third-party forms part of John's user activity data in this instance, Organisation DEF may provide John with access to the data without redacting the personal data of the third-party.

Example:

Jane applies to Condominium ABC for access to CCTV footage of herself at the Condominium's taxi drop off point where she had an altercation with a third-party. As the taxi drop off point is open to the public, ABC can rely on the publicly available data exception and need not mask the image of the third-party within the footage in providing Jane access to the requested footage.

Example:

Jack is a subsidiary proprietor/owner of a unit in Condominium XYZ. Jack applies to Condominium XYZ's management for access to CCTV footage of himself at the condominium's lift lobby as he believes he dropped his personal belongings there. There were other people with Jack at the lift lobby at that time and Jack wishes to approach them for assistance in recovering his personal belongings.

Under Section 47 of the Building Maintenance and Strata Management Act (BMSMA), a subsidiary proprietor/owner of a condominium unit may make an access request for the CCTV footage without the need to redact/mask the footage.[44] As PDPA is considered a baseline law, other sectoral regulations, such as BMSMA, which permit the access to unredacted footage, will take precedence in this instance.

Example:

There is a children's party being held at the function room of Condo KLM where a CCTV is installed. Jessie and her daughter, who do not stay or own a unit in Condo KLM, are guests of the host of the party. Jessie loses her personal belongings at the party. She decides to go directly to Condo KLM's management to request for a copy of the CCTV footage to assist her in locating the belongings.

KLM assesses that there is legitimate interest in providing Jessie with access to the footage, without masking the images of other individuals, to assist her in recovering her personal belongings. KLM also assesses that in doing so, there is no adverse effects to individuals present at the party. As such, KLM allows Jessie access to the requested footage. KLM designs an approval process for such requests and addresses risks of abuse by limiting Jessie's access to viewing of the relevant CCTV footage under supervision.

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 Obligation. That subsection provides that where an organisation has disclosed personal data to a prescribed law enforcement agency without the consent of the individual under the PDPA or 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, paragraph 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 paragraph 1(e) of the Fifth Schedule, access need not be provided in

[44] In *Cheong Yoke Ling @ Zhang Yuling and another v Management Corporation Strata Title Plan No 508 and others* [2020] SGDC 295, the District Court held that where a request for inspection had been made under Section 47 of BMSMA, the MCST could allow inspection without redacting personal data (i.e. the images of third parties).

respect of a document related to a prosecution if all proceedings related to the prosecution have not been completed.

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 the 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 2021[45], 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, organisations should 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 Section 22A of the PDPA and the Personal Data Protection Regulations 2021 requires organisations to preserve a complete and accurate copy of the personal data if they refused to provide that personal data.

15.40 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.

[45] In particular, see PDPA section 21(2) to 21(7) and Part 2 of the Personal Data Protection Regulations 2021.

15.41 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.

Preservation of personal data after rejecting an access request

15.42 If an organisation determines that it is appropriate under section 21 of the PDPA and Part 2 of the Personal Data Protection Regulations 2021[46] to not provide some or all of the personal data requested in the individual's access request ("withheld personal data"), the organisation must preserve a complete and accurate 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 Commission and the Commission determines that it will take up the review application, as soon as the organisation receives a Notice of Review Application from the Commission, it must preserve a complete and accurate copy of the withheld personal data until the review by Commission is concluded and any right of the individual to apply for reconsideration and appeal is exhausted.

15.43 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 sections 48I and 48J of the PDPA.

15.44 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. 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 ABC assesses the access request and provides Mary access to the requested personal data captured in the CCTV footage, ABC must delete

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

the footage thereafter if the purpose for collecting the personal data is no longer served by retention and it has no other business or legal purpose to retain the footage in accordance with the PDPA[47].

b) If, however, ABC determines that it is to reject Mary's request to access the personal data captured in the CCTV footage, 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

15.45 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.

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

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

15.48 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.

15.49 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

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

correct the personal data in their possession or under their control unless they are 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.

15.50 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.

<u>Exceptions to the obligation to correct personal data</u>

15.51 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[48];

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

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

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

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

f) derived personal data.

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, the individual requests that ABC amend his performance track record to something he considers to be more favourable and accurate compared to the one kept by ABC. 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

15.52 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.

[48] The term "evaluative purpose" is defined in section 2(1) of the PDPA to mean:
(a) 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) the purpose of determining whether any contract, award, bursary, scholarship, honour or other similar benefit should be continued, modified or cancelled;
(c) 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) such other similar purposes as the Minister may prescribe.

If an organisation is unable to correct the personal data within 30 days[49] 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

15.53 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 DPO 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).

15.54 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.

[49] 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.

Accuracy of derived personal data

16.9 The Commission recognises that organisations may derive personal data from the raw personal data collected either directly from the individual or from third party sources. In such cases, organisations should ensure that the raw personal data is materially accurate before further processing takes place, as well as the accuracy of processing (e.g. computation of mean and median from the range of input data is accurate). Where the derived data involves grouping or labelling individuals based on pre-defined categories and profiles, organisations should ensure that the categorisation and selection criteria (i.e. business rules) are applied accurately at the data processing stage.

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 (a) unauthorised access, collection, use, disclosure, copying, modification or disposal, or similar risks; and (b) the loss of any storage medium or device on which personal data is stored. 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;

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

iv. the personal data is used for an organisation's business improvement purposes such as improving, enhancing or developing goods or services, or learning about and understanding the behaviour and preferences of its customers; or

v. retention of the personal data is necessary for research, archival, historical, artistic or literary purpose(s) that benefits the wider public or a segment of the public.

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.

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

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 chapter 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 organisations to transfer personal data to another organisation outside Singapore in circumstances where it relinquishes possession or direct control over the personal data. Such circumstances include transferring personal data to another company within the same group for centralised corporate functions, or to a data intermediary for data processing. In situations where personal data transferred or situated overseas remains in the possession or control of an organisation, the organisation has to comply with all the Data Protection Provisions. Such situations include where an employee travels overseas with customer lists on his notebook; an organisation owns or leases and operates a warehouse overseas for archival of customer records; or an organisation stores personal data in an overseas data centre on servers that it owns and directly maintains. In these examples, the organisation has direct primary obligations under the Data Protection Provisions to, *inter alia*, protect the personal data, give effect to access and correction requests, and include these overseas data repositories in its data retention policy.

19.2 This is because the Transfer Limitation Obligation is a manifestation of the Accountability Obligation. When an organisation discloses personal data to another organisation, and both are in Singapore, the receiving organisation is subject to the PDPA and has to protect the personal data that it thereby receives. Likewise, when an organisation discloses personal data to its data intermediary, and both are in Singapore, the data intermediary is subject to the Protection, Retention Limitation and Data Breach Notification Obligations for the personal data that it thereby receives. However, when an organisation transfers personal data to another organisation that is outside Singapore (for example, a data intermediary or another company in the same group), the recipient organisation is not subject to the PDPA. The Accountability Obligation requires that the transferring organisation takes steps to ensure that the recipient organisation will continue to protect the personal data that it has received to a standard that is comparable to that established in PDPA. This is the *raison d'etre* for the Transfer Limitation Obligation.

19.3 Thus, 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, i.e. to ensure that organisations provide a standard of protection to transferred personal data 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

19.4 The Personal Data Protection Regulations 2021 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 or specified certifications to provide the transferred personal data a standard of protection that is comparable to that under the PDPA.

19.5 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[50] 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 rights and obligations provided by the binding corporate rules; or

d) any other legally binding instrument.

19.6 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 Personal Data Protection Regulations 2021, "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

[50] 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 Part 3 of the Personal Data Protection Regulations 2021) in relation to the transfer. These 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.

Obligation if:

a) it is receiving the personal data as an organisation[51] 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.

19.7 Organisations are encouraged to rely on legally enforceable obligations or specified certifications outlined in paragraphs 19.5 and 19.6, especially when they have an ongoing relationship with the recipient organisation. Legally enforceable obligations provide better accountability. In addition, under the Personal Data Protection Regulations 2021, a transferring organisation is also taken to have satisfied the Transfer Limitation Obligation in certain circumstances. As good practice, organisations are encouraged to rely on these circumstances only if they are unable to rely on legally enforceable obligations or specified certifications:

a) the individual whose personal data is to be transferred gives his consent to the transfer of his personal data, after he has been informed about how his personal data will be protected in the destination country[52];

b) the individual is deemed to have consented to the disclosure by the transferring organisation of the individual's personal data where the transfer is reasonably necessary for the conclusion or performance of a contract between the organisation and the individual, including the transfer to a third party organisation);

c) the transfer is necessary for a use or disclosure that is in the vital interests of individuals or in the national interest, and the transferring organisation has taken reasonable steps to ensure that the personal data will not be used or disclosed by the recipient for any other purpose;

d) the personal data is data in transit; or

e) the personal data is publicly available in Singapore.

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

[51] As defined under the PDPA.

[52] 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.

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 ABC and its head office. ABC has reviewed these binding corporate rules and assessed that they comply with the conditions prescribed under the Personal Data Protection Regulations 2021 and would provide protection that is comparable to the standard under the PDPA. In this case, ABC's transfer of the personal data to its parent company 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 relies on section 15(6) of the PDPA 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.

Example:

Cedric is a client of Organisation GHI. 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. 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, 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 (pursuant to paragraph 2 under Part 1 of the First Schedule to the PDPA), 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[53].

Example:

Alpha.com, a travel website that is based in Singapore, is launching a joint travel promotion 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. Alpha.com will need to transfer the customers' personal data to Air Bravo, which is located in Japan, for the joint promotion.

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).

[53] 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.

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 US, Company PQR, as a data intermediary to use its CRM system to process and store customers' information. MNO will need to transfer its customers' personal data to Company PQR in the US to use its CRM system.

Company PQR informs MNO that it is certified under the APEC CBPR System but not under the APEC PRP System. 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, 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 US, Company XYZ, as its data intermediary to conduct analyses on its consumers' preferences on its behalf. STU will need to transfer its customers' personal data to Company XYZ in the US to conduct the analyses.

Company XYZ informs STU that it is certified under the APEC PRP System. 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, 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 US travel packages with resort stays at Resort Delta, a resort and travel services provider based in the US. 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 US for their room reservations.

Resort Delta informs Company Charlie that it is certified under the APEC PRP System in the US. 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 19.5 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

19.9 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[54]	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		✓

[54] 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.

S/N	Area of protection	Recipient is:	
		Data Intermediary[54]	Organisation (except data intermediary)
6	Access		✓
7	Correction		✓
8	Data Breach Notification	✓ To notify organisation of data breaches without undue delay	✓ To assess and notify the Commission/affected individuals of data breaches, where relevant

19.10 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. The Commission also recognises and encourages the use of the ASEAN Model Contract Clauses ("MCCs")[55], which are contractual terms setting out baseline responsibilities, required personal data protection measures, and related obligations of the parties that protects the data of individuals, to fulfil the Transfer Limitation Obligation.

Data in transit

19.11 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.

[55] Refer to ASEAN's website for the MCCs, and PDPC's website for the Commission's additional guidance to companies in Singapore to wish to utilise the MCCs in their business contracts.

20 The Data Breach Notification Obligation

20.1 Part 6A of the PDPA sets out the requirements for organisations to assess whether a data breach is notifiable, and to notify the affected individuals and/or the Commission where it is assessed to be notifiable. Data intermediaries that process the personal data on behalf and for the purposes of another organisation (including a public agency) are also required to notify that other organisation or public agency of a data breach detected. This obligation is referred to in these Guidelines as the Data Breach Notification Obligation ("DBN Obligation").

Duty to conduct assessment of data breach

20.2 Once an organisation has credible grounds to believe that a data breach has occurred (whether through self-discovery, alert from the public or notification by its data intermediary), the organisation is required to take reasonable and expeditious steps to assess whether the data breach is notifiable under the PDPA.

20.3 Assessments should be done expeditiously as the likelihood of significant harm to affected individuals may increase with time. Any unreasonable delay in assessing a data breach will be a breach of the DBN Obligation and the Commission can take enforcement action.

20.4 While there may be varying circumstances that would affect the time taken to establish the facts of a data breach and determine whether it is notifiable, organisations should generally do so within 30 calendar days. If an organisation is unable to complete its assessment within 30 days, it would be prudent for the organisation to be prepared to provide the Commission an explanation for the time taken to carry out the assessment.

20.5 To demonstrate that it has taken reasonable and expeditious steps to assess whether the data breach is notifiable, the organisation must document all steps taken in assessing the data breach[56]. Please refer to paragraphs 20.38 – 20.45 on the information to be provided in notifications.

Data breaches within an organisation

20.6 A data breach that relates to the unauthorised access, collection, use, disclosure, copying or modification of personal data within an organisation is not a notifiable data breach. For example, where the HR department of an organisation mistakenly sends an email attachment containing personal data to another department within

[56] The organisation may be required to produce supporting documentation on the steps taken for its assessment of the data breach as part of its notification to the Commission, or for any investigation by the Commission of a suspected breach.

the same organisation that is not authorised to receive it, and the data breach is contained within the organisation, the data breach is not subject to the DBN Obligation.

Example: Misplaced storage drive

Sarah, a HR executive, misplaces an organisation-issued storage device containing the personal data and work evaluation reports of her company's staff and interns in her company's premises.

After a few days, the misplaced storage drive is found in her company's premises by another staff, Rachel. Sarah's company confirms that Rachel immediately returned the storage drive to the HR department upon finding it, and that no one accessed the storage drive while it was misplaced.

In this case, the DBN Obligation would not apply as it occurred within the organisation.

Data breaches discovered by a data intermediary

20.7 Where a data breach is discovered by a data intermediary that is processing personal data on behalf and for the purposes of another organisation or public agency, the data intermediary is required to notify the organisation or public agency without undue delay from the time it has credible grounds to believe that the data breach has occurred[57]. This ensures the organisation is (a) informed of data breaches in a timely way; (b) able to decide on the immediate actions to take to contain the data breach; and (c) able to assess whether the data breach is a notifiable data breach.

20.8 The DBN Obligation does not impose a requirement on the data intermediary to assess whether the data breach is notifiable, or to notify affected individuals and/or the Commission. The organisation that engaged the data intermediary remains responsible for doing so, even if it enlists the help of a data intermediary to conduct the assessment of the data breach or to notify the affected individuals and/or the Commission on its behalf.

20.9 As a good practice, organisations should establish clear procedures for complying with the DBN Obligation when entering into service agreements or contractual arrangements with their data intermediaries. These agreements take into consideration factors relating to the data processing, such as the volume and types of personal data involved, the type and extent of data processing, and the potential

[57] A data intermediary processing personal data on behalf of and for the purposes of a public agency must also notify the public agency of the occurrence of the data breach without undue delay if the data intermediary has reason to believe that a data breach has occurred in relation to that personal data.

harm that may result from a data breach[58].

Data breaches involving more than one organisation

20.10 In situations where a data breach involves personal data in the possession or under the control of more than one organisation, the organisations involved are individually responsible for complying with the DBN Obligation in respect of that data breach.

20.11 Organisations may agree that one of the organisations takes the lead in conducting the assessment to determine whether the breach is notifiable. Organisations have to draw its own conclusion from the assessment, and should accurately document and record the agreements, breach assessments and decisions.

20.12 Where a data breach is notifiable to the Commission, each organisation has to notify the Commission. As a matter of administrative convenience, organisations may use the same information where relevant to individually submit the notification. Where the data breach is notifiable to affected individuals, the Commission may provide further guidance to the organisations involved on managing the notification to affected individuals so that affected individuals only receive notifications and updates from a single source in respect of the notifiable data breach to minimise confusion.

Example: Data breach involving multiple organisations

As part of a business partnership, retailers ABC, DEF, and GHI establish a joint membership scheme where consumers can join as members to receive retail benefits.

A data breach involving the unauthorised disclosure of individuals' personal data and financial information is discovered when a member alerts ABC that she received an email containing the personal data of another member that was sent to her erroneously. The email contains the other member's purchasing history and the credit card details used for the payment of each purchase.

ABC obtains the agreement of all the organisations involved to take the lead in conducting the assessment of the data breach and share its findings and assessments with the rest. ABC determines that the data breach is notifiable. DEF and GHI come to their own conclusions and agree with ABC's assessment.

[58] The contractual clauses may include requirements around the communication of data incidents, processes for confirming a data breach, and responsibility for containing and remediating a data breach, where relevant.

The agreement, assessment and conclusions are documented and recorded by all the organisations involved.

ABC, DEF and GHI notify the Commission of the data breach in compliance with the DBN Obligation by each submitting a DBN through the breach notification portal, and attaching a common notification template to be used for the notification of the affected members.

The organisations, in consultation with the Commission, agree that ABC is best positioned to notify the affected members and provide further updates (if any), as it is the organisation with the closest and most direct relationship with the members.

Criteria for data breach notification

Significant harm to affected individuals

20.13 Organisations are required to assess whether a data breach is notifiable as it is likely to result in significant harm[59] to the affected individuals. Given the likelihood of harm arising from a data breach, notification ensures affected individuals are aware and able to take steps to protect themselves (e.g. change password, cancel credit card, monitor account for unusual activities).

20.14 To provide certainty to organisations on the data breaches that are notifiable, the Personal Data Protection (Notification of Data Breaches) Regulations 2021 provides the personal data (or classes of personal data) that is deemed to result in significant harm to affected individuals if compromised in a data breach. Where a data breach involves any of the prescribed personal data, the organisation will be required to notify the affected individuals and the Commission of the data breach.

20.15 The personal data (or classes of personal data) prescribed include:

a) Individual's **full name** or **alias**[60] or **full national identification number**[61] in combination with any of the following personal data in sub-paragraphs (i) to (xxv):

[59] Significant harm could include severe physical, psychological, economic and financial harm, and other forms of severe harms that a reasonable person would identify as a possible outcome of a data breach.

[60] Full name refers to the full name of the individual from official sources (e.g. NRIC/passport) that includes the individual's first and last name. It does not apply to the individual's initials. Alias refers to an alternate name an individual habitually uses to identify himself/herself and provided to/used by the organisation.

[61] National identification number refers to any government-issued identification number, including the NRIC number, birth certificate number, FIN, work permit number, passport number, and any foreign national identification number.

Financial information which is not publicly disclosed

(i) The amount of any wages, salary, fee, commission, bonus, gratuity, allowance or other remuneration paid or payable to the individual by any person[62], whether under a contract of service or a contract for services.

(ii) The income of the individual from the sale of any goods or property[63].

(iii) The number of any credit card, charge card or debit card issued to or in the name of the individual.

(iv) The number assigned to any account the individual has[64] with any organisation that is a bank or finance company.

(v) The net worth[65] of the individual.

(vi) The deposit of moneys by the individual with any organisation.

(vii) The withdrawal by the individual of moneys deposited with any organisation.

(viii) The granting by an organisation of advances, loans and other facilities by which the individual, being a customer of the organisation, has access to funds or financial guarantees.

(ix) The incurring by the organisation of any liabilities other than those mentioned in paragraph (viii) on behalf of the individual.

(x) The payment of any moneys, or transfer of any property[66], by any person[67] to the individual, including the amount of the moneys paid or the value of the property transferred, as the case may be. This includes payments of money or transfers of property to discharge (partially or fully) any debt owed to the individual, including a debt owed by the

[62] Any person refers to the individual's employer (where the individual is an employee under a contract of service) or the other party to a contract for services entered into with the individual, as the case may be. It is not limited to the organisation affected by the notifiable data breach.

[63] "Property" includes any thing in action and any interest in real or personal property.

[64] The loss of bank account details by any organisation (and not just by the bank or finance company itself) is deemed to result in significant harm to the individual.

[65] The "net worth" of an individual includes any of the following:

(a) the amount of any moneys, and value of any property, in which the individual has a legal or beneficial interest;

(b) the amount of any debts and other liabilities owed by the individual to any person.

[66] "Property" includes securities and units in unit trusts, as well as interests in real property (i.e. land and building).

[67] "Persons" includes the organisation affected by the data breach, and also includes another individual.

organisation concerned.

(xi) The creditworthiness of the individual. This includes the individual's loan/credit history, repayment/default history and credit rating/status, and includes credit reports prepared by a credit bureau (whether or not the credit bureau is licensed under other written law).

(xii) The individual's investment in any capital markets products[68].

(xiii) The existence, and amount due or outstanding, of any debt –

a. owed by the individual to an organisation[69]; or

b. owed by an organisation to the individual.

Identification of vulnerable individuals[70]

(xiv) Any information that identifies, or is likely to lead to the identification of, the individual as a child or young person[71] who –

a. is or had been the subject of any investigation under the Children's and Young Person's Act ("CYPA");

b. is or had been arrested, on or after 1 July 2020, for an offence committed under any written law;

c. is or had been taken into care or custody by the Director-General of Social Welfare, a protector, any officer generally or specially authorised in that behalf in writing by the Director-General or protector or a police officer under the CYPA;

d. is attending or had attended a family programme in relation to an application to be made under section 50 of the CYPA[72];

[68] "Capital markets products" as defined in the Securities and Futures Act ("SFA") includes securities (e.g. shares and bonds defined in the SFA) and unit trusts. "Investment in any capital markets product" includes any of the following:

(a) the nature, quantity and value of any capital markets products purchased or sold by the individual;

(b) the nature and value of any capital markets products held by or in the name of the individual.

[69] The organisation concerned need not be the organisation in possession or control of the personal data concerned.

[70] Examples include court-related documents or information (e.g. statement of facts/charge sheets), court orders (e.g. care and protection orders, Family Guidance orders, probation orders, Juvenile Rehabilitation Centre orders, orders in relation to vulnerable adults), family violence/child abuse history, details of incidents, family circumstances or conflicts.

[71] Child or young person means a person below the age of 18 years.

[72] Section 50 of the CYPA relates to the Power of Youth Court to make family guidance orders.

e. is or was the subject of an order made by a court under the CYPA; or

f. is or had been concerned in any proceeds in any court or on appeal from any court, whether the individual is the person against or in respect of whom the proceedings are taken or a witness in those proceedings.

(xv) Any information that identifies, or is likely to lead to the identification of –

a. an individual who has been or is the subject of any investigation, examination, assessment or treatment under the Vulnerable Adults Act ("VAA") relating to whether the individual is a vulnerable adult experiencing or at risk of abuse, neglect or self-neglect;

b. a vulnerable adult who has been committed to a place of temporary care and protection or place of safety designated under section 19(1) of the VAA or to the care of a fit person under the VAA;

c. a vulnerable adult who is the subject of an order made by a court under the VAA;

d. a place of temporary care and protection or place of safety designated under section 19(1) of the VAA in which an individual or a vulnerable adult mentioned in sub-paragraph a, b or c is committed, or the location of such a place of temporary care and protection or place of safety; or

e. a fit person under whose care an individual or a vulnerable adult mentioned in sub-paragraph a, b or c is placed, or the location of the premises of such a fit person.

(xvi) Any of the following –

a. the name or address of any woman or girl in respect of whom a specified offence[73] is alleged to have been committed;

b. any particulars given, in any proceedings in any court relating to

[73] "Specified offence" in sub-paragraph (xvi) means an offence under section 354, 354A, 375, 376, 376A, 376B, 376C, 376D, 376E, 376F, 376G or 377B of the Penal Code (Cap. 224), including an attempt to commit or cause the commission of any such offence; or an offence under Part XI of the Women's Charter (Cap. 353).

a specified offence, which identify, or are calculated to lead to the identification of, any woman or girl in respect of whom the specified offence is alleged to have been committed;

c. the name and address of any witness, in any proceedings in any court relating to a specified offence, which may lead to the identification of any woman or girl in respect of whom the specified offence is alleged to have been committed;

d. the particulars of any evidence given by any witness, in any proceedings in any court relating to a specified offence, which may lead to the identification of any woman or girl in respect of whom the specified offence is alleged to have been committed;

e. any picture of, or any picture including a picture of (i) any woman or girl in respect of whom a specified offence is alleged to have been committed; or (ii) any witness in any proceedings in any court relating to a specified offence.

(xvii) Any information that identifies, or is likely to lead to the identification of –

a. the individual as a resident of a place of safety established under section 177 of the Women's Charter (Cap. 353) ("WC"); or

b. the location of a place of safety established under section 177 of the WC at which the individual is residing.

Life, accident and health insurance information which is not publicly disclosed

(xviii) Any of the following –

a. the terms and conditions of any accident and health policy or life policy (called in this item the applicable policy) of which the individual is the policy owner or under which the individual is a beneficiary;

b. the premium payable by the policy owner under the applicable policy;

c. the benefits payable to any beneficiary under the applicable policy;

d. any information relating to any claim on, or payment under, the

applicable policy[74], including the condition of the health of any individual and the diagnosis, treatment, prevention or alleviation of any ailment, condition, disability, disease, disorder or injury that individual has suffered or is suffering from;

e. any other information that the individual is the policy owner of, or a beneficiary under, an applicable policy.

Specified medical information

(xix) The assessment, diagnosis, treatment, prevention or alleviation by a health professional[75] of any of the following affecting an individual –

a. any sexually-transmitted disease, such as Chlamydial Genital Infection, Gonorrhoea and Syphilis;

b. Human Immunodeficiency Virus ("HIV") Infection;

c. schizophrenia or delusional disorder;

d. substance abuse and addiction, including drug addiction and alcoholism.

(xx) The provision of treatment to an individual for or in respect of –

a. the donation or receipt of a human egg or human sperm; or

b. any contraceptive operation or procedure or abortion.

(xxi) Any of the following –

a. subject to section 4(4)(b) of the PDPA[76], the donation and removal of any organ from the body of the deceased individual for the purpose of its transplantation into the body of another individual;

b. the donation and removal of any specified organ from the individual, being a living organ donor, for the purpose of its

[74] To be clear, where the individual is a beneficiary under the policy, the triggering event may relate to another individual (e.g. the death of the insured person under a life policy).

[75] Health professional refers to a registered medical practitioner under the Medical Registration Act or a registered dentist under the Dental Registration Act.

[76] Section 4(4)(b) of the PDPA provides that the PDPA shall not apply in respect of personal data about a deceased individual, except that the provisions relating to the disclosure of personal data and section 24 (protection of personal data) shall apply in respect of personal data about an individual who has been dead for 10 years or fewer.

transplantation into the body of another individual;

c. the transplantation of any organ mentioned in sub-paragraph a or b into the body of the individual.

(xxii) Subject to section 4(4)(b) of the PDPA, the suicide or attempted suicide of the individual.

(xxiii) Domestic abuse, child abuse or sexual abuse involving or alleged to involve the individual.

Information related to adoption matters

(xxiv) Any of the following –

a. information that the individual is or had been adopted pursuant to an adoption order made under the Adoption of Children Act (Cap. 4), or is or had been the subject of an application for an adoption order;

b. the identity of the natural father or mother of the individual;

c. the identity of the adoptive father or mother of the individual;

d. the identity of any applicant for an adoption order;

e. the identity of any person whose consent is necessary under that Act for an adoption order to be made, whether or not the court has dispensed with the consent of that person in accordance with that Act;

f. any other information that the individual is or had been an adopted child or relating to the adoption of the individual.

Private key used to authenticate or sign an electronic record or transaction

(xxv) Any private key that is used or may be used –

a. to create a secure electronic record or secure electronic signature;

b. to verify the integrity of a secure electronic record; or

c. to verify the authenticity or integrity of a secure electronic signature.

Individual's account identifier and data for access into the account (without individual's name, alias or full identification number)

b) Personal data relating to an individual's account (both active and dormant) with an organisation, including –

(i) the individual's account identifier, such as an account name or number or a username; and

(ii) any password, security code, access code, response to a security question, biometric data or other data that is used or required to allow access to or use of the individual's account.

20.16 The prescribed personal data or classes of personal data, or other prescribed circumstances excludes any personal data that is publicly available[77] and any personal data that is disclosed under any written law (e.g. pay information issued by employers under the Employment Act).

Example: Unauthorised access of patients' medical records

The database administrator of a medical clinic discovers an unauthorised access of some of its patients' medical records. The medical clinic immediately assesses the data breach, including the number of patients' records and the types of data affected. The medical clinic determines that the data breach involves medical records including personal data such as patients' full NRIC numbers, and diagnosis and treatment of sexually-transmitted diseases. The medical records of approximately 50 patients are affected.

The data breach is assessed to be notifiable as it involves individuals' full national identification numbers and their diagnosis and treatment of sexually-transmitted diseases, and these are deemed to likely result in significant harm to the affected individuals. The medical clinic is required to notify the Commission and the affected individuals of the data breach.

Example: Theft of portable storage drive containing hotel guests' details

A portable storage drive containing the details of approximately 1,000 guests of a hotel chain is stolen. The drive includes personal data of guests such as their full names, passport details, flight information, durations of stay with the hotel chain, and credit card details.

[77] To be clear, the personal data must not be publicly available solely because of any data breach.

The data breach is assessed to be notifiable as it involves guests' full national identification numbers and credit card details, and these are deemed to likely result in significant harm to the affected individuals. The hotel chain must notify the Commission and the affected individuals of the data breach.

20.17 Where different categories of personal data are lost or compromised at different times, the affected organisation must notify the Commission and/or affected individuals if the organisation assesses that the different data breaches are likely to be linked. This may be based on whether the same perpetrator is involved or based on the surrounding circumstances of the data breaches.

20.18 For example, where there are two data breaches which occur at different times, but a combined database containing both sets of personal data subsequently discovered online. In such instances, the affected organisation must notify the Commission and/or affected individuals if it learns that a third party (who may or may not be implicated in the data breach) has combined the different sets of compromised personal data and disclosed or used the combined set of personal data.

Example: Where combination of compromised personal data from different data breaches meets the requirement for notification

The database administrator of a voluntary welfare organisation ABC discovers an unauthorised access of some of its customers' full name and contact details.

As the data breach only involves customers' full name and contact details, the data breach is deemed to be unlikely to result in significant harm to an individual and organisation need not notify the affected students of the data breach.

Six months later, ABC discovers that the same set of customers' full name, contact details had been posted on an online forum together with their confidential financial information.

ABC notifies the Commission and affected individuals of the data breaches as the combination of compromised personal data (i.e. customers' full name and financial information) meets the requirement for notification.

Significant scale of breach

20.19 Data breaches of a significant scale may indicate a systemic issue within the organisation. Notifying the Commission of such data breaches will allow it to provide guidance to organisations on remedial actions to address the data breach as well as any systemic changes to prevent future occurrences.

20.20 Data breaches that meet the criteria of significant scale are those that involve the personal data of 500 or more individuals. Where a data breach affects 500 or more individuals, the organisation is required to notify the Commission, even if the data breach does not involve any prescribed personal data in paragraph 20.15.

20.21 If an organisation is unable to determine the actual number of affected individuals in a data breach, the organisation should notify the Commission when it has reason to believe that the number of affected individuals is at least 500. This may be based on the estimated number from a preliminary assessment of the data breach. The organisation may subsequently update the Commission of the actual number of affected individuals when it is established.

Example: Unauthorised access to database containing customers' profiles

The IT administrator of online retail store discovers an unauthorised access to its customers' database. The database contained customers' names, membership numbers, contact information and their current balance of loyalty points and dates of their expiry.

The online retail store is unable to determine the exact number of individuals whose personal data is affected in the data breach at the outset. Nevertheless, as the affected database contains the personal data of 700 customers, the online retail store proceeds to notify the Commission of the data breach. Subsequently, the online retail store determines the exact number of customers whose personal data is compromised and provides the updated information to the Commission.

As the data breach does not involve any of the prescribed personal data, the data breach is deemed to be unlikely to result in significant harm to an individual and the online retail store would not be required under the DBN Obligation to notify the affected customers of the data breach.

Example: Disclosure of 250 students' library loan history

A private education institution discovers an unauthorised disclosure of its students' library loan records. The data breach involves the personal data of 250 students, including their full names, student matriculation numbers and library loan histories for the past one year.

As the data breach does not involve any of the prescribed personal data, the data breach is deemed to be unlikely to result in significant harm to an individual and the private education institution need not notify the affected students of the data breach. In addition, as the scale of the data breach is not

significant (i.e. fewer than 500 affected students), the private education institution need not notify the Commission of the data breach.

Example: Loss of document containing personal data of 10 cyclists

A member of cycling interest group misplaced a document containing the cycling route of a previous cycling expedition and names of the 10 cyclists involved in the expedition.

As the data breach does not involve any of the prescribed personal data, and the data breach is not of a significant scale (i.e. fewer than 500 affected individuals), the cycling interest group need not notify the affected cyclists nor the Commission of the data breach.

Timeframes for notification

20.22 Upon determining that a data breach is notifiable, the organisation must notify:

a) the Commission as soon as practicable, but in any case, no later than three (3) calendar days[78]; and

b) where required, affected individuals as soon as practicable, at the same time or after notifying the Commission.

20.23 These timeframes for notifying the Commission and/or the affected individuals commences from the time the organisation determines that the data breach is notifiable. Any unreasonable delays in notifying the relevant parties will be a breach of the DBN Obligation.

20.24 Prescribing a cap of three (3) calendar days provides clarity for organisations as to the definitive time by which they will have to notify the Commission by.

20.25 Where an organisation is required to notify affected individuals of a data breach, it should notify the affected individuals at the same time or after it notifies the Commission.

Exceptions from the requirement to notify affected individuals

20.26 Section 26D of the PDPA provides for exceptions to the requirement to notify affected individuals of a notifiable data breach in certain circumstances.

[78] The first day of the three days starts on the day after the organisation makes the determination that there is a notifiable breach. To illustrate, if an organisation determines on 1st January that a data breach is notifiable, it must notify the Commission by 4th January.

20.27 **Where an exception applies** to a data breach that is likely to have significant harm to the affected individuals, the organisation need not notify the affected individuals, but it is still required to notify the Commission of the data breach. In the event that the Commission determines that the exception does not apply, the organisation would be required to notify the affected individuals of the data breach.

Remedial action

20.28 An organisation may rely on the remedial action exception if timely remedial actions have been taken by the organisation or its data intermediary, in accordance with any prescribed requirements, that renders it unlikely that the data breach will result in significant harm to the affected individual.

20.29 Such remedial actions need not necessarily be taken before notifying the Commission. Remedial actions (or further remedial actions) may also be taken after notifying the Commission and receiving guidance from the Commission. In the event that, after notifying the Commission, the organisation applies further remedial actions such that the data breach is no longer likely to have significant harm to the individuals, the organisation may rely on the exception not to notify the individuals concerned.

Example: Disclosure of an email attachment containing the personal data of 1,000 customers

A travel agency has a panel of vendors that processes its payments. An email attachment containing the personal data of 1,000 customers of the travel agency is sent to the wrong vendor by accident. The attachment includes full names, credit card details and passport numbers.

The employee who sent the email immediately contacts the receiving vendor, which confirms that the attachment has not been accessed and that it has permanently deleted the email with the attachment.

The travel agency assesses that it may rely on the remedial action exception as it has taken reasonable measures to address the data breach such that it is not likely to result in significant harm to the affected individuals.

However, the travel agency is still required to notify the Commission of the data breach according to the requirements under the DBN Obligation as the data breach involves more than 500 individuals, including their financial information and national identification numbers.

Technological protection

20.30 Where there are appropriate technological measures applied to the personal data (e.g. encryption, password-protection, etc) before the data breach which renders the personal data inaccessible or unintelligible to an unauthorised party, the exception for technological protection applies. In such cases, the organisation need not notify the affected individuals of the data breach.

20.31 In assessing whether the technological protection measures taken are sufficient for the technological protection exception to apply, organisations should take into consideration whether the technological protection is of a commercially reasonable standard and the prevailing industry practices in the sector. Organisations can also consider the availability and affordability of the options in determining what are reasonable technological protection measures.

Example: Loss of encrypted storage drive

A HR director misplaces an encrypted storage drive containing 200 employees' medical insurance details of his company such as employees' full names, medical schemes, past medical claims, and remaining claims balance.

The HR director's company assesses that the technological protection exception applies, as the encryption standard (AES 256-bit) in the storage drive is of a reasonable standard when the loss occurred and that any unauthorised access to the encrypted data of the misplaced storage drive is unlikely. As such, the company need not notify the affected employees of the data breach.

However, as the personal data involved includes employees' financial information, the company must notify the Commission of the data breach.

Example: Loss of laptop containing health information

Pharmaceutical research laboratory maintains a list of patients undergoing fertility treatment. The list contains personal data of 1,000 patients, including their full names, medical histories and treatment details. Only researchers who deal with these patients are given access to the list. The list is stored in the pharmaceutical research laboratory's intranet and can also be accessed with the correct credentials through authorised laptops. There are three layers of security measures put in place for accessing these laptops – (i) BIOS password; (ii) BitLocker; and (iii) Windows password. One of their researchers loses his authorised laptop.

The pharmaceutical research laboratory assesses that the technological protection exception applies, as it is unlikely that a third party could overcome the three layers of protection measures put in place to access the list via the

lost laptop. In addition, the credentials of the researcher are not stored on the laptop.

However, as the personal data involved includes individuals' health information (including their fertility treatment), and the number of potentially affected individuals is more than 500, the pharmaceutical research laboratory must notify the Commission of the data breach.

Notification allows the Commission to assess whether there is any systemic issue within the organisation, for example, lapse in security arrangements leading to higher risk of similar incidents occurring. The Commission can advise the organisation on taking preventive measures to lower the risk of similar incidents.

Prohibition and waiver of the requirement to notify affected individuals

20.32 Organisations are prohibited from notifying the affected individuals if a prescribed law enforcement agency so instructs them. This is to cater to situations where the breach is the subject of an ongoing or potential investigation by a law enforcement agency and notifying the affected individuals will compromise investigations or prejudice enforcement efforts under the law. Organisations are also prohibited from notifying the affected individuals if the Commission so directs them.

20.33 In addition, the Commission may, on the written application of an organisation, waive the requirement for an organisation to notify affected individuals in exceptional circumstances where notification to affected individuals may not be desirable. This includes circumstances where there are overriding national security or national interests, or there are ongoing investigations by an agency authorised by law[79] where such investigations are not publicly known.

20.34 In deciding whether to grant a waiver, the Commission will have regard to advice from the relevant law enforcement agency or public agency. For instance, a law enforcement agency may prohibit an organisation from notifying affected individuals for a period of time to avoid compromising an investigation. A law enforcement agency may also delay an organisation's notification if the notification would likely lead to further data breaches, should vulnerabilities in an organisation's IT security system become publicly known before it could be rectified.

Mode of notification of data breach

20.35 Where organisations are required to notify affected individuals of a data breach, they should ensure that the mode of notification used is appropriate and effective in

[79] Including investigations conducted by an organisation to discharge obligations under the law.

reaching the affected individuals in a timely way. Organisations may employ their regular mode of communication with the affected individuals to send the notification.

20.36 Where there is no regular mode of communication with the affected individuals, the organisation should determine the most appropriate mode of notification to reach out to the affected individuals. As there are many different modes of notification that could evolve with technology, organisations may determine the most efficient and effective mode of notification to inform affected individuals.

Example: Disposal of client's personal data

An employee of a voluntary welfare organisation discovers that case documents containing their ex-clients' financial, medical and family history are disposed of in an unsecured manner instead of being shredded as per the voluntary welfare organisation's data retention policy. However, the voluntary welfare organisation is not able to ascertain the scale of the data breach as the documents were sold to a 'rag-and-bone' man.

The data breach is assessed to pose a significant harm to the affected individuals, as the compromised personal data includes confidential financial information, amongst other types of personal data. As such, the voluntary welfare organisation should notify the Commission and the affected individuals of the data breach.

The voluntary welfare organisation should also assess the mode and manner of notifying the affected individuals that would best serve the interest of the affected individuals. As the affected individuals could be significantly distressed given the sensitivity of the personal data breached, the voluntary welfare organisation decides to notify the affected individuals through personal phone calls by trained personnel to address any immediate questions and allay their concerns.

Information to be provided in notification of data breach

20.37 An organisation notifying affected individuals and/or the Commission of a notifiable data breach is required to provide relevant details of the data breach to the best of its knowledge and belief. The notification should also include relevant information about the organisation's data breach management and remediation plans. Please refer to the Personal Data Protection (Notification of Data Breaches) Regulations 2021 for more information. Organisations may provide their notification on the

Commission's website[80].

Notification to the Commission

20.38 To ensure proactive steps are taken by the organisation to manage and remediate the data breach, information to be provided in the organisation's notification to the Commission shall include:

a) **Facts of the data breach**

(i) the date on which and the circumstances in which the organisation first became aware that a data breach has occurred;
(ii) information on how the notifiable data breach occurred;
(iii) the number of affected individuals affected by the notifiable data breach;
(iv) the personal data or classes of personal data affected by the notifiable data breach; and
(v) the potential harm to the affected individuals as a result of the notifiable data breach.

b) **Data breach handling**

(i) A chronological account of the steps taken by the organisation after the organisation became aware that the data breach had occurred, including the organisation's assessment under section 26C(2) or (3)(b) of the PDPA that the data breach is a notifiable data breach;
(ii) information on any action by the organisation, whether taken before or to be taken after the organisation notifies the Commission of the occurrence of the notifiable data breach –
  (a) to eliminate or mitigate any potential harm to any affected individual as a result of the notifiable data breach; and
  (b) to address or remedy any failure or shortcoming that the organisation believes to have caused, or have enabled or facilitated the occurrence of, the notifiable data breach; and
(iii) information on the organisation's plan (if any) to inform all or any affected individuals or the public that the notifiable data breach has occurred and how an affected individual may eliminate or mitigate any potential harm as a result of the notifiable data breach. The organisation may provide in general terms the steps taken or intended to be taken.

[80] Submit the notification at https://eservice.pdpc.gov.sg/case/db. For urgent notification of major cases, organisations may also contact the PDPC at +65 6377 3131 during working hours.

c) **Contact details**

(i) Contact details of at least one authorised representative of the organisation. The representative(s) need not be the organisation's DPO (or a person assuming the DPO's responsibilities in the organisation).

20.39 Where the data breach notification to the Commission is not made within three (3) calendar days of ascertaining that it is a notifiable breach, the organisation must also specify the reasons for the late notification and include any supporting evidence. The reasons for the late notification will go toward the gravity of the organisation's contravention of the DBN Obligation and consequently the nature and severity of the penalties imposed on the organisation, if any.

20.40 Where the organisation does not intend to notify any affected individual, the notification to the Commission must additionally specify the grounds (whether under the PDPA or other written law[81]) for not notifying the affected individual.

20.41 Any application to the Commission to waive the requirement to notify an affected individual under section 26D(7) of the PDPA may be submitted together with the notification to the Commission. For more information on waivers of requirement to notify affected individuals, refer to paragraphs 20.32 – 20.34.

Notification to affected individuals

20.42 Notification to affected individuals should be clear and easily understood. It should include guidance on the steps affected individuals may take to protect themselves from the potential harm arising from the data breach. Where appropriate, organisations should notify parents or guardians of young children whose personal data has been compromised.

20.43 Where the data breach involves information related to adoption matters or the identification of vulnerable individuals, organisations should first notify the Commission for guidance on notifying affected individuals.

20.44 Organisations are not required to provide to the Commission the notification to be sent to affected individuals. Organisations should include the following information in their notifications to affected individuals:

a) **Facts of the data breach**

(i) the circumstances in which the organisation first became aware that a notifiable data breach has occurred; and

[81] For instance, in reliance on any application exceptions in section 26D(5) or (6)(a) of the PDPA, or any prohibition or restriction under other written law.

(ii) the personal data or classes of personal data relating to the affected individual affected by the notifiable data breach.

b) **Data breach management and remediation plan**

(i) Potential harm to the affected individual as a result of the notifiable data breach;
(ii) Information on any action by the organisation, whether taken before or to be taken after the organisation notifies the affected individual –
  (a) To eliminate or mitigate any potential harm to the affected individual as a result of the notifiable data breach;
  (b) To address or remedy any failure or shortcoming that the organisation believes to have caused, or have enabled or facilitated the occurrence of, the notifiable data breach; and
(iii) Steps that the affected individual may take to eliminate or mitigate any potential harm as a result of the notifiable data breach, including preventing the misuse of the affected individual's personal data affected by the notifiable data breach.

c) **Contact details**

(i) Contact details of at least one authorised representative whom the affected individual can contact for further information or assistance. The representative(s) need not be the organisation's DPO (or a person assuming the DPO's responsibilities in the organisation), or the same representative provided in the organisation's notification to the Commission.

20.45 Organisations may customise their notification to affected individuals, as long as it includes the required content. In addition, decision on the appropriate actions that the individual may take is dependent on the circumstances of the data breach. This may include choosing to tailor the recommended protective actions that individuals could take depending on the individual's circumstances or providing general recommendations that apply to all affected individuals.

Notification to other regulators

20.46 Where an organisation is required to notify a sectoral regulator or law enforcement agency of a data breach under other written laws, the organisation must notify that sectoral regulator or law enforcement agency accordingly. Additionally, it must also notify the Commission and affected individuals (if required) according to the timeframes for data breach notification under the PDPA. An organisation is not regarded to have fulfilled the DBN Obligation under the PDPA just by fulfilling any other breach notification requirements set out under other written laws.

21 The Accountability Obligation[82]

21.1 In data protection, the concept of accountability refers to how an organisation discharges its responsibility for personal data in its possession or which it has control over[83]. 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 in Part 3 of the PDPA on "General Rules with Respect to Protection of and Accountability for Personal Data" and premised on section 11(2) within Part 3 of the PDPA, which states, "An organisation is responsible for personal data in its possession or under its control.".

21.2 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 paragraph 21.15 are not mandatory but are good practices to help organisations in meeting their obligations under the PDPA.

Appointing a Data Protection Officer

21.3 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 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, they co-operate to ensure that

[82] 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.

[83] For more information on accountability, please refer to www.pdpc.gov.sg/help-and-resources/2021/09/accountability.

the organisation complies with the PDPA.

21.4 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.

21.5 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[84]. 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.

21.6 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(5)(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.[85] These individuals and persons may be the same individual or the organisation may have different persons undertaking such roles.

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

[85] 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.

21.7 The business contact information of the relevant person may be provided on BizFile+ for companies that are registered with ACRA, or provided in a readily accessible part of the organisation's official website[86] such that it can be easily found. It 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

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

21.9 Firstly, an organisation is required to develop and implement data protection policies and practices to meet its obligations under the PDPA[87]. Policies can be internal or external facing; and practices can include establishing governance structures and designing processes to operationalise policies. Organisations should develop policies and practices by taking into account matters such as the types and amount of personal data it collects, and the purposes for such collection[88]. This also entails ensuring that policies and practices are easily accessible to the intended reader. Furthermore, the organisation should put in place monitoring mechanisms and process controls to ensure the effective implementation of these policies and practices.

21.10 Secondly, an organisation must develop a process to receive and respond to complaints that may arise with respect to the application of the PDPA[89]. 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.

21.11 Thirdly, an organisation is required to provide staff training and communicate to its staff information about its policies and practices[90]. 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 and awareness programme builds a staff culture that

[86] See Part 1A of the Personal Data Protection Regulations 2021.
[87] See section 12(a) of the PDPA.
[88] See paragraph 21.15 for other measures an organisation may wish to adopt when developing its data protection policies and practices.
[89] See section 12(b) of the PDPA.
[90] See section 12(c) of the PDPA.

is sensitive and alert to data protection issues and concerns.

21.12 Finally, an organisation is required to make information available on request concerning its data protection policies and practices and its complaint process[91]. 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.

21.13 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. Please refer to the Commission's website for resources on demonstrating organisational accountability.

Other provisions related to the Accountability Obligation

21.14 The Data Protection Provisions also provide for specific circumstances where organisations have to be answerable to individuals and the Commission, 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) organisations have to notify the Commission and/or affected individuals when a data breach is likely to result in significant harm or is of a significant scale;

c) organisations have to conduct risk assessments to identify and mitigate adverse effects for certain uses of personal data such as for legitimate interests;

d) individuals may submit a complaint to the Commission and the Commission may review or investigate an organisation's conduct and compliance with the PDPA[92];

e) 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

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

[92] Sections 48H, 48I and 48J of the PDPA specify what the PDPA may do upon a review or investigation respectively.

$1 million (or in due course, up to $1 million or 10% of the organisation's annual turnover in Singapore, whichever is higher); and

f) individuals who suffer loss or damage directly as a result of a contravention of Parts 4, 5, 6 or 6A of the PDPA by an organisation may commence civil proceedings against the organisation[93].

Other measures relating to accountability

21.15 Although not expressly provided for in the PDPA, organisations may wish to consider demonstrating organisational accountability through measures such as conducting Data Protection Impact Assessments ("DPIA") in appropriate circumstances, adopting a Data Protection by Design ("DPbD") approach, or implementing a Data Protection Management Programme ("DPMP"), to ensure that their handling of personal data is in compliance with the PDPA[94]. 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.

[93] Parts 4, 5, 6 and 6A of the PDPA relate respectively to (a) collection, use and disclosure of personal data; (b) access to and correction of personal data; (c) care of personal data (containing provisions relating accuracy, protection, retention and transfer of personal data); and (d) notification of data breaches.

[94] For more information, please refer to the Guide to Data Protection Impact Assessments, Guide to Data Protection by Design for ICT Systems, Guide to Managing Data Intermediaries under the PDPA and Guide to Developing a Data Protection Management Programme on the PDPC's website.

PART IV: OFFENCES AFFECTING PERSONAL DATA AND ANONYMISED INFORMATION

22 Overview

22.1 Offences under Part 9B of the PDPA hold individuals accountable for egregious mishandling of personal data in the possession of or under the control of an organisation (including a public agency). The offences are for:

a) Knowing or reckless unauthorised disclosure of personal data;

b) Knowing or reckless unauthorised use of personal data for a gain for the individual or another person, or to cause a harm or a loss to another person; and

c) Knowing or reckless unauthorised re-identification of anonymised information.

23 Offences for egregious mishandling of personal data

23.1 These offences do not detract from the policy position to hold organisations primarily accountable for data protection. Organisations remain liable for the actions of their employees in the course of their employment with the organisations[95]. These offences are to criminalise egregious misconduct by individuals whose actions had not been authorised by the organisation. To be clear, circumstances where the conduct is in the nature of a private dispute are not intended to be the subject of criminal prosecutions under these offences. Examples of private disputes include, disputes over ex-employees taking an organisation's customer list when joining a competitor or setting up a competing business, where the ex-employee obtained the consent of the customers to do so.

Authorisation

23.2 These offences are not intended to cover instances where the individuals are authorised to disclose, use or re-identify the data. Authorisation may take different forms: it may be found in an organisation's written polices, manuals and handbooks, or an organisation may provide ad-hoc authorisation for a specific action or activity (which could be verbal or in writing). Authorisation should be provided by someone in the organisation who is empowered to do so or who is ostensibly empowered to do so by reason of his seniority or position in the organisation. Below are instances where individuals are considered to be acting under authorisation:

a) **Employees** acting in the course of their employment (including volunteers), in accordance with their employers' policies and practices, or whose actions are authorised by their employers. Employees should be assured that if they adhere to their employer's policies and practices, they will not run the risk of criminal sanctions for these offences.

b) **Service providers** engaged and authorised by organisations through service contracts or written agreements to carry out the disclosure, use or re-identification of data.

Applicable defences

23.3 The PDPA provides for the following defences for these offences:

a) **The information is publicly available and where that information was publicly available solely because of an applicable contravention, the accused did not know, and was not reckless as to whether, that was the case**. This defence is intended to only cover personal data that is already in

[95] Refer to section 53 of the PDPA.

the public domain. For example, a dataset contains identity information (e.g. name, photo, email address) and other personal data (e.g. financial data). An individual will not be able to rely on this defence where the affected person's *identity information* is publicly available (e.g. on social media) but where other *re-identified personal data* of the affected person in the dataset is not publicly available;

b) **Where the conduct is permitted or required under other laws**;

c) **Where the conduct is authorised or required by an order of the court**; and

d) **Where the individual reasonably believes that he had the legal right to do so**. This defence covers situations such as journalistic reporting and whistleblowing.

23.4 Part 4A of the Personal Data Protection Regulations 2021 additionally provides defences for the offences in paragraphs 22.1(a) and (b) above relating to the knowing or reckless unauthorised disclosure and use of personal data[96]. The defences cover situations where **consent has been provided by the individual to whom the personal data relates**. For example, a relationship manager who obtains consent from his clients to continue to use and disclose their personal data when he moves to another company; a professional who brought in his clients when he joined a partnership and brings them along when he moves to another partnership; or an account manager who brings the customers he had worked with from his previous company to his new employment where he has obtained the customers' consent to do so. In these situations, while there may be a dispute over whether the relationship manager, professional or account manager has the legal right to do so, the dispute is in the nature of a private civil dispute and not a criminal offence.

Re-identification of anonymised information

23.5 For the offence outlined in paragraph 22.1(c) of knowing or reckless unauthorised re-identification of anonymised information, additional defences are provided for the following circumstances:

a) **Testing the effectiveness of the anonymisation of personal data in the possession or under the control of an organisation or public agency, as the case may be**;

b) **Testing the integrity and confidentiality of anonymised information in the**

[96] A similar defence is not provided for the offence outlined in paragraph 22.1(c) of knowing or reckless unauthorised re-identification of anonymised information. To be clear, the re-identification of anonymised information with the authorisation of the organisation is not an offence.

possession or under the control of an organisation or public agency; *and*

c) **Assessing, testing or evaluating the systems and processes of an organisation or public agency for ensuring or safeguarding the integrity and confidentiality of anonymised information in the possession or under the control of the organisation, or transmitted or received by the organisation or public agency**.

23.6 As such, these additional defences may be applicable to the following individuals:

a) **Data Professionals**. Cybersecurity specialists, data scientists, AI engineers and statisticians in the information security and encryption industry, whose work involves the re-identification of anonymised data in order to carry out research and development or to test the robustness of their organisations' information security products and service, or their clients' information security systems.

b) **Service providers** engaged and authorised by organisations to recover data from anonymised dataset (e.g. dataset anonymised by a former employee in the course of work but who has since left and none of the current employees have the decryption key) or to carry out security testing activities, including re-identifying anonymised datasets to test whether anonymisation employed is robust.

c) **Researchers, teachers and academics** who need to re-identify anonymised data as part of their research work or for teaching on anonymisation and encryption.

d) **White-hat hackers** who independently carry out effectiveness testing of organisations' information security systems either in their personal capacity or as part of bug bounty programmes.

PART V: OTHER RIGHTS, OBLIGATIONS AND USES

24 Overview

24.1 The Data Protection Provisions first came into operation on 2 July 2014, a date specified by the Minister, and referred to 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.

24.2 Since the Data Protection Provisions took effect, 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.

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

25 Rights and obligations, etc. under other laws

25.1 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.

25.2 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.

25.3 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[97].

25.4 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

[97] 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.

26 Use of personal data collected before 2 July 2014

26.1 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 4 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.

26.2 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.

26.3 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.

26.4 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 9 and 9A of the PDPA (which apply concurrently with the Data Protection Provisions). Before sending a specified message to a Singapore telephone number, the organisation must check with the Do Not Call Registry to confirm that the number is not listed on a Do Not Call Register, unless it has obtained "clear and unambiguous consent" in evidential form from the individual to the sending of the message. Please see the Advisory Guidelines on the Do Not Call Provisions for more information.

26.5 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 4 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.

26.6 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