PERSONAL DATA
PROTECTION COMMISSION
SINGAPORE

ADVISORY GUIDELINES FOR THE SOCIAL SERVICE SECTOR

Issued 11 September 2014
Revised 18 January 2024

Supported by:

INFOCOMM MEDIA DEVELOPMENT AUTHORITY

In support of:

SG:DIGITAL

TABLE OF CONTENTS

PART I: INTRODUCTION

1 Introduction

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

1.2 Developed in consultation with the National Council of Social Service ("NCSS"), these Guidelines aim to address the unique circumstances faced by social service agencies ("SSAs") in complying with the PDPA. Social service agencies are non-profit organisations that provide services to benefit the community. They are typically set up as societies, companies limited by guarantee, or trust.

1.3 Section 4(1)(c) of the PDPA provides that the Data Protection Provisions[1] shall not impose any obligation on any public agency. Public agencies include the Government and specified statutory bodies, including the NCSS. These Guidelines have been updated to reflect the changes to the PDPA in 2021, where organisations in the course of collecting, using or disclosing personal data on behalf of a public agency will need to comply with the PDPA.

1.4 These Guidelines indicate the manner in which the Commission will interpret certain provisions of the PDPA in relation to some examples. As with all Guidelines issued by the Commission, these Guidelines are not meant to be an exhaustive representation of the circumstances faced by the social service sector and do not prescribe how organisations may wish to ensure compliance with the PDPA.

1.5 Some examples in this document refer to figures (e.g. 14-day opt out period for withdrawal of consent), which are purely for illustrative purposes and not prescribed by the PDPC.

[1] As defined in the document titled "Introduction to the Guidelines", "Data Protection Provisions" refer to the PDPA's data protection obligations set out in Parts 3 to 6A of the PDPA.

2 Important terms used in the PDPA

Volunteers

2.1 Pursuant to section 4(1)(b) of the PDPA, employees who are acting in the course of their employment with an organisation 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.

2.2 Notwithstanding this exclusion for employees, SSAs remain primarily responsible for the actions of the employees (including volunteers) which result in a contravention of the Data Protection Provisions, provided the employees/volunteers are acting in the course of their employment.

2.3 Under the Accountability Obligation of the PDPA, SSAs are required to develop and implement policies and practices that are necessary for the SSAs to meet its obligations under the PDPA. SSAs are required to communicate to their employees (including volunteers) information about the SSA's policies and practices.

2.4 For more information on employees and employment, please refer to Chapter 6 of the Key Concepts Guidelines relating to employees and Chapter 6 of the Selected Topics Guidelines on employment.

PART II: APPLICATION OF THE DATA PROTECTION PROVISIONS TO THE SOCIAL SERVICE SECTOR

Please note that the following section and examples do not illustrate the application of the Do Not Call Provisions, which are addressed later in these Guidelines.

3 The Consent, Purpose Limitation and Notification Obligations

3.1 The Commission understands that SSAs may collect, use or disclose a client's personal data including full name, NRIC number, contact details, financial and family situation, medical history, etc. for purposes such as evaluating the client's suitability for social services or administering social services to the clients.

3.2 The PDPA requires organisations to, among other things, notify an individual of the purposes for the collection, use and disclosure of his personal data[2] and obtain his consent, unless any relevant exception to consent[3] applies. Moreover, organisations shall only collect, use and disclose personal data that are relevant for the purposes, and for purposes that a reasonable person would consider appropriate in the circumstances.

3.3 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. Please refer to the Advisory Guidelines on Key Concepts in the PDPA (Chapter 12) for the requirements that must be complied with by either the individual or the organisation in relation to the withdrawal of consent. However, the organisation can continue to use and disclose personal data in their possession if allowed under other provisions.

---

[2] 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". While some data may necessarily relate to an individual, other data may not, on its own, relate to an individual. Such data would not constitute personal data unless it is associated with, or made to relate to, a particular individual. Generic information that does not relate to a particular individual may also form part of an individual's personal data when combined with personal data or other information to enable an individual to be identified.

[3] Please refer to the First (collection, use and disclosure of personal data without consent) and Second (additional bases for collection, use and disclosure of personal data without consent) Schedules under the PDPA for any exceptions which may apply.

3.4 The Commission is aware that, depending on the nature of their services and demographics of the client or beneficiary, some SSAs may collect, use or disclose the personal data of minors and would accordingly have to obtain consent under the PDPA. Please refer to the Advisory Guidelines on Selected Topics ("Selected Topics Guidelines") on "data activities relating to minors" for more information relating to persons who may exercise rights or powers under the PDPA, and considerations when obtaining consent from minors.

3.5 The following will highlight how consent may apply in common social service scenarios, how deemed consent applies as well as the exceptions to consent.

3.6	**Examples: Using personal data** SSA ABC arranges with Company XYZ such that the purpose and amount needed for donations to SSA ABC are listed on Company XYZ's public website. Company XYZ has a database of regular donors to whom it sends emails to solicit donations on a periodic basis. The donors could choose to donate to SSA ABC by referring to the instructions on Company XYZ's website and provide their financial information to Company XYZ for processing of the transaction. Before proceeding, donors will indicate their consent to disclosing their personal data to SSA ABC when they donate through Company XYZ for purposes such as issuing tax deductible receipts to their email address. **<u>Treatment</u>** In processing the financial transaction from donors on its website, Company XYZ is considered to have collected, used and disclosed personal data. By receiving personal data of donors from Company XYZ, SSA ABC is considered to have collected and subsequently used the personal data. Accordingly, Company XYZ and SSA ABC will have to comply with the PDPA in respect of such collection, use and disclosure.
3.7	SSA DEF engages Company GHI for online on its upcoming programmes and events as sponsored social media posts. No individuals' personal data is given to Company GHI for generating the social media posts. The posts appear in the social media feed of users in a random manner.

	Treatment In this case, neither SSA DEF nor Company GHI would be considered to have collected or used the personal data of the users. Hence, both SSA DEF and Company GHI would not be subject to the Data Protection Provisions for this set of activities.

3.8	**Example: Clients voluntarily giving their personal data for welfare services** Seniors' activity centre ABC gives out free food items to senior citizens by leaving them at the door of the activity centre for self-collection by the senior citizens. There is a notice pasted at the door of the activity centre indicating that the seniors can leave their contact details if they are interested to be contacted for seniors' programmes, free or subsidized healthcare or financial support. To ensure that the personal data of the interested seniors are not shown to the public, interested seniors will fill in their names and contact details in a blank form placed at the door of the activity centre. They will drop the completed form inside a metal box that can only be accessed when the appropriate personnel from Seniors' activity centre ABC uses a key to open the lock on the box. On the form, there is a question clearly asking the seniors' consent for collection, use and disclosure of their personal data for the specific purpose and a checkbox beside the question for seniors to tick. **Treatment** If the senior citizen were to fill in their names and contact details in the blank form and indicated at the checkbox that they consent to the collection, use and disclosure of their personal data for the specified purpose, Seniors' activity centre ABC has obtained express consent from the interested seniors. The consent is obtained in writing and provides the clearest indication that the individual has consented to the notified purposes of the collection, use or disclosure of their personal data. Seniors' activity centre ABC must ensure that the words on the notice and on the form are clear and noticeable, so that there is a higher certainty that the seniors would read and understand the purpose of the collection,

	use and disclosure of their personal data. By taking measures to ensure that the personal data left by interested seniors are not accessible to the public (e.g. using a metal box that can only be opened by authorised persons), Seniors' activity centre ABC has also complied with the Protection Obligation of the PDPA.
3.9	**Example: Collection, use, and disclosure of personal data for client surveys** SSA ABC intends to conduct a survey on the impact of its services on individual clients, which involves the collection and use of personal data (including clients' full names, contact details and income levels). SSA ABC intends to publish the results of the survey in a manner that identifies the individual clients[4] in their annual report and on their website. **<u>Treatment</u>** SSA ABC must obtain consent from the individual clients to collect, use and disclose their personal data before conducting the survey, unless an exception applies. If SSA ABC intends to use or disclose personal data that had previously been collected for other purposes for this survey, SSA ABC may wish to consider whether the exception for use or disclosure of personal data without consent for research in Division 3[5] of Part 2 of the Second Schedule or Division 2[6] of Part 3 of the Second Schedule respectively would apply.

[4] The Data Protection Provisions will not apply to the disclosure of the results if VWO ABC discloses anonymised data. The data could be anonymised in various ways before publication, such as through removing personal identifiers or aggregating data points so that individual clients can no longer be identified. Chapter 3 of the Selected Topics Guidelines relating to Anonymisation provides more information on anonymisation and re-identification risks.

[5] An organisation may use personal data about an individual without consent of the individual if, subject to conditions, the personal data is used for a research purpose, including historical or statistical research. The conditions are - (a) the research purpose cannot reasonably be accomplished unless the personal data is used 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 an decision that affects the individual; and (d) if the results of the research are published, the organisation publishes the results in a form that does not identify the individual.

[6] An organisation may disclose personal data about an individual without consent of the individual subject to the same conditions (a) to (d) listed in footnote 5 above, and (e) it is impracticable for the organisation to seek the individual's consent for the disclosure.

3.10 **Example: Disclosure of clients' personal data to a third party**

SSA ZYX receives an email request from a neighbourhood grassroots club for a list of SSA ZYX's needy clients and their addresses in order for the grassroots club to deliver some food rations to these clients.

Treatment

The Data Protection Provisions will generally apply to SSA ZYX's disclosure of its clients' personal data to the grassroots club.

Among other things, consent would be required for such disclosure unless an exception applies, such as when the disclosure is necessary for any purpose which is clearly in the interests of the individual, if consent for its disclosure cannot be obtained in a timely way. Please refer to Chapter 12 of the Key Concepts Guidelines on the "Consent Obligation" for more information.

Deemed consent

3.11 *Deemed consent by conduct:* In situations where an individual (without actually giving consent) voluntarily provides his personal data to an organisation for an appropriate purpose, and it is reasonable that he would voluntarily provide the data, the individual's consent to the collection, use or disclosure of personal data is deemed to have been given by the individual's act of providing his personal data.

3.12 **Example: Consent for photo-taking at a private function for clients**

SSA GHI hosts a private dinner function for families and engages a volunteer photographer to take photographs of attendees for its newsletter.

SSA GHI does not explicitly ask the families for consent to take their photographs for the newsletter. However, in this context, consent is deemed to have been given when the individual voluntarily permits a photograph or video recording to be taken of him for SSA GHI's intended purpose, and it is reasonable that he would do so (e.g.

	the individual voluntarily stands in the frame of the photographer's camera without objection). The measures that SSA GHI may take to better ensure that the attendees are aware of the purpose for which their photographs are collected, used and disclosed, could include: a) Clearly stating in its invitation to families that photographs of attendees will be taken at the function for publication in its newsletter; and b) Putting up an obvious notice at the reception or entrance of the function room to inform attendees that photographs will be taken at the event for publication in its newsletter. After seeing the notice at the reception, Mary informed the staff manning the reception that she does not want her photograph to be taken for publication in the newsletter. To facilitate Mary's refusal for her photograph to be taken, the reception staff gives her a lanyard of a different colour from the rest of the participants. This is so that the volunteer photographer can easily identify Mary, to avoid taking her photograph and publishing her photograph in SSA GHI's newsletter. Barry, who was initially deemed to have consented to his photograph being taken during the private function and published in SSA GHI's newsletter, subsequently withdraws his consent after the photograph has been published. SSA GHI is required under the PDPA to cease further publication of the photograph, unless such disclosure without Barry's consent is required or authorised under the PDPA or other written law, for example, if the photograph is already publicly available, or SSA GHI is able to effect the withdrawal of consent (e.g. by masking the image of the individual) before publishing or continuing to publish the photograph.

3.13 *Deemed consent by contractual necessity:* Pursuant to Section 15(3), if an individual gives, or is deemed to have given, consent to the collection, use or disclosure of his personal data to one organisation ("A") for the purpose of a contractual transaction, the consent may cover sharing of his personal data by A with other organisations (and onward sharing by downstream organisations, as the case may be) so long as it is reasonably necessary for A to provide the personal data to the other organisations (likewise, for onward sharing by downstream organisations) to perform or conclude A's contractual obligations.

3.14	**Example: Disclosing donors' data to downstream organisations involved in fulfilling transaction** Mary donates $300 to SSA ABC which provides treatment and care to cancer patients. She provides her personal data (i.e. NRIC number, residential address, bank account details) through an online donation form on SSA ABC's website. The form clearly states that the purpose of collection, use and disclosure of donors' personal data is for SSA ABC to process the donation (e.g. through GIRO deduction from the bank) and for tax relief purposes. **Treatment** As Mary had consented to the collection, use and disclosure of her personal data 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 collect, use or disclose Mary's personal data, where the collection, use or disclosure is reasonably necessary to fulfil the transaction between Mary and SSA ABC. The parties include, for example, Mary's bank, SSA ABC's bank, the online payment gateway in which payment for the transaction is processed, the banks' processors and the tax authority.
3.15	**Example: Disclosure of personal data to medical escorts for caregiving** SSA DEF offers caregiving services to patients that need help to move around or have no caregiver to accompany them for their regular medical check-ups at the hospitals or clinics. In the provision of such caregiving services, SSA DEF engages medical escorts who accompany the patients to and from their homes and the hospitals or clinics for their medical check-ups, help to note down the doctor's prescriptions and help to schedule the next appointment. SSA DEF provides the patients' name, medical conditions and home addresses to the medical escorts for the purpose of fulfilling these caregiving services. In this case, as it is reasonably necessary for SSA DEF to provide the medical escorts with the personal data of patients for the medical escorts to fulfil the caregiving services for the patients, deemed consent by contractual necessity applies.

3.16 *Deemed consent by notification:* Section 15A provides that if an individual does not take any action to opt out of the collection, use or disclosure of his personal data for a purpose that he has been notified of, the individual is deemed to consent to the collection, use or disclosure of personal data by the organisation even for secondary use purposes that are different from the primary purposes for which it had originally collected the personal data for[7].

3.17 Nonetheless, the individual must have been notified that their personal data would be used for such secondary use purposes. The organisation must meet stipulated conditions by conducting an assessment to identify any adverse impact on the individuals arising from the proposed collection, use or disclosure of his personal data, and implement mitigating measures in relation to the adverse impacts identified. Please refer to the Advisory Guidelines on Key Concepts in the PDPA (Chapter 12) for more information on the stipulated conditions.

3.18

Example: Use of clients' personal data for publicity purposes

Various medical institutions refer individuals to SSA ABC for the use of SSA ABC's facilities and services. SSA ABC accepts these individuals as its clients and receives their personal data from the medical institutions for the purpose of facilitating their use of its facilities and services. At the end of each year, SSA ABC engages in publicity to draw attention to its programmes and services, and it wants to use and disclose these clients' names in the publicity materials for that purpose.

SSA ABC conducts an assessment to identify any adverse effect and determines that there are no likely adverse effects to the clients in using and disclosing their name for this new purpose. It also assesses that emailing its clients on the intended sharing of their personal data for the stated purpose is an appropriate and effective method of notification, as it regularly sends such emails to them on its latest programmes. It also assesses that 10 days is a reasonable period for the clients to opt out.

Treatment

[7] Primary purposes are the purposes for which the personal data was originally collected for. Secondary purposes are any purposes which the personal data is further used for after collection.

	SSA ABC sends emails to its clients, notifying them of the intended use and disclosure of their name for the purpose and provides a contact number for any queries on the intended use and disclosure. In the email, SSA ABC stipulates that those who wish to opt out should reply to the email within 10 days from the date of the email, stating that they want to opt out. Clients who do not opt out within the 10-day opt-out period are deemed to have consented to the disclosure of their personal data for the purpose. Nonetheless, SSA ABC must allow and facilitate any withdrawal of consent after the 10-day opt-out period.
3.19	**Example: Publishing photographs taken at a private event on social media** SSA DEF will be conducting a private 1-day retreat for its clients, which include children below the age of 13, and its employees. It wishes to take photographs of the attendees and publish some of the photographs on its social media accounts to generate publicity about its programmes. SSA DEF conducts an assessment to identify any adverse effect and determines that there are no likely adverse effects to the attendees in collecting, using and disclosing their personal data for this purpose. It also assesses that clearly stating in its email invitation to clients or their parents/guardians (for clients below the age of 13) and email notification to employees that photographs of attendees will be taken at the event for publication on its social media accounts is an appropriate and effective method of notification. SSA DEF also assesses that 14 days is a reasonable period to opt out. **Treatment** In its email invitations and notifications to clients and employees respectively, SSA DEF notifies them of the intended collection, use, and disclosure of their personal data for the purpose and provides a contact number for any queries. In the email, SSA DEF stipulates that those who wish to opt out of having their photographs taken at the event should reply to the email within 14 days from the date of the email, stating that they want to opt out. Clients and employees who do not opt out within the 14-day opt-out period are deemed to have consented to the collection, use and disclosure of their personal

	data for the purpose. Nonetheless, SSA DEF must allow and facilitate any withdrawal of consent after the 14-day opt-out period.[8]

Exceptions for collection, use or disclosure of personal data without consent

3.20 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) in circumstances provided in the First (collection, use and disclosure of personal data without consent), Second (additional bases for collection, use and disclosure of of personal data without consent) Schedules to the PDPA.

3.21 Such exceptions include where the collection, use or disclosure of personal data is necessary for evaluative purposes (such as in relation to the grant of financial or social assistance, or the delivery of appropriate health services, under any scheme administered by a public agency)[9]. However, these exceptions to the Consent Obligation do not affect rights or obligations by or under other laws. For example, even if an exception applies under the PDPA, organisations are required to comply with any legal obligations of confidentiality that they may have.

[8] More details can be found in the chapter on Photography, Video and Audio Recordings in the Advisory Guidelines on the PDPA for Selected Topics.

[9] For completeness, "evaluative purpose" is defined under the PDPA to mean –

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

3.22	**Example: Disclosure of personal data without consent in an emergency situation** Maggie works at a day care centre for senior citizens. One day, an elderly client at the centre, Mr. Tan, falls ill after his meal and has to be admitted to the hospital. Maggie provides the hospital staff with Mr. Tan's personal data such as his full name, NRIC number, and medical allergies. **Treatment** Maggie may disclose Mr. Tan's personal data without consent, as there is an applicable exception under the paragraph 2 of Part 1 of the First Schedule to the PDPA which relates to the disclosure of an individual's personal data, without consent, that is necessary to respond to an emergency that threatened, among other things, his health.
3.23	**Example: Exception to the Consent Obligation for evaluative purposes** Don is an employee of SSA DEF that provides social and recreational activities and food rations to low-income households. He receives a call from Audrey, a social worker with SSA 123. Audrey enquires on the services that one of SSA DEF's clients, Mr. Ong, had been receiving, and to understand Mr. Ong's financial situation. Audrey explains to Don that Mr. Ong had approached SSA 123 recently to apply for their pilot social assistance scheme administered by a public agency[10]. **Treatment** In this case, consent is not required for SSA 123 to collect and use Mr. Ong's personal data if the collection or use is necessary for an evaluative purpose[11] (e.g. to determine Mr. Ong's suitability or eligibility for grant of social assistance under the

[10] "Public agency" is defined under the PDPA to include: (a) the Government, including any ministry, department, agency, or organ of State; (b) any tribunal appointed under any written law; or (c) any statutory body specified under subsection (2).

[11] See definition of "evaluative purpose" under the PDPA in footnote 16 in these guidelines, and paragraph 2 of Part 3 of the First Schedule to the PDPA.

	scheme administered by the public agency). Similarly, consent is not required for SSA DEF to disclose Mr. Ong's personal data to SSA 123 if the disclosure is necessary for an evaluative purpose[12]. Both SSA 123 and SSA DEF should also ensure that they remain compliant with relevant sectoral laws and regulatory requirements such as data sharing agreements between SSA 123 and SSA DEF.

Business improvement exception

3.24 The business improvement exception allows organisations to use, without consent, personal data they have collected for business improvement purposes, such as developing new goods or services and understanding individual behaviour and preferences. To rely on this exception, organisations must ensure that the purpose cannot be reasonably achieved without using the data in an individually identifiable form and that the use of the data is one that a reasonable person would consider appropriate in the circumstances[13].

3.25 Subject to certain conditions being fulfilled, the business improvement exception also permits the sharing of personal data between entities belonging to a group of companies, without consent, for improving goods and services, developing new business methods or processes, understanding behaviour and preferences of customers, and identifying suitable goods and services for customers.

3.26 This exception cannot be used to send direct marketing messages to individuals, for which explicit consent must generally be obtained. For further information on the business improvement exception, please refer to paragraphs 12.71 – 12.77 of the Key Concepts Guidelines.

[12] See paragraph 2 of Part 3 of the First Schedule to the PDPA.

[13] 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. Organisations should expect to take some time and exercise reasonable effort to determine what is reasonable in their circumstances. More details on "reasonableness" can be found in Chapter 9 of the Advisory Guidelines on Key Concepts in the PDPA.

3.27	**Example: Use of personal data to improve client services** SSA ABC wants to use its clients' personal data (i.e. age, type of services requested) to derive insights on client demographics to better tailor the services it provides to its clients and improve its outreach to them. SSA ABC assesses that (a) this purpose cannot reasonably be achieved without the use of personal data in individually identifiable form; and (b) its use of personal data is considered appropriate to a reasonable person. **Treatment** SSA ABC may rely on the business improvement exception to use its clients' personal data without consent to understand them better and to enhance the services it provides them. However, if SSA ABC assesses that this purpose can reasonably be achieved without the use of personal data in individually identifiable form, it may not rely on the business improvement exception. Instead, SSA ABC may consider anonymising the data before using it for such a purpose. Anonymisation is the process of removing identifying information, such that the remaining data does not identify any particular individual. Personal data that has been anonymised is no longer considered personal data for the purposes of the PDPA.[14]
3.28	**Example: Use of personal data to better understand donors** SSA DEF wants to use its donors' personal data (i.e. frequency of donation) to derive insights about their profiles and contributions to improve its donor retention rate. SSA DEF assesses that (a) this purpose cannot reasonably be achieved without the use of personal data in individually identifiable form; and (b) its use of personal data is considered appropriate to a reasonable person. **Treatment** SSA DEF may rely on the business improvement exception to use its donors' personal

[14] More details can be found in the chapter on Anonymisation in the Advisory Guidelines on the PDPA for Selected Topics.

	data without consent to understand them better.

Legitimate interests exception

3.29 In general, "legitimate interests" refer to any lawful interests of an organisation or person, including other organisations. Part 3 of the First Schedule to the PDPA outlines specific purposes that would generally be considered "legitimate interests," such as evaluation, investigation, or debt recovery. It also sets out a broad exception that can be relied on for other purposes that meet the definition of "legitimate interests."

3.30 Before relying on the legitimate interests exception, organisations must identify and articulate the legitimate interests, conduct an assessment to identify and mitigate any adverse effects on individuals, and disclose reliance on the exception. The Commission uses a commercially reasonable standard to assess the appropriateness of the mitigatory measures. Examples of reasonable measures include minimizing the amount of personal data collected, implementing access controls, deleting personal data immediately after use. Organisations should also provide the business contact information of a person who can address individuals' queries about their reliance on the exception.

3.31 This exception cannot be used to send direct marketing messages to individuals, for which explicit consent must generally be obtained. For further information on the “legitimate interests” exception, please refer to paragraphs 12.56 – 12.70 of the Key Concepts Guidelines.

3.32	**Example: Fraud detection and prevention of misuse of services** SSA ABC intends to use personal data about its clients and their use of its services to detect fraud and prevent the misuse of its services, where one client attempts to receive the same services multiple times. SSA ABC conducts an assessment of legitimate interests, and assesses that the benefits of the use of personal data (e.g. preventing fraud or misuse of services) is

	in the legitimate interests of SSA ABC and outweigh any likely adverse effect to the individual client (e.g. potential enforcement actions by authorities). SSA ABC also states in its data protection policy on its website that it is relying on the legitimate interest exception to use personal data to detect fraud and prevent misuse of services. **Treatment** SSA ABC may rely on the legitimate interests exception to use personal data about its clients and their use of its services to detect fraud and prevent the misuse of services.
3.33	**Example: Recording of residential facilities for safety and security of residents** SSA ABC provides residential facilities for the shelter and care of some of its clients. It wants to monitor and record, via CCTV, some portions of the residential facilities for the safety and security of its residents. SSA ABC conducts an assessment of legitimate interests, and assesses that the benefits of the collection, use and disclosure of personal data through the recording of the residential facilities (e.g. detect if any residents have injured themselves, deter break-ins to the residential facilities) is in the legitimate interests of SSA ABC and outweigh any likely adverse effect to the individual. SSA ABC also states in its intake form for prospective residents that it is relying on the legitimate interests exception to collect, use, and disclose personal data for the safety and security of all its residents. **Treatment** SSA ABC may rely on the legitimate interests exception to collect, use, and disclose personal data through CCTV recordings of some portions of its residential facilities to protect the safety and security of its residents. As good practice, SSA ABC may wish to put up notices to inform individuals that the areas are under CCTV surveillance. To comply with the Protection Obligation of the PDPA, SSA ABC implements reasonable security arrangements to protect the CCTV surveillance footage, such

	as encrypting the footage in the database and restricting employee access to the footage on a need-to-know basis.
3.34	**Example: Recording of counselling sessions to improve supervision and delivery of casework by social worker** SSA DEF provides counselling services to its clients at its premises. It wants to record the counselling sessions, via CCTV, to improve the supervision and delivery of casework by the social worker or counsellor. SSA DEF conducts an assessment of legitimate interests, and assesses that the benefits of the collection, use and disclosure of personal data through the recording of the sessions (e.g. provide a more conducive environment and better counselling services for the clients) is in the legitimate interests of SSA DEF and outweigh any likely adverse effect to the individual client (e.g. minor discomfort of being watched). SSA DEF also states in its counselling session intake form that it is relying on the legitimate interests exception to collect, use, and disclose personal data to deter undesirable behaviour by counselling clients. **Treatment** SSA DEF may rely on the legitimate interests exception to collect, use, and disclose personal data through CCTV recordings of counselling sessions to improve supervision and performance of the social worker or counsellor. As good practice, SSA DEF may wish to put up notices to inform its clients that the counselling sessions are under CCTV surveillance. To comply with the Protection Obligation of the PDPA, SSA DEF implements reasonable security arrangements to protect the CCTV surveillance footage, such as encrypting the footage in the database and restricting employee access to the footage on a need-to-know basis.
3.35	**Example: Recording of helpline calls on domestic abuse** SSA 123 provides a helpline service to its clients. It wants to record the helpline calls regarding domestic abuse suffered by its clients. The purpose of the recording is to equip SSA 123 to better fulfil its responsibilities to such clients, such as

	providing the client with the necessary support and taking action on their behalf. SSA 123 conducts an assessment of legitimate interests, and assesses that the benefits of the collection, use and disclosure of personal data through the recording of the helpline calls is in the legitimate interests of SSA 123, and outweigh any likely adverse effect to the individual client. SSA 123 also 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 to provide better services to its clients. **Treatment** SSA 123 may rely on the legitimate interests exception to collect, use, and disclose personal data through the recording of helpline calls regarding domestic abuse suffered by its clients to better fulfil its responsibilities to such clients.
3.36	**Example: Joint assessment for better coordination of social services** Madam Koh, a client with multiple social and medical needs, approaches SSA ABC to apply for social service assistance. While interviewing Madam Koh during the application process, Peter, a social worker at SSA ABC, found out that Madam Koh has also been receiving social services from SSA XYZ. Peter believes there could be better coordination between the two SSAs in terms of providing social services to Madam Koh. Peter proceeds to call Paula from SSA XYZ (whose name was shared by Madam Koh as the social worker handling her case) to invite Paula to a case conference and to discuss possible options to render assistance to Madam Koh. The case conference is likely to involve the mutual disclosure of Madam Koh's personal data such as her medical history, family conditions, services that Madam Koh is currently receiving, or has received in the past, by both SSA ABC and SSA XYZ, as represented by Peter and Paula. SSA ABC and SSA XYZ conduct a joint assessment of legitimate interests, and assess that the benefits of the disclosure of Madam Koh's personal data (e.g. prevent overlapping services and ensure fair distribution of welfare resources for all clients)

	is in the legitimate interests of both SSA ABC and SSA XYZ, and outweigh any likely adverse effect to the individual (e.g. minor embarrassment to Madam Koh if data about her family condition is leaked). Both SSAs also include in their respective data protection policies on their websites that they are relying on the legitimate interests exception to disclose personal data for better coordination of social services and management of resources. **Treatment** SSA ABC and SSA XYZ may rely on the legitimate interests exception to disclose personal data of their clients to one another to ensure better coordination of social services and management of resources.
3.37	**Example: Disclosing existing personal data to volunteers to conduct surveys** SSA DEF provides caregivers to patients, to discuss medical procedures with them and provide support mentally to them. To garner feedback and improve their caregiving services, SSA DEF engages volunteers to visit the homes or the hospital wards of patients to conduct a face-to-face survey. The personal data of patients (e.g. names, medical conditions, home addresses and location of hospital wards) that were previously collected by SSA DEF for provision of care to the patients are provided to the volunteers to visit the homes/hospital wards of patients and conduct the face-to-face surveys. **Treatment** SSA DEF wishes to rely on deemed consent by notification. It conducts an assessment to identify any adverse effect and determines that there are no likely adverse effects on the patients in using their personal data for this new purpose. SSA DEF assesses that 14 days is a reasonable period for the patients to opt out. It also assesses that notifying the patients through a message sent by the caregivers using a communication channel (e.g. WhatsApp) that the patients are used to, that their personal data would be used to conduct face-to-face surveys for the stated purpose, and of the opt-out period is an appropriate and effective method of notification. In the message to the patients, SSA DEF notifies the patients that they may opt out of the surveys by replying to the message within 14 days from the

	date of the message. Patients who do not opt out within the 14-day opt-out period are deemed to have consented to the collection, use and disclosure of their personal data for this purpose. However, SSA DEF will allow and facilitate any withdrawal of consent from the patients after the 14-day opt-out period. Alternatively, SSA DEF may rely on the legitimate interests exception if it conducts an assessment and determines that the benefits of the collection and use of personal data (e.g. names, medical conditions, home addresses and location of hospital wards) for volunteers of SSA DEF to visit the homes/hospital wards to conduct face-to-face surveys with the patients is in the legitimate interests of SSA DEF and outweigh any adverse effect on the patients. SSA DEF also states in the caregiver application form that it is relying on the legitimate interests exception to collect and use personal data for the purpose of improving caregiving services through conducting of face-to-face surveys by volunteers.

Obtaining consent from source(s) other than the individual

3.38 The Commission is aware that in some circumstances, an organisation may obtain personal data about an individual with the consent of the individual, but from a source other than an individual ("third party"). These may include:

a) Where the third party source can validly give consent to the collection, use and disclosure of the individual's personal data; 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.

3.39 SSAs may wish to consider how best to obtain consent from clients who are individuals that may not have the capacity to give consent for themselves, such as a client who is mentally unwell, or is a minor[15]. In this regard, the Data Protection Provisions do not affect any authority, right, obligation or limitation under other laws and SSAs should accordingly ensure compliance with other laws such as the Mental

[15] Please refer to the Personal Data Protection Regulations 2021 and Advisory Guidelines on Selected Topics relating to persons who may exercise rights or powers under the PDPA, and considerations when obtaining consent from minors.

Capacity Act.

3.40	**Examples: Consent for collection of personal data from third parties** Adam, an only child who lives with his elderly parents, has not been able to find a job for a year. He learns about a financial assistance programme offered by SSA ABC and decides to apply for it. As part of its enrolment process, SSA ABC requires all applicants to provide the personal data of family members living in the same household, including their full names, and employment status. SSA ABC collects and uses these personal data to evaluate a client's suitability for its programme. Adam had not obtained either parent's consent before disclosing their personal data to SSA ABC. **Treatment** Before disclosing personal data of an individual, the consent of the individual should typically be obtained, unless an exception applies. In this case, SSA ABC can collect Adam's parents' personal data from Adam without his parents' consent, pursuant to Paragraph 8 of Part 3 of the First Schedule to the PDPA. This exception relates to a situation where personal data of an individual (i.e. Adam's parents) was provided to the organisation (i.e. SSA ABC) by another individual (i.e. Adam) to enable the organisation to provide a service for the personal or domestic purposes of that other individual (i.e. Adam). SSA ABC should also ensure that it remains compliant with relevant sectoral laws and regulatory requirements.
3.41	Madam Lim visits SSA ABC and chats with Robert, who is employed by SSA ABC as a social worker, to find out more about a new social assistance programme which it is launching next month. Robert assesses that Madam Lim does not meet the requirements to qualify for SSA ABC's programme, but intends to refer Madam Lim to a programme offered

	by SSA XYZ. Robert obtains Madam Lim's consent to disclose her personal data to SSA XYZ as part of the professional referral process. **Treatment** Before SSA XYZ collects Madam Lim's personal data from SSA ABC (through SSA ABC's employee Robert), SSA XYZ should exercise due diligence to check and ensure that SSA ABC had obtained consent from Madam Lim to disclose her personal data. In this scenario, SSA XYZ is obtaining Madam Lim's personal data from a third party source – SSA ABC. Organisations should adopt appropriate measures to verify that the third party source has obtained consent from the individual concerned. Depending on the circumstances, this may be met by obtaining the individual's consent in writing or in other evidential form through the third party, or obtaining and documenting in an appropriate form, verbal confirmation from the third party that the individual has given consent. In addition, SSA XYZ could, as good practice, verify with Madam Lim when contacting her for the first time that she had provided consent through SSA ABC for SSA XYZ to contact her. Please refer to Chapter 12 of the Key Concepts Guidelines for more information on considerations when collecting personal data from third party sources.

4 The Access and Correction Obligation

4.1 The Access and Correction Obligations (PDPA sections 21, 22 and 22A) state that 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. For more information on the Access and Correction Obligations, do refer to Chapter 15 of the Advisory Guidelines on Key Concepts in the PDPA.

4.2 The following examples illustrate the application of the Access and Correction Obligations.

4.3

Example: Accessing personal data of one individual which was provided by another individual

SSA ABC is launching a new social service scheme targeting the elderly.

Madam Chua, a widow who lives in a one-room apartment, intends to apply for SSA ABC's new scheme.

As part of the application process, Madam Chua is required to provide SSA ABC with the personal data of her family members or those in her support system in order for SSA ABC to assess her suitability. Madam Chua discloses the full names of her five children, and their marital status. In addition, Madam Chua discloses that one of her children, Alan is not her biological son and was adopted. She added that Alan was not aware that he was an adopted child.

Alan learns about his mother's application for the social service scheme and makes an access request for the personal data SSA ABC has about him, and how it had been used by SSA ABC.

Treatment

Generally, SSA ABC should provide Alan access to his personal data which is in the possession or under the control of SSA ABC and information about the ways in which such personal data has been or may have been used or disclosed by SSA ABC over the past year.

	However, SSA ABC must consider if any prohibition under section 21 applies.[16] For example, section 21(3) of the PDPA prohibits SSA ABC from providing Alan with his personal data or other information, as the case may be, if doing so could reasonably be expected to cause immediate or grave harm to the safety or to the physical or mental health of the individual who made the request.[17] In this regard, SSA ABC may reject Alan's access request as disclosure may cause harm to his mental health. SSA ABC may also wish to consider if any of the exceptions to the Access Obligation set out in the Fifth Schedule apply. SSA ABC should generally exercise due diligence and adopt appropriate measures to verify the identity of Alan before providing him with access to his personal data.

[16] Please refer to Sections 21(3) and (4) of the PDPA for the full list of circumstances under which organisations must not provide individuals with access to their personal data.

[17] This is set out in Section 21(3)(b) of the PDPA.

5 The Accuracy Obligation

5.1 Pursuant to 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. For more information on the Accuracy Obligation, do refer to Chapter 16 of the Advisory Guidelines on Key Concepts in the PDPA.

5.2 The following examples illustrate the application of the Accuracy Obligation.

5.3	**Example: Giving of bursary awards to students based on household income data** SSA ABC administers bursary awards to high performing students from low-income households every year. The information required to assess if a student meets the conditions to receive the bursary award may include the student's household income, CPF contributions from the parents and the student's school examination results. SSA ABC collects the required information every year and do not rely on previous years' information to assess the students' eligibility for the current year. **<u>Treatment</u>** SSA ABC has put in place the processes and mechanisms to collect the personal data of students every year that the bursary is administered. This ensures that the information used to assess the eligibility of the students for the bursary is up to date and complete such that a reliable assessment can be made. In this case, SSA ABC has complied with the Accuracy Obligation.
5.4	**Example: Providing of intervention services based on case diagnosis** SSA DEF provides case interventions for families (e.g. domestic abuse, strained relationships, neglected children), where their case officers have consultations

	with the families to understand and administer the appropriate care and support (e.g. intervention programs to help family members reconcile differences, financial assistance, medical care). Personal data that are collected by the case officers and stored in SSA DEF's database may comprise family history, state of relationships, household income and past inflicted injuries. **Treatment** As the appropriate care and support are provided to the families based on the case diagnosis by officers, it is important that SSA DEF puts in place processes to ensure that the case diagnosis is up to date and complete, for example, case workers follow their agency's standard practice to update the case notes and interventions after significant case milestones and close the case promptly when it is resolved or referred to another agency. In general, SSAs shall determine the frequency of case sessions based on the specific circumstances of the cases. SSAs must do their due diligence and reasonably ensure the accuracy of personal data collected from their clients.
5.5	**Example: Ensuring the contact information of bone marrow donors are up to date** SSA GHI provides bone marrow donation services where they match the DNA patterns of donors with patients in need of a bone marrow transplant. They store the records of DNA patterns together with the contact information of the donors within their database until they are able to match the donor with a patient. After many years have lapsed since the donors' information were obtained, their contact information may be outdated. **Treatment** As the contact information of the donors are not used by SSA GHI to make a decision that affects the donor but is merely used as a means of communication with the donor, it is not mandatory under the Accuracy Obligation to ensure that the contact information is up to date and complete. On the other hand, donors' DNA patterns are used to match with patients and to make a decision on whether the donor is suitable for bone marrow transplant

	with a particular patient. However, DNA patterns generally remain the same throughout a person's life and do not need to be updated. As a good practice and for the effectiveness of the bone marrow donation services, SSA GHI can regularly contact the donors via emails or other channels to reaffirm their willingness as a donor and update their contact information if needed.

6 The Protection Obligation

6.1 The PDPA requires an organisation to make reasonable security arrangements to protect personal data in its possession or under its control 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.

6.2 There is no 'one size fits all' solution for organisations to comply with the Protection Obligation. Generally, SSAs should consider factors such as the nature of the personal data in their possession who or under their control (as the case may be), and the adverse impact to individuals if an unauthorised person obtained, modified, or disposed of the personal data, to determine the security arrangements that are reasonable and appropriate in the circumstances.

6.3 Please refer to Chapter 17 of the Key Concepts Guidelines for more information relating to the Protection Obligation, and more examples of security arrangements. The following examples illustrate the application of the Protection Obligation.

6.4

Example: Protecting personal data that has been collected

SSA XYZ operates a day activity centre for senior citizens. As part of its security procedures, SSA XYZ requires all visitors to the centre to sign up for a visitor pass at the reception. Visitors are requested to provide their name and contact number in order to be issued a visitor pass. SSA XYZ records such information in their visitor management system which contains a database for visitors.

Treatment

SSA XYZ should consider the specific circumstances when assessing whether it is reasonable to collect the personal data of visitors to their premises.

Generally, SSA XYZ is required to comply with the Protection Obligation in respect of the personal data recorded in the visitors' database. Security arrangements implemented by organisations may take various forms such as administrative measures, physical measures, or technical measures.

In the case of SSA XYZ, for example, an administrative measure would be to design the visitor digital database on the laptop such that the visitor keying in their

	personal data is unable to view the personal data of other visitors. SSA XYZ avoids using a visitors' excel sheet where visitors may view the personal data of other visitors when keying in the excel sheet. Other administrative measures include restricting employee access to the visitors' database on a need-to-know basis and using privacy filters to minimise unauthorised persons from viewing the personal data on the laptop. Technical measures that SSA XYZ can implement would be password-encrypting the visitors' database and activating self-locking mechanisms for the laptop screen if the laptop is left unattended for a certain period of time.
6.5	**Example: Protecting personal data collected through a website** SSA ABC operates an online portal which allows individuals to sign up as volunteers. The registration process involves the collection of personal data of individuals who sign up, such as their full names, mobile numbers and email addresses. **Treatment** SSA ABC is required to comply with the Protection Obligation by making reasonable security arrangements to protect the personal data collected by SSA ABC through the portal. An example of a technical measure which SSA ABC could adopt would be to encrypt all personal data captured through the registration process before it is being transferred to SSA ABC's local database for storage.
6.6	**Example: Protecting personal data in photographs taken** John, a volunteer at SSA ABC, is assisting SSA ABC to organise a gathering for its clients, donors and volunteers at its centre. As John is an avid photographer, SSA ABC requests John to take photographs of the event, so that SSA ABC can post them on its official website and official social media network accounts. SSA obtains the requisite consent from those attending the event for their photographs to be taken for these purposes. Subsequently, John intends to use some of the unpublished photographs from SSA ABC's event to create a montage and post it on his personal social media network profile page.

	Treatment Even as a volunteer, John is regarded as an employee of SSA ABC under the PDPA. As John was acting as an employee within the meaning of the PDPA when taking the photographs, the unpublished photographs belong to SSA ABC and John should not share them on his personal account without explicit consent from SSA ABC[18]. SSA ABC should implement reasonable security arrangements to safeguard itself against such risks. For example, SSA ABC may implement policies and procedures (e.g. disciplinary measures in the event of breaches) for employees to ensure protection of the personal data in its possession or under its control, including photographs taken of the SSA's clients, donors and volunteers and/or conduct training for employees to impart good practices on handling personal data. Please refer to Chapter 17 on the Protection Obligation in the Key Concepts Guidelines for more information.
6.7	**Example: Reasonable security arrangements to protect elderly clients' personal data** SSA ABC engages volunteers to distribute care packs to the homes of more than 200 elderlies all over Singapore. The volunteers will need access to the personal data of the elderly clients (e.g. names, home addresses and phone numbers). To comply with the Protection Obligation, SSA ABC puts in place reasonable security arrangements, such as administrative and physical measures etc., to protect the elderly clients' personal data after assessing the nature of personal data in its possession and the possible impact to the elderly clients concerned if the data is obtained by an unauthorised person. For instance, SSA ABC only allows volunteer access to personal data on a need-to-know basis and ensures that each volunteer holds only an appropriate amount of the personal data. Volunteer leaders are assigned to each district, and only holds the data of elderly clients in that district. Volunteer leaders will further delegate the work of distributing care packs among

[18] SSA ABC may be liable for John's conduct under the PDPA, as John is regarded as an employee of SSA ABC. In this case, John's actions may potentially cause SSA ABC to breach the Protection Obligation. Nevertheless, according to Section 48D of the PDPA, if John shares the photographs on his personal account, knowing that the disclosure is not authorised by SSA ABC, or is reckless to whether the disclosure is or is not authorised by SSA ABC, John may be held liable.

	the volunteers under them and only provide required personal data of elderly clients to the volunteers (e.g. a pair of volunteers only delivers care packs to five homes, so they only hold the personal data of elderly clients living in those homes). To reduce the risk of personal data being leaked (e.g. elderly clients' personal data accidentally forwarded to unrelated third parties), SSA ABC provides the personal data of the elderly only on the day of distributing the care packs and in hardcopy. After the care packs have been distributed, the volunteers are to return the hardcopy papers of the elderly clients' personal data to the volunteer leaders, who will properly dispose of the documents. SSA ABC sometimes uses messaging platforms (e.g. WhatsApp) to communicate with volunteers and send volunteers the personal data of clients via a photograph for distribution of care packs to their homes. SSA ABC only sends the photograph on the day of distributing the care packs, and instructs the volunteers to delete the photograph from their phones and their "recently deleted" folder after the care packs have been distributed. Alternatively, for added security, SSA ABC may upload the personal data of the clients on a system, where volunteers can only view the data but not download into their phones. It is advisable for SSA ABC to implement measures in selecting and training the volunteer leaders, who hold higher responsibility in handling the personal data of elderly clients. SSA ABC shall also conduct basic data protection training for all their volunteers, and ensure volunteer leaders supervise the volunteers under them. Under the PDPA's Accountability Obligation, organisations are responsible for personal data in their possession or control. As volunteers are considered as employees of an organisation for the purpose of the PDPA, SSA ABC is required to provide training for its volunteers and communicate to its volunteers information about its policies and procedures.

7 The Retention Limitation Obligation

7.1 The Retention Limitation Obligation 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 the retention is no longer necessary for legal or business purposes.

7.2 The PDPA does not prescribe a specific retention period for personal data. However, SSAs should review the personal data they hold on a regular basis to determine if that personal data is still needed. The retention period for personal data under the PDPA can depend on whether the personal data is required for research or archival purposes that benefit the wider public or a segment of the public. SSAs should not keep personal data "just in case", when it is no longer necessary for the purposes for which the personal data was collected or for any legal or business purpose.

7.3 Please refer to Chapter 18 of the Key Concepts Guidelines for more information relating to the Retention Limitation Obligation. The example below illustrate the application of the Retention Limitation Obligation to the social service context.

7.4

Example: Retention of volunteers' data for organisational use

SSA ABC engages volunteers over a period of one week to distribute food to elderlies living alone. SSA ABC keeps a record of personal data of the volunteers within their Volunteer Management System (VMS). After the week, SSA ABC retains these personal data as, based on past experience, the volunteers may wish to retrieve their volunteering records in the future, and SSA ABC has assessed based on past experiences that these identifiers (e.g. full name, type of volunteering activity, date(s) of volunteering and number of volunteering hours) are sufficient for such purpose.

As SSA ABC is retaining the personal data of volunteers for a valid business purpose, the Retention Limitation Obligation does not require SSA ABC to cease to retain the personal data after the volunteering activity ends. As a good practice, SSA ABC sets an appropriate retention period based on its experience with ex-volunteers requesting access to their volunteering records. At the end of the retention period, the VMS automatically purges these data.

8 The Transfer Limitation Obligation

8.1 The Transfer Limitation Obligation (PDPA section 26) states that an organisation must not transfer personal data to a country or territory outside Singapore except in accordance with the requirements prescribed under the PDPA. For more information on the Transfer Limitation Obligation, do refer to Chapter 19 of the Advisory Guidelines on Key Concepts in the PDPA.

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

8.3

Example: Transferring clients' personal data across borders for research to improve welfare services

SSA ABC provides welfare services to clients in Singapore and intends to transfer clients' personal data out of Singapore to their headquarters situated in another country via the group's centralized clients' management system. The agency headquarters is accumulating the data from various countries for the purpose of conducting demographic research to improve the welfare services administered to their clients in the region.

Treatment

SSA ABC has to ensure that it takes appropriate steps to ensure that their agency headquarters situated overseas 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.

Since SSA ABC and the agency headquarters belong under the same group, they may rely on binding corporate rules. The conditions of the transfer, including protections that will be accorded to the personal data transferred, can be set out in binding corporate rules that apply to both SSA ABC and the agency headquarters. In this case, SSA ABC's transfer of clients' personal data to its agency headquarters would be in compliance with the Transfer Limitation Obligation.

If the data that is being exchanged between SSA ABC across borders is aggregated and does not contain personal identifiers of clients, such data will not be considered personal data, and the Transfer Limitation Obligation of the PDPA will

	not apply.
8.4	**Example: Outsourcing outreach services for donors to overseas call centre** SSA 123 operates in and provides charity services to clients in Singapore. In terms of reaching out to donors to financially support their charity programs, they have outsourced the outreach services to a call centre located in a neighbouring country. SSA 123 will have to transfer the personal data (e.g. name, contact details) of regular donors with an existing relationship with them to the call centre to inform about new charity programs and to encourage donations. **Treatment** The call centre that processes donors' personal data given by SSA 123 for outreach services can be considered a data intermediary of SSA 123. Therefore, SSA 123 is responsible for complying with all the obligations under the PDPA in respect of personal data processed by the call centre. To ensure that the overseas call centre is bound by legally enforceable obligations to provide the transferred personal data of donors a standard of protection that is comparable to that under the PDPA, SSA 123 may establish a written contract with the overseas call centre that imposes such a standard.
8.5	**Example: Engaging a cloud service provider to store personal data of clients** SSA DEF engages a cloud service provider (CSP) to store a sizeable volume of personal data of their clients (e.g. name, age, gender, home address, household income). Before signing up for its services, SSA DEF enquired on where the data centres that store the personal data of their clients are located, and they understand from the CSP that the data centres are located overseas. **Treatment** Where the CSP is processing personal data on behalf and for the purposes of another organisation pursuant to a contract which is evidenced or made in writing,

	the CSP is considered a data intermediary. SSA DEF is still responsible for complying with all obligations under the PDPA in respect of personal data processed by the CSP on its behalf and for its purposes. The CSP is specifically subject to the Protection, Retention Limitation and Data Breach Notification Obligations under the PDPA with regards to the personal data that it processes or hosts in data centres outside Singapore. Any issues of compliance can be provided for in the written contract between SSA DEF and its CSP. Before signing up for the CSP's services to store clients' personal data, SSA DEF can notify its clients in writing that it is adopting a cloud-based solution to store its clients' personal data, and asks for the clients' consent to move their data to the cloud-based solution. SSA DEF also provides its clients with a written summary of the extent to which their 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 the clients provide their consent, SSA DEF would be able to rely on the CSP's services to transfer its clients' personal data to data centres located overseas in compliance with the Transfer Limitation Obligation. Alternatively, SSA DEF can use the services of a CSP that has legally enforceable obligations to ensure a comparable standard of protection for the transferred personal data. For example, SSA DEF can carry out due diligence and determine if the CSP is certified under the APEC CBPR system in the overseas country, which will ensure that the clients' personal data stored in the overseas data centres are protected to a standard comparable to the PDPA. SSA DEF can refer to the list of CBPR-certified organisations on the APEC website (www.cbprs.org). For more information on using cloud service providers in relation to the PDPA, please refer to Chapter 9 of the Advisory Guidelines on the PDPA for Selected Topics.

9 The Data Breach Notification Obligation

9.1 The Data Breach Notification Obligation (PDPA sections 26A to 26E) states that 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. For more information on the Data Breach Notification Obligation, do refer to Chapter 20 of the Advisory Guidelines on Key Concepts in the PDPA.

9.2 The following examples illustrate the application of the Data Breach Notification Obligation.

9.3

Example: Contractual requirements to report data breaches to funders

SSA 123 is funded by multiple public agencies. The funding contracts require SSA 123 to immediately report to these public agencies in the event of a data breach that is assessed to result in significant harm to affected individuals or is of a significant scale.

Treatment

According to Section 4(6)(a) of the PDPA, the provisions of the PDPA will not affect other legal obligations of SSA 123, such as SSA 123's contractual obligations to its funders, i.e. other public agencies. However, the performance of a contractual obligation is not an excuse for SSA 123 to contravene the PDPA.

Hence, in case of a data breach assessed to result in significant harm to affected individuals or is of a significant scale, SSA 123 must, in addition to its complying with its contractual obligations to its funders, comply with the Data Breach Notification Obligation by notifying the PDPC and/or the affected individuals where necessary.

9.4

Example: Data breaches of significant harm and of significant scale

SSA ABC deals with cases of youth offenders. It discovered that one of its staff had misplaced a secure thumb drive containing the full names of 20 young persons and information that leads to the identification of them as having been the subject of investigations under the Children and Young Persons Act (CYPA) or had been arrested, on or after 1 July 2020, for an offence committed under any written law.

Another social service agency, SSA DEF, administers bursary awards to high performing students from lower income households. The database administrator of SSA DEF discovers an unauthorized access of the personal data of their bursary award candidates. The unauthorized access is found to involve the email addresses and first names of 600 candidates, but not any of their financial information (e.g. debit card number, parents' salary).

Treatment

Both SSA ABC and SSA DEF shall conduct an assessment of the data breach once they discover it, generally within 30 calendar days, to establish the facts of the data breach and determine whether it is notifiable.

The data breach faced by SSA ABC would likely result in significant harm to affected individuals and SSA ABC should notify the PDPC no later than 3 calendar days[19] upon determining that the data breach is notifiable, and the affected individuals at the same time or after notifying the PDPC. The Personal Data Protection (Notification of Data Breaches) Regulations 2021 provides that a combination of an individual's full name and personal data of vulnerable individuals, such as those of youth offenders or potential youth offenders contained in the misplaced thumb drive, is deemed to result in significant harm to affected individuals if compromised in a data breach.

The data breach faced by SSA DEF is of a significant scale as it affects the personal data of 500 or more individuals, even if the personal data compromised (i.e. email addresses and first names) do not fall under the prescribed classes of data deemed by the Personal Data Protection (Notification of Data Breaches) Regulations 2021 to cause significant harm. SSA DEF must notify the PDPC of the data breach no later than 3 calendar days upon determining that the data breach is notifiable, but is not required to notify affected individuals.

10 Organisations and Data Intermediaries

10.1 Generally, organisations[20] that SSAs typically work with (such as sponsors, donors or service providers) will also be subject to the Data Protection Obligations, unless they fall within a category of organisations that is expressly excluded. For example, organisations which are data intermediaries are partially excluded from the application of the Data Protection Provisions, as explained further below.

10.2 A data intermediary is an organisation that processes personal data on behalf of another organisation, but excludes an employee of that other organisation. In some situations, SSAs may engage data intermediaries to process personal data. 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 Protection Obligation, Retention Limitation Obligation and the Data Breach Notification Obligation, and not any of the other Data Protection Provisions.

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

10.4 In any case, under section 4(3) of the PDPA, the organisation that engages the data intermediary would still have the same obligations under the PDPA in respect of personal data processed on its behalf as if the personal data were processed by the organisation itself.

10.5 SSAs should note that whether an organisation charges a SSA for its services generally does not affect whether that organisation is a data intermediary of the SSA. Please refer to Chapter 6 of the Key Concepts Guidelines for more information on when an organisation is considered a data intermediary, as well as the obligations applicable to data intermediaries and the organisations that engage data intermediaries, under the PDPA.

---

[19] Please refer to Annex D of PDPC's Guide on Managing and Notifying Data Breaches for a chronology flowchart on the data breach notification timeline.

[20] 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".

10.6

Example: Engaging a data intermediary to manage payroll

Company 789, which is owned by one of SSA GHI's Board Members, provides pro-bono services to process the payroll for all employees working in SSA GHI's various centres in Singapore. Company 789 holds records of SSA GHI's employees such as their full names, NRIC numbers, duration of employment, salary and bank account details. Company 789 is processing the personal data solely for the purposes of payroll administration pursuant to a written agreement with SSA GHI.

Treatment

In this case, Company 789 is considered a data intermediary processing personal data on behalf of and for the purposes of SSA GHI pursuant to a contract evidenced or made in writing. The fact that Company 789 does not charge SSA GHI for its services does not affect Company 789's status. Company 789 will be subject only to the Protection Obligation, Retention Limitation Obligation, and Data Breach Notification Obligation under the PDPA in respect of such processing, while SSA GHI will have the same obligations under the PDPA in respect of the personal data of SSA GHI's employees processed on its behalf by Company 789, as if the personal data were processed by SSA GHI itself.

10.7

Example: Engaging a data intermediary to host personal data on cloud

SSA 123 engages Company ABC, based in Singapore, to develop a HR management system for its employees. This system utilizes a cloud storage solution, provided and administered by Company ABC, for the storage of data. After development, SSA 123 stores its employees' personal data, such as their full names, NRIC numbers, salary and bank account details, on the HR management system. Company ABC provides these services, including the cloud storage solution, to SSA 123 pursuant to a written agreement between both parties.

Treatment

In this case, Company ABC is considered a data intermediary processing personal data on behalf of and for the purposes of SSA 123 pursuant to a contract evidenced

	or made in writing.[21] Company ABC will be subject only to the Protection Obligation, Retention Limitation Obligation, and Data Breach Notification Obligation under the PDPA in respect of such processing, while SSA 123 will have the same obligations under the PDPA in respect of the personal data of their employees processed on its behalf by Company ABC, as if the personal data were processed by SSA 123 itself. To comply with the Protection Obligation, Company ABC can ensure that the cloud storage solution has industry standards like ISO27001, the ability to produce technical audit reports such as the SOC-2 upon request and Tier 3 of the Multi-Tiered Cloud Security ("MTCS") Certification Scheme. In particular, SSA 123 must comply with the Transfer Limitation Obligation if, in providing the cloud storage service, Company ABC has to transfer the personal data to its servers located overseas. SSA 123 may do so by ensuring that the cloud storage solution utilised by Company ABC accords a comparable standard of protection to the transferred personal data. One option is for SSA 123 to ensure that Company ABC uses a cloud storage solution that has legally enforceable obligations. For example, the cloud storage solution is certified under the APEC CBPR system in the overseas country, which will ensure that the clients' personal data stored in the overseas data centres are protected to a standard comparable to the PDPA. SSA 124 and Company ABC can refer to the list of CBPR-certified organisations on the APEC website (www.cbprs.org).[22]

[21] Under the PDPA, processing of personal data includes the holding of personal data (see section 2(1) of the PDPA).

[22] Further details on complying with the Transfer Limitation Obligation can be found in Chapter 9 on Cloud Services in the Advisory Guidelines on the PDPA for Selected Topics.

11 Rights and obligations, etc under other laws

11.1 Section 4(6) of the PDPA states that unless otherwise provided in the PDPA, nothing in Parts 3 to 6 of the PDPA shall affect any authority, right, privilege or immunity conferred, or obligation or limitation imposed, by or under the law, including legal privilege, except that the performance of a contractual obligation shall not be an excuse for contravening the PDPA, and the provisions of other written law shall prevail to the extent that any provision of Parts 3 to 6 is inconsistent with the provisions of that other written law.

11.2 Similarly, section 13(b) of the PDPA provides that an organisation shall not, on or after the appointed day (i.e., 2 July 2014), collect, use or disclose personal data about an individual without the consent of the individual unless the collection, use or disclosure, as the case may be, without the consent of the individual is required or authorised under the PDPA or any other written law.

11.3 Section 19 of the PDPA provides that notwithstanding the other provisions of Part 4 of the PDPA, an organisation may use personal data collected before the appointed day (i.e., 2 July 2014) for the purposes for which the personal data was collected, unless consent for such use is withdrawn or the individual 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. For avoidance of doubt, the Do Not Call Provisions will apply to the sending of specified messages to Singapore telephone numbers, even if the Singapore telephone numbers are collected before the appointed day.

PART III: APPLICATION OF THE DO NOT CALL PROVISIONS TO THE SOCIAL SERVICE SECTOR

The following sections and examples set out the application of the Do Not Call Provisions to scenarios faced in the social service sector. They are not meant to exhaustively address every obligation in the PDPA that would apply in that scenario. In particular, they do not illustrate the application of the Data Protection Provisions, which were addressed earlier in these Guidelines.

12 The Do Not Call Provisions

12.1 Messages with a purpose to offer to supply, advertise or promote goods or services, land or an interest in land, or a business or investment opportunity, or a supplier of such goods, services, land or opportunity are specified messages and the Do Not Call Provisions will apply to such messages. Messages which do not contain any of such purposes would not be considered specified messages.

12.2 In addition, some types of messages, listed in the Eighth Schedule to the PDPA, are excluded from the definition of a specified message. Some examples include:

a) "business-to-business" marketing messages;

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

c) any message the sole purpose of which is to facilitate, complete or confirm a transaction that the recipient of the message has previously agreed to enter into with the sender;

d) any message that is sent while the sender is in an ongoing relationship with the recipient of the message; and the sole purpose of which relates to the subject matter of the ongoing relationship; or

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

12.3 The Do Not Call Provisions apply to a specified message (in the form of voice calls, text messages or faxes) addressed to a Singapore telephone number, if the sender of the specified message is present in Singapore when the specified message is sent, or the recipient of the specified message is present in Singapore when the specified message

is accessed.

Duty to check the Do Not Call Registers

12.4 One significant obligation under the Do Not Call Provisions is that the organisation sending the specified message will have to check the Do Not Call Registry (the "DNC Registry") established by the Commission under the PDPA to confirm that the number is not listed on the DNC Register, unless the user or subscriber of the Singapore telephone number has given clear and unambiguous consent in written or other accessible form.

12.5 The PDPA lists obligations for third-party checkers[23] who check the DNC Registry for an organisation and provide to the organisation information on whether the Singapore telephone number is listed in the relevant DNC Register. The checker must make sure that information provided to the organisation is accurate and up-to-date in accordance with the provisions relating to the DNC Registry[24], and to provide to the organisation the date of retrieval of this information and its validity period.

12.6 **Examples: Whether messages are specified messages[25]**

SSA ABC runs a caregiver support group for families taking care of the elderly and will be conducting a seminar to impart skills in caring for the elderly.

a) SSA ABC sends an SMS to various individuals who are clients and volunteers to publicise the event. The message is likely to be **a specified message** to the extent that it is an offer to provide a service.

b) SSA ABC calls SSA XYZ's office line to inform SSA XYZ about the seminar and ascertain whether SSA XYZ would like to promote the upcoming seminar to SSA XYZ's clients and volunteers. **Such a call is <u>not</u> a specified message** as under the Eighth Schedule, a message sent to an organisation (other than an individual acting in a personal or domestic capacity) for any business

[23] Please refer to section 43A of the PDPA for definition of a third-party checker and the full set of obligations for checkers.

[24] Including Part 5A of the Personal Data Protection (Do Not Call Registry) Regulations 2013.

[25] Please refer to the Advisory Guidelines on the Do Not Call Provisions for more information and examples on when messages are considered specified messages.

	purposes of the receiving organisation is excluded from the meaning of specified message. c) Should SSA XYZ market SSA ABC's seminar to individuals listed in SSA XYZ's own database of clients and volunteers by sending messages to their telephone numbers, SSA XYZ **will be sending a specified message** to those individuals. d) SSA ABC sends an SMS to its clients and volunteers, who had signed up for the seminar, informing of a postponement in the seminar. SSA ABC **is <u>not</u> sending a specified message** to the extent that the message does not offer to supply a good or service or have any of the other purposes listed in the definition of a specified message.
12.7	SSA XYZ is organising an annual charity fund-raiser. e) SSA XYZ sends an SMS to its donors and volunteers to donate money during the annual fund-raiser. To the extent that the SMS does not offer to supply a good or service or have any of the other purposes listed in the definition of a specified message, such a message would <u>not</u> be a specified message. f) SSA XYZ sends an SMS to its clients, donors and volunteers informing that it has partnered Company ABC to sell ABC's limited-edition products at the annual fund-raiser. In this case, as SSA XYZ is offering to supply or promoting Company ABC's products, it is **considered to be sending a specified message.** g) SSA XYZ calls its donors and volunteers to thank them for the donations/assistance rendered at the charity fund-raiser. SSA XYZ **is <u>not</u> sending a specified message** as the message does not offer to supply a good or service or have any of the other purposes listed in the definition of a specified message.

12.8	**Example: Obtaining clear and unambiguous consent for future volunteering opportunities** John volunteers at SSA GHI where volunteers accompany elderly clients for an outdoor walk at the nature park. When John signed up for this volunteering activity in a form, he checked a box to indicate that he consents to receiving specified messages by SMS for future volunteering opportunities with SSA GHI, even after the outdoor walk with elderly clients. John would be considered to have provided clear and unambiguous consent for SSA GHI to send text messages for future volunteering opportunities. Therefore, SSA GHI may send such messages to John without checking the DNC Registry.

Dictionary Attacks and Address-Harvesting Software

12.9 Section 48B of the PDPA provides that organisations must not send, cause to be sent, or authorise the sending of messages to recipient telephone numbers that are obtained by dictionary attack or address-harvesting. Dictionary attack is the method by which the telephone number is obtained using automated means that generate possible telephone numbers by combining numbers into numerous permutations, whereas address-harvesting is a software specifically designed or marketed for use for searching the Internet for telephone numbers and the telephone numbers are collected, compiled, captured or otherwise harvested.

END OF DOCUMENT