Copyright

Document Version Control Log

Ver. No.	Change Summary	Change Owner	Date Approved
1-2014	Release of Personal Data Protection Manual	Risk Management & Compliance	July 2014
1-2018	Annual review of manual and following key changes: • Change from Manual to Handbook • Amended from 8 obligations to 9 obligations • Merge Retention Policy – Corporate Employees into Handbook • Include Critical Data definitions (Per Global Data Governance) • Include the sharing of PDPC views on use of randomly generated numbers for cold calling • Replace PIAS Consent to Refer Form to Client Referral Services Consent Form • Update data protection email address to 'dataprotection@pias.asia' • Added new section – Section 13 Do Not Call (DNC) Provisions	Jafmine Tan (Risk Management & Compliance)	October 2018
1-2024	Review of Handbook: • Updated Section 1 – 10, Section 12 - 14 • Included new Section 11 – Data Breach Notification Obligation • Included new Section 16 – Related Policies/Standards/Resources • Updated Annex A - E	Kelly Lam, Tang Ming Yang, Chua Mei Na (Risk Management & Compliance)	December 2024

Table of Contents

1. INTRODUCTION

1.1. Background to the Personal Data Protection Act 2012

1.1.1. The Personal Data Protection Act 2012 (the "**PDPA**") is a baseline standard of protection for personal data in Singapore, administered and enforced by the Personal Data Protection Commission ("**PDPC**") since 2 January 2013. It contains two main set of provisions, covering personal data protection and the Do Not Call Registry. It applies to Professional Investment Advisory Services Pte Ltd (the "**Organisation**") and the Organisation must comply with it.

1.1.2. Penalties for breaching the Data Protection Provisions can include fines up to S$1 million or 10% of the Organisation's annual turnover, whichever is higher. For any intentional or negligent contravention of DNC Provisions involving the use of dictionary attacks and address-harvesting software, fines can reach up to S$200,000 for individuals and S$1 million or 5% of the Organisation's annual turnover, whichever is higher, for the Organisation. Contraventions of other DNC provisions can include a fine up to S$200,000 for individuals and S$1 million for the Organisation.

1.2. Compliance Handbook as part of Employment Contract

1.2.1. This Personal Data Protection Handbook ("Handbook") sets out various policies that all employees must comply with. From 2 July 2014 onwards, all employees and agents of the Organisation must strictly comply with this Handbook and all policies set out therein. This Handbook forms a part of the terms of the employment contract between the Organisation and the employee. **FAILURE BY THE EMPLOYEE TO COMPLY WITH THIS POLICY OR A BREACH BY THE EMPLOYEE OF THE TERMS OF THIS POLICY WILL SUBJECT THE EMPLOYEE TO DISCIPLINARY PROCEEDINGS INCLUDING POSSIBLE TERMINATION AT THE DISCRETION OF THE ORGANISATION.**

1.2.2. Penalties for breach of PDPA can be very high, with the PDPC being empowered to impose financial penalties of up to S$1 million or 10% of the Organisation's annual turnover in Singapore, whichever is higher for non-compliance with PDPA. The PDPC can also give directions to stop the Organisation from continuing certain activities. A breach of PDPA may also carry with it criminal and/or civil liability under PDPA.

1.2.3. Investigations require significant time, resources and management input that can be disruptive to business and may also have a negative impact on the Organisation's general reputation. All employees are therefore expected to be fully aware of the dos and don'ts for compliance with PDPA. Further, should the Organisation be fined for breaches of PDPA as a result of an action or omission of any employee, the Organisation reserves its right to claim compensation and damages from that employee.

1.3. Objectives of the Personal Data Protection Handbook

1.3.1. This handbook defines the policies adopted by the Organisation in relation to its obligations under PDPA. Employees and advisers are required to be aware of the obligations imposed by the PDPA. Unless otherwise stated, all obligations of the Organisation under PDPA are to be taken as obligations of individual employees as well. This handbook is also designed to:

(a) assist employees and advisers in understanding the requirements of PDPA;

(b) increase awareness of what is prohibited and what constitutes unacceptable behaviour under PDPA; and

(c) to serve as a reference guide for employees and advisers to ensure that they do not breach personal data protection laws in their daily duties, business dealings and practices.

1.3.2. All employees and advisers should note that this Handbook does not constitute or should not be taken as a replacement for seeking legal advice. If you are not sure and need specific advice for your actions or conduct, you should contact the Data Protection Officer immediately.

1.4. The Organisation's Data Protection Officer

1.4.1. The Organisation will have one or more Data Protection Officers. If in doubt on any aspect of PDPA or this Handbook, please do not hesitate to contact the Data Protection Officer via pias.dataprotection@singlife.com.

1.4.2. The DPO may delegate activities to other individuals provided such alternatives are competent to fulfil the required activities and must ensure that there are appropriate oversight controls in place. The DPO will remain accountable for all activities that are delegated.

1.5. Amendments/Frequency of Review

1.5.1. The Organisation reserves its right to amend this Handbook from time to time. The amended Handbook will similarly apply to you and become part of your employment contract with the Organisation. The Handbook is to be reviewed by DPO and/or Risk Management and Compliance annually as part of Group Risk's Annual Policies and Procedures Attestation.

1.6. What to Do if You are Aware Of or Suspect a Data Breach

1.6.1. If you have a concern or a problem that you believe may be a violation of PDPA, or the data protection principles or methods of compliance set out in this Handbook, please report it immediately to the Data Protection Officer.

1.6.2. If you spot or become aware that a data breach has occurred within the Organisation, immediately inform your line manager and the Data Protection Officer. Dealing with a data breach quickly can limit the damage that it causes.

1.6.3. All employees and advisers should remember that examples provided in this Handbook are for illustration purposes only and are non-exhaustive. If you are unsure whether a specific conduct or activity is prohibited or adequate for compliance, or whether certain contractual terms are adequate for compliance with PDPA or this Handbook, please seek advice from the Data Protection Officer. Do not proceed with any conduct, activity or agreement unless clearance has been given by the Data Protection Officer.

2. OVERVIEW OF PERSONAL DATA PROTECTION ACT 2012

2.1. Objective of PDPA

2.1.1. The overall objective of PDPA is to circumscribe an organisation's activities relating to the collection, use and disclosure of personal data. PDPA seeks to balance an individual's right to protect his / her personal data versus the commercial or operational need of organisations to process personal data. Broadly, PDPA contains 2 main sets of provisions. One relates to data protection principles while the other relates to the Do Not Call registry ("DNC"). In this section we explain in detail what constitutes personal data under PDPA, examples of personal data collected by the Organisation, an overview of the obligations under PDPA that are applicable to such personal data and an overview of the DNC obligations.

2.1.2. 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 PDPC and affected individuals of data breaches; and

(e) Having policies and practices to comply with PDPA.

2.1.3. PDPA also sets out offences that hold individuals accountable for egregious mishandling of personal data. The offences are for knowing or reckless unauthorized (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.

2.2. Personal Data under PDPA

2.2.1. PDPA will apply to all personal data. Personal data is defined under 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*"

2.2.2. PDPA defines an "individual" to mean a "natural person, whether living or deceased". Please see the explanation at paragraph [**2.2.9**]. below on the meaning of "natural person".

2.2.3. The above definitions cast the net wide on the extent of data that will fall within the definition of personal data and consequently under the ambit of PDPA. Personal data includes electronic and non-electronic form and regardless of whether such data is true or accurate. PDPA generally applies to all personal data that the Organisation collects, uses and discloses in the Organisation's daily activities, business dealings and practices, including but not limited to:

(a) personal data relating to the Organisation's customers; and

(b) personal data relating to the Organisation's employees and advisers.

2.2.4. Personal data can be factual (such as name, NRIC, photograph, email address or medical records) or it can be an opinion (such as an employment appraisal or evaluation). It is important that the information has the ability to identify the individual concerned. In this regard, mere mention of an individual's name in a document would not constitute personal data, but other personal details such as contact details or department would fall within the scope of PDPA.

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

2.2.6. When is Data Considered "Personal Data"

2.2.6.1. 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.

2.2.6.2. 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.

2.2.6.3. The PDPC sets out a few of their considerations in determining personal data.

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

(a) 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, the 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.

(b) In general, the PDPC will apply a "practicability" threshold in determining whether the Organisation is likely to have access to other data that will identify an individual. As such, the 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.

2.2.6.3.2. Nature of data

(c) 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.

2.2.6.3.3. Purpose of the dataset or document

(d) 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. Such as customer database which includes extracts compiled in a document or communications content to name/blacklist specific individuals. Situations when it is not considered as personal data includes content of email messages where the content is not intended to convey additional information about an individual and private communications (e.g. WhatsApp messages and chats).

2.2.7. Generally, the types of personal data that the Organisation handles include, for example:

(a) data about an employee such as salary or work appraisal;

(b) customer details such as names, phone numbers or addresses;

(c) data relating to policies and claims; and

(d) data provided to third parties including other insurers or business partners.

2.2.8. 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;

(b) Personal data about a deceased individual who has been dead for more than 10 years[1]; and

[1] *For personal data about a deceased individual who has been dead for 10 years or less, PDPA applies to a limited extent. For such personal data, only the provisions relating to the disclosure and protection of personal data will apply.*

2.2.9. Note that corporate bodies and other entities are not considered natural persons and so PDPA does not provide protection for data relating to corporate bodies and other entities. However, as corporations engage in dealings through their employees, when dealing with corporations, it is likely that the Organisation will come into possession of the personal data of an individual in that corporation who serves as the contact point. Personal data that may be collected in this context could include name, designation, business telephone number, business address, business email address, business fax number etc. Where such personal data is not provided by the individual solely

for his personal purposes, such personal data would be considered business contact information ("BCI"). BCI is exempted from the application of the data protection provisions. Further elaboration on the BCI exemption is elaborated upon separately in this Handbook at [**1.1.1**].

2.3. PDPA Obligations Applicable to Personal Data

2.3.1. Where the Organisation is in possession or control of personal data, it will be required to adhere to the following 11 main obligations of PDPA:

(a) Consent obligation;

(b) Purpose Limitation obligation;

(c) Notification obligation;

(d) Access and Correction obligation;

(e) Accuracy obligation;

(f) Protection obligation;

(g) Retention Limitation obligation;

(h) Transfer Limitation obligation;

(i) Accountability obligation;

(j) Data Breach Notification obligation; and

(k) Data Portability* (This will take effect when the Regulations are issued.)

2.3.2. The Organisation's policies on the abovementioned data protection principles are set out in the sections below.

2.4. The DNC Obligations

2.4.1. Where the Organisation intends to send marketing messages to Singapore telephone numbers via voice/phone calls, SMS/MMS (text messages) or fax, the Organisation will also be required to comply with the provisions relating to the DNC regime. The Organisation's policies for compliance with the DNC regime are set out separately in the Organisation's DNC Policy.

2.5. Critical Data and Personal Data (Ref: Singlife's Data Risk Governance Framework)

2.5.1. In the Organisation, the scope of data is vast, therefore Singlife Data Risk Governance Framework has introduced a method for prioritising the most critical data, so that focus on applying the framework can be simply achieved flexibly through effective prioritisation according to current business conditions, risks and appetite.

2.5.2. All data must be classified as either critical or non-critical data. Critical data, including personal data, must be properly safeguarded and used only for authorized purposes.

2.5.3. Critical Data has been clearly defined as 'Confidential' or 'Secret' data (classified in accordance with the Group's Information Classification Document) with the potential of Moderate, Major and Very Severe impact of financial loss/misstatement, conduct and reputation loss as well as operational

disruption in the event of loss or unauthorized access to such data per the Integrated Assurance Framework ("IAF").

2.5.4. Personal Data is a personal information or personally identifiable information ("PII"). Personal Data is a sub-set of Critical Data. Please see the definition of "Personal Data" at paragraph [**2.2.1**].

3. THE CONSENT OBLIGATION

3.1. Introduction

3.1.1. This section provides details on the Consent Obligation outlined above that must be considered with regard to personal data collected, used or disclosed by the Organisation. **ALL EMPLOYEES AND ADVISERS ARE TO ADHERE STRICTLY TO THE METHODS OF COMPLIANCE AS SET OUT OR REFERRED TO IN THIS SECTION.**

3.1.2. Under PDPA, the Organisation must obtain the consent of the individual before collecting, using or disclosing his personal data for any purpose, and such consent must be obtained prior to such collection, use or disclosure.

3.1.3. The collection, use or disclosure of personal data without consent is only lawful if the collection, use or disclosure falls under an exception in the First Schedule or Second Schedule of PDPA respectively, or is required or authorized under any other written law. When in doubt, the practice should be to always obtain consent of the individual prior to collecting, using or disclosing his personal data.

3.2. Express Consent

3.2.1. Express consent is where the individual actively communicates his consent. For example, where an individual ticks a box on a form stating that he consents to the collection, use or disclosure of his personal data, this consent would be express.

3.2.2. The Organisation's policy is that express consent should be obtained.

3.2.3. Employees and advisers are to follow the practices set out in **Annex A** which set out the company's policies with regard to obtaining consent and how individuals are to communicate their express consent.

3.2.4. **EMPLOYEES AND ADVISERS ARE TO FOLLOW THE INSTRUCTIONS AND/OR PRACTICES IN ANNEX A CLOSELY TO ENSURE THAT INDIVIDUALS ARE PROVIDED WITH SUFFICIENT INFORMATION ON THE PURPOSES FOR ANY INTENDED COLLECTION, USE OR DISCLOSURE OF THAT INDIVIDUAL'S PERSONAL DATA, PRIOR TO OR AT THE TIME OF OBTAINING THAT INDIVIDUAL'S CONSENT.**

3.3. Written Consent

3.3.1. Under PDPA, when intending to collect, use or disclose personal data, individuals must be provided with the means to expressly indicate their consent. As a matter of best practice, consent should be obtained in writing and in a manner that is accessible in case it is required for reference in the future.

3.4. Failure to Opt Out

3.4.1. There are various methods of obtaining consent from an individual for the collection, use and disclosure of his personal data for a specified purpose. The Organisation's default position is that consent must be obtained expressly by way of an "opt-in" process.

3.4.2. The PDPC has further recommended that the Organisation obtains an individual's consent through a positive action of the individual, rather than relying on inaction. This is due to the risk that an opt-out process may not be sufficient to satisfy the Notification Obligation and the Consent Obligation.

3.5. Obtaining Consent from a Person Validly Acting on Behalf of an Individual

3.5.1. Consent may also be given, or deemed to have been given, by any person validly acting on behalf of an individual for the collection, use or disclosure of the individual's personal data. Such individuals may be minors, deceased persons or persons who lack the mental capacity to give consent. In such situations, the consent of the person validly acting on behalf of the individual is no different from the consent of the individual himself.

3.5.2. 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.

3.5.3. Please note that the Organisation's default position is that as far as possible, consent should be obtained directly from the individual whose personal data is being collected. If another individual is providing consent on behalf of another individual, then additional precaution should be taken. Refer to **Annex B** for further information on the obtaining of consent from another person validly acting on behalf of another individual.

3.6. When Consent is Not Validly Given

3.6.1. Consent as a prerequisite

3.6.1.1. Under PDPA, consent is only valid if it is freely given. The Organisation cannot require the individual to consent to the collection, use or disclosure of his personal data as a condition of providing a product or service where such collection, use or disclosure of the personal data is beyond what is reasonable to provide the product or service to that individual.

3.6.1.2. For example, where standard terms and conditions are issued to the individual pursuant to the provision of certain products or services, such terms and conditions should not require the individual to consent to the collection, use or disclosure of their personal data for purposes which are not integral to provide that product or service. Such terms and conditions which are not integral for the provision of the product or service should be contained in a separate portion or a separate form where the individual is given the option to provide his consent. Be sure to check to make sure that the individual is aware of this portion/form. When collecting personal data through a form, it is good practice 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. Should the individual decide to withhold consent for these purposes, you must not verbally or otherwise suggest that the product/service cannot otherwise be provided.

3.6.1.3. For example, where an individual provides his personal data for the purposes of signing up for a travel insurance policy, the Organisation cannot require that he consent to the collection, use or disclosure of his personal data for the Organisation's marketing purposes. Consent for such marketing purposes is not integral for the provision of the travel insurance policy.

3.6.1.4. Where marketing to the individual is not integral to the provision of the goods or service for which the individual seeks to be provided with, the Organisation must separately obtain the consent of the individual to collect, use or disclose his personal data for marketing purposes. This means that consent for collecting, using or disclosing the individual's personal data for marketing purposes cannot be contained in the terms and conditions, where such terms and conditions do not allow the individual the option to opt out.

3.6.2. Consent as a result of false or misleading information

3.6.2.1. Take note that consent will also be invalid where it is given as a result of false or misleading information or has been obtained through deceptive or misleading 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. Thus, all employees and advisers will need to ensure that they do not misrepresent, mislead or provide false information whenever consent is being obtained from individuals.

3.7. Obtaining Personal Data from Third Party Sources with the Consent of the Individual

3.7.1. There are two situations in which the Organisation 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"):

(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

3.7.2. An example is 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 In these situations, no such collection should be engaged in unless the employee or adviser is satisfied that the party providing the personal data has obtained the consent of the individual to disclose his personal data to the Organisation for the specified purpose(s). For advisers who are receiving leads from third parties please ensure that the existing **Client Referral Form** is completed and signed by the third parties. Please refer to the Docushare under **PIAS Resource Library > Forms > PDPA forms > Consent from Prospects Listing folder for a copy of the form.

3.7.3. The 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), It should also exercise appropriate due diligence to check that valid consent has been obtained/given.

3.7.4. Warranties or contractual obligations requiring third parties to obtain the individual's consent prior to disclosing personal data to the Organisation should be included in contracts with such third parties. When in doubt, the employee or adviser should always approach the individual himself to obtain consent.

3.7.5. The situation may also arise where the Organisation is providing a service to another organisation and such service requires the disclosure of personal data by that other organisation to the Organisation. In such a situation where the Organisation is the data intermediary, employees and advisers should aim to satisfy themselves that the disclosure by the other organisation to the Organisation is within the purposes for which the individual gave his consent to that organisation. This can also be achieved by including contractual obligations or undertakings in the contracts with such other organisations. For more details of a Data Intermediary, please refer to Section **[12.5].**

3.8. Disclosing Personal Data to Third Parties

3.8.1. Where the Organisation intends to disclose personal data to third parties, it must obtain the consent of the individual for the disclosure of his personal data by the Organisation to the third party for specified purpose(s). The purpose(s) must be notified to the individual.

3.8.2. Such consent should be recorded, alongside the identity of the third party to whom the personal data was disclosed and the purposes for which such disclosure was made. For advisers who are disclosing client's personal data to a Referral Service Partner, please use the existing **Client Referral Services Consent Form** to ensure consent is obtained prior to disclosure. Please refer to the Docushare under **PIAS Resource Library > Forms Listing for a copy of the form.

3.8.3. Where an employee or adviser is aware that personal data collected from an individual is being disclosed to a third party without that individual's consent and the exceptions as set out in [**3.9**] does not apply, **THE EMPLOYEE OR ADVISER MUST NOTIFY THE DATA PROTECTION OFFICER IMMEDIATELY**.

3.9. Exceptions to the Consent Obligation

3.9.1. The Organisation may collect, use or disclose personal data without the individual's consent in circumstances that fall within the scope of the exceptions listed in the First Schedule or Second Schedule of PDPA, respectively.

3.9.2. If the Organisation disclose personal data to third party without the individual's consent as set out in the First Schedule and Part 3 of the Second Schedule of PDPA, the Organisation has to be made aware of the purpose of collection of personal data by the third party and is required to determine if the disclosure of the data is in accordance with PDPA.

3.9.3. Take note that as with the general nature of exceptions, these are to be construed narrowly. When in doubt on whether an exception under PDPA applies, contact the Data Protection Officer.

3.10. Dealing with Corporate Clients

3.10.1. The Organisation need not abide by the data protection obligations when dealing with personal data where the personal data constitutes Business Contact Information ("BCI").

3.10.2. Further information about BCI:

3.10.2.1. PDPA defines BCI as: "An individual's name, position name or title, business telephone number, business address, business electronic mail address or business fax number and any other similar information about the individual, not provided by the individual solely for his personal purposes."

3.10.2.2. The definition of BCI is dependent on the purpose for which such contact information may be provided by an individual as it recognizes that an individual may provide certain work-related contact information solely for personal purposes. This would be required to comply with the Data Protection Provisions. In most instances, information that is provided on an individual's business card is likely to be considered as business contact information. It is also likely to include contact information on other forms of communication sent by individuals in the context of business transactions such as email signatures.

3.10.2.3. However, do note that in certain situations, the personal data that is typically considered as BCI (e.g. personal data on name cards) may fall within the scope of PDPA. This will be where the BCI is provided solely for personal purposes.

3.10.2.4. The Organisation will not be required to comply with the obligations under Parts 3 to 6A of PDPA with regard to BCI, except where it is otherwise expressly referred to. Currently, such reference is limited only to the obligation to provide the BCI of (1) the Organisation's Data

Protection Officer or his delegation and (2) on request from an individual, a representative from the Organisation who can answer questions on the collection, use or disclosure his personal data.

3.10.2.5. If you are not sure about whether personal data falls within the scope of BCI, please contact the Data Protection Officer.

3.10.3. When dealing with corporate clients (i.e. customers who are corporations), you must be mindful that you are dealing with employees of the corporate client. Personal data of such employees may not always be BCI. This will be where the BCI is provided solely for personal purposes

3.10.4. Where personal data of employees of corporate clients is BCI, you would not be required to handle the BCI in accordance with the data protection obligations. Refer to [**3.10.1**] for further elaboration on BCI. In relation to the consent obligation, you need not seek prior consent from the individual to collect, use and disclose his personal data where such personal data constitutes BCI. You also do not need to seek a warranty from any third party that may be providing you with an individual's personal data, that such third party has the authority to provide you such personal data and has obtained the requisite consent of the individual for the collection, use and disclosure of his personal data.

3.10.5. Where personal data collected from employees of a corporate client is not BCI, you must abide by all the data protection principles under PDPA. You will therefore need to seek consent from the individual to collect, use and disclose his personal data prior to or, at the very latest, at the time of the collection of the individual's personal data. The same requirements in relation to requiring a warranty from a third party where such third party is providing you with the employee's personal data would also apply. This situation may arise where the company is the one providing you with the personal data of its employees. Be sure to request and keep a record for a warranty by using the **Undertaking for Corporate Employee Benefits Form**. Please refer to the Docushare under **PIAS Resource Library > Forms > PDPA forms > Consent from Prospects Listing folder for a copy of form.

3.11. Withdrawal of Consent

3.11.1. An individual who has previously consented to the collection, use or disclosure of his personal data for notified purposes can withdraw his consent at any time upon giving reasonable notice.

3.11.2. As a general rule of thumb, a withdrawal notice of at least ten (10) business days from the day the organisation receives the withdrawal notice is considered to be of a reasonable notice by the PDPC. Should the 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.

3.11.3. The Organisation must not be seen to restrict, prevent or otherwise prohibit an individual from withdrawing his consent to the collection, use and disclosure of his personal data. Rather, PDPA requires the Organisation to have in place an internal policy to deal with notifications of such withdrawal of consent. Even in the case of the Organisation requiring certain personal data from the individual in order to fulfill a contract (e.g. to collect, use and disclose an individual's name, address and contact number to effect the delivery of products purchased from the Organisation), the Organisation is not allowed to stipulate, as a term of the contract, that the individual cannot withdraw consent to the collection, use and disclosure of his personal data for purposes of the contract. However, PDPA makes clear that if the individual subsequently withdraws consent to the collection,

use and disclosure of his personal data such that it is impossible for the organisation to fulfill the contractual obligations, any legal consequences arising out of such withdrawal would not be affected.

3.11.4. The Organisation is advised to make an appropriate consent withdrawal policy that is clear, easily accessible and flexible to enable and facilitate individuals from withdrawing their consent. For instance, providing sufficient information to individuals as to how they may withdraw their consent, or distinguishing between purposes necessary and optional to the provision of the products/services to allow individuals to withdraw consent for optional purposes without concurrently withdrawing consent for the necessary purposes.

3.11.5. Upon receiving notice of an individual's withdrawal, PDPA requires the Organisation to do the following:

(a) inform the individual of the consequences of his withdrawal of consent (it could simply be that the Organisation will stop collecting, using and disclosing his personal data or it could be that the Organisation would no longer be able to provide the product or service to him);

(b) cease collecting, using or disclosing the individual's personal data for the purposes for which consent was previously provided, unless such collection, use or disclosure without consent falls under an exception in PDPA or is authorised by any other written law; and

(c) where the Organisation ceases to collect, use or disclose the individual's personal data as above, the Organisation must also cause all of its data intermediaries and agents to cease processing the personal data as well.

3.11.6. Except for its data intermediaries and agents, note that the 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. However, as the withdrawal does not affect the individual's rights to access his personal data in the possession or control of the Organisation, the individual may request information about the ways in which his personal data may have been disclosed by the Organisation. The individual may then withdraw consent from such organisations directly.

3.11.7. The Organisation's policies and practices to be followed in processing withdrawals of consent are set out in **Annex C**. Please refer to the Docushare under **PIAS Resource Library > Forms > PDPA forms Listing folder for a copy of the **Withdrawal of Consent Form**.

4. PURPOSE LIMITATION OBLIGATION AND NOTIFICATION OBLIGATION

4.1. Introduction

4.1.1. The 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 where applicable, that the individual concerned has been informed of by the Organisation.

4.1.2. Where consent has been obtained from an individual for the collection, use or disclosure of his personal data for reasonable purposes which have been notified to him, fresh consent must be sought from the individual to use or disclose his personal data for a purpose different from the original purpose for which he consented to his personal data being collected, used or disclosed.

4.1.3. On or before collecting, using or disclosing personal data, the Organisation must notify the individual of the purposes for which it intends to collect, use or disclose his personal data. The Organisation must be aware of the purposes for which personal data is being collected, used or disclosed and must only collect, use or disclose personal data which is consistent with those purposes. Where it is unclear if the collection, use or disclosure of personal data is consistent with such purposes, contact the Data Protection Officer for further clarification.

4.1.4. On request by the individual, the Organisation must inform the individual the BCI of a person who is able to answer on behalf of the Organization the individual's questions about the collection, use or disclosure of the personal data. In the Organisation's context, please contact the Data Protection Officer.

4.2. Form of Notice of Purpose

4.2.1. PDPA does not prescribe a specific manner or form for the notification to be provided to individuals. The Organisation is free to provide the notification in any manner and form so long as it is able to provide the individual with the necessary information to understand the purposes for which his personal data is being collected, used or disclosed.

4.2.2. As a matter of best practices, the notification should be in written form. Note however that 'written form' is not limited to documentary form (i.e. paper) and can include notification in electronic format such as through including it on websites/web pages through which individuals may sign up for services or register accounts.

4.2.3. The notification should be reviewed and regularly updated so as to ensure that the list of purposes which are notified to the individual remain relevant to the Organisation's requirements. The manner in which the notification is provided should also be reviewed to ensure that it is suitable bearing in mind the circumstances and manner in which personal data is being collected, the amount of personal data being collected, the frequency at which personal data is collected and the channel through which the notification is provided (Example: face-to-face or through a telephone conversation).

4.3. Consent Clause to include Purpose Notification At or Prior to the Point of Collection of Personal Data

4.3.1. PDPA requires that individuals be made aware of the purpose(s) for which their personal data is being collected, used and disclosed. Any consent obtained from an individual in relation to the collection, use or disclosure of his personal data must be in relation to purposes which have been specified to the individual. All forms or standard templates used to obtain consent from an individual

must be amended to include a notification of the purposes for which the personal data is to be collected, used or disclosed.

4.3.2. As a matter of best practices, the consent clause should include lines such as "I confirm that I have read, understood and agree to be bound by the terms of PIAS's Personal Data Protection Policy (which may be found on (https://www.proinvest.com.sg/pdpa) as may be amended, supplemented and/or substituted by PIAS from time to time, and confirm that I am aware that the latest version of such terms (amended, supplemented and/or substituted version) will be posted on PIAS's website and such version shall bind me upon posting and/or where I continue to use the relevant services offered by PIAS to which such terms relate to."

4.3.3. Where you intend to disclose personal data to third parties you must also inform the individual of the purposes for which that third party intends to collect, use or disclose the personal data you will be providing to it. Seek written communication from the third party as well as a brief elaboration of the purposes and activities for which it requires the personal data. By doing so you will gain a better understanding of what you need to notify the individual of.

4.3.4. As part of the Organisation's effort to be PDPA compliant, new forms and clauses with the relevant purpose notification have already been incorporated or are in the process of being incorporated into all relevant business processes. **ALL ADVISERS/ EMPLOYEES ARE TO ENSURE THAT THEY ADHERE STRICTLY TO USING THE FORMS AND/OR CLAUSES PROVIDED**.

4.3.5. Please note that you are not to make any amendments to any forms or standard templates used. Should you be of the view that the purpose notification included in the forms and standard templates does not adequately encompass the purposes for which your department collects, uses or discloses personal data, please inform the Data Protection Officer.

4.4. Exceptions to Notification Obligation

4.4.1. The Organisation is required to notify individuals of the purposes for the collection, use or disclosure of their personal data unless the Organisation is collecting, using or disclosing the personal data without the individual's consent in the circumstances specified in the First Schedule or Second Schedule of PDPA.

5. ACCESS AND CORRECTION OBLIGATION

5.1. Introduction

5.1.1. This section provides details on the Access and Correction Obligations that 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 the Organisation, and the corresponding obligations of the Organisation to provide access to, and correction of, the individual's personal data. Access and Correction Obligations operate together to provide individuals with the ability to verify their personal data held by the Organisation.

5.1.2. 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 organization pursuant to a contract which is evidenced or made in writing. Please refer to Section [**12.5]** for the explanation of the concept of a Data Intermediary,

5.1.3. While the Organisation may provide standard forms or procedures for individuals to submit access and/or correction requests, the Organisation should accept all requests made in writing and sent to the BCI of its DPO or left at or sent by pre-paid post to the registered office, where sufficient information has been provided for the Organisation to meet the requests.

5.2. Access Obligation

5.2.1. Under PDPA, on request of an individual, an organization must, as soon as reasonably possible, provide the individual with:

(a) personal data about the individual that is in the Organisation's possession or under the Organisation's control; and

(b) information about the ways in which the personal data mentioned in paragraph (a) has been or may have been used or disclosed by the organisation within a year preceding the date of the request.

5.2.2. The Organisation must respond to each request made to it on or after 1 February 2021 as accurately and completely as necessary and reasonably possible.

5.2.3. Such requests apply to personal data held in both paper files and electronically, and will include personal data contained in any internal reports (including the comments or observations of the employee preparing the report). Access requests also apply to personal data of the requesting individual captured in unstructured forms such as personal data of that individual contained/embedded in emails. These access requests must be dealt with in a fair and prompt manner. Amendments or deletions must not be made to data as a result of a subject access request having been received from an individual.

5.3. Dealing with Access Requests

5.3.1. Individuals have the right to be given a description of personal data that is in the possession or control of the Organisation and information about the ways in which such personal data have been or may have been used or disclosed by the Organisation within a year before the date of the individual's request, including:

(a) the purposes for which the personal data is collected, used or disclosed;

(b) the recipients of the personal data to whom the personal data was disclosed. The Organisation is required to specify and identify the actual third-party recipient to whom the requesting individual's personal data had been disclosed. For example, instead of stating that you disclosed the individual's personal data to a certain category of third parties, you must state that disclosure is in fact to Company ABC Pte Ltd (i.e. identify the company to whom the personal data had been disclosed to); and

(c) information comprising the personal data.

The Organisation's response to an access request must take into account any personal data which is in the possession of the Organisation's data intermediaries. In responding to an access request, the Organisation is required to provide the individual access to the complete set of personal data requested by the individual which is in the Organisation's possession or under its control.

5.3.2. The Organisation must provide an applicant access to the applicant's personal data requested on or after 1 February 2021 –

(a) by providing the applicant with a copy of the personal data and use and disclosure information in documentary form;

(b) if sub-paragraph (a) is impracticable in any particular case, by allowing the applicant a reasonable opportunity to examine the personal data and use and disclosure information; or

(c) in any other form requested by the applicant as is acceptable to the Organisation.

5.3.3. As a matter of good practice, the Organisation does not allow disclosure of personal information via telephone. All reply to the individual has to be in writing.

5.3.4. The access request made by an individual must also be in writing and must include sufficient detail to enable the Organisation, with a reasonable effort, to -

(a) identify the applicant making the request;

(b) identify, in relation to an access request, the personal data and use and disclosure information requested by the application; and

(c) ensure that, in relation to an access request made by a third party on behalf of an individual, the third party has the legal authority to validly act on behalf of the individual.

5.3.5. When dealing with a request, the Organisation must be aware of the potential conflict between the individual's right of access and a third-party individual's rights to privacy or confidentiality, including a third party who is the source of that personal data. In such a scenario, the Organisation is obliged to disclose as much information as possible to the extent that the identity of the third party is not disclosed. This may necessitate the appropriate deletion or redaction of names or other identifying particulars from the information. However, be aware that this may be inadequate in circumstances where the identity of the third party is apparent from the context of the information. In such a scenario, please contact the Data Protection Officer before taking any action or disclosing any information to the individual.

5.3.6. If you receive any access enquiries from any individual, please inform the individual to contact DPO at pias.dataprotection@singlife.com.

5.3.7. A reasonable fee may be charged for processing an access request. The quantum of this fee will be limited only to the extent of the costs incurred at a marginal or incremental level, that are proportionate to the time and effort spent by the Organisation to respond to the request. It is important to ensure such fee cannot be profit oriented and the quantum of the fee charged is within the scope of the guidance provided above because a disproportionate fee quantum may be grounds for a complaint to the PDPC.

5.3.8. Before a fee can be charged, the Organisation must provide the individual with a written estimate of the fee and if the Organisation wishes to charge a fee that is higher than the written estimate provided, the Organisation has to notify the applicant in writing of the higher fee. The Organisation should also inform the individual of relevant details dealing with such fee such as accepted modes of payment and payment processing time. The Organisation is not required to respond to an access request unless the individual agrees to pay the fee.

5.3.9. The request must be complied with promptly and in any case within thirty (30) days of receipt of:

(a) the fee; and

(b) upon the provision of sufficient information to enable the Organisation to identify the individual and the personal data being sought.

Where a request cannot be complied with within the above time frame, the Organisation would have to inform the individual in writing of the reasonably soonest time in which the Organisation will respond. The Organisation may also require a deposit from the individual, as determined by the Organisation, so long as such a deposit does not exceed the total estimated fee required from the individual.

5.3.10. When an access request cannot be fulfilled, the Organisation shall respond to the individual providing the reason for rejection.

5.3.11. 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.

5.3.12. Note that where a vague or undefined request is made (for example a request along the lines of "please provide a copy of all personal data you have about me"), in certain circumstances it is permitted to request that individual to provide more specific information, such as the range of dates upon which emails were exchanged between the individual and the Organisation, which will help narrow the search for copies of personal data of the individual. The Organisation would not be obliged to comply with the request until it was supplied with such further information requested.

5.3.13. As a result of the Access Obligation under PDPA, the Organisation must implement and adhere to policies in relation to responding to access requests by individuals. Access requests can be made by an individual at any time, for any number of times.

5.3.14. If the personal data requested by the individual can be retrieved by the individual himself, the Organisation may inform the individual how he may retrieve the data requested.

5.3.15. Information which may assist the Organisation in responding to an access request may include:

(a) the categories and extent of personal data held of each individual;

(b) where such personal data is kept or stored within the Organisation or on the Organisation's behalf;

(c) the ways in which the personal data is used or disclosed;

(d) the identity of any data intermediaries who process personal data on the Organisation's behalf, as well as the personal data that such data intermediaries process and the purposes for such processing;

(e) the identity of any instructing organisation on whose behalf the Organisation processes personal data, as well as the personal data that the Organisation processes on its behalf and the purposes for such processing; and

(f) whether the individual's personal data has been destroyed and maintaining records of the same which provide details of what has been destroyed and on what date the destruction has taken place.

5.3.16. Please note that the above list is neither exhaustive nor meant to be taken as an obligation to record the particular information identified.

5.3.17. For the procedure to follow when an access request is received, please refer to **Annex D**. Please refer to the Docushare under **PIAS Resource Library > Forms > PDPA forms Listing folder for a copy of the Access Request Form.

5.3.18. Exceptions to the Information to be Provided in response to an Access Request

5.3.18.1. Please refer to Section 21 or the Fifth Schedule of PDPA for a list of exceptions where the Organisation is excluded from complying with the Access Obligation.

5.3.18.2. The Organisation must not provide the individual with the individual's personal data or other information if the provision of that personal data or other information could reasonably be expected to:

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

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

(c) reveal personal data about another individual;

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

(e) be contrary to the national interest.

Where (c) and (d) does 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.

5.3.18.3. The Organisation must not inform the individual that the Organisation has disclosed personal data about the individual to a prescribed law enforcement agency if the disclosure was made under PDPA or any other written law without the individual's consent.

5.3.19. As with the general nature of exceptions, **DO NOT RELY ON ANY OF THE EXCEPTIONS SET OUT ABOVE BEFORE CONTACTING THE DATA PROTECTION OFFICER**.

5.3.20. Preservation of Copies of Personal Data stemming from Access Request

5.3.20.1. While processing an access request

5.3.20.1.1. If the Organisation refuses to provide the personal data, the Organisation should preserve a complete and accurate copy of the personal data.

5.3.20.1.2. If the Organisation has scheduled periodic disposal or deletion of personal data, the Organisation is to identity 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.

5.3.20.1.3. However, the Organisation should not unnecessarily preserve personal data "just in case" to meet possible access request and should not retain personal data indefinitely unless there is a business or legal purpose to do so.

5.3.20.2. After rejecting an access request

5.3.20.2.1. If the Organisation rejects an access request, it should continue to preserve the requested personal data for a reasonable period (minimally 30 days) after rejecting the request.

5.3.20.2.2. In the event the individual submits an application to the PDPC to review the Organisation's rejection of the access request, the Organisation should continue to preserve the requested personal data until PDPC's review is concluded and any right of the individual to apply for reconsideration and appeal is exhausted.

5.4. Correction Obligation

5.4.1. Under PDPA, any individual may request the Organisation to correct an error or omission in the individual's personal data that is in the Organisation's possession or under its control. Further to such a request, the Organisation shall:

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

(b) send the corrected personal data to every other organisation(s) to which the personal data was disclosed by the Organisation within a year before the date the correction was made, unless:

(i) those other organisation(s) do(es) not need the corrected personal data for any legal or business purpose; or

(ii) the Organisation has the consent of the individual to only send the corrected personal data to specific organisations to which the personal data was disclosed within a year before the date the correction was made.

5.4.2. As with access requests, correction requests will apply both to personal data held in paper files and electronically, and will include personal data contained in any internal reports, unless an exception under the Sixth Schedule of PDPA applies (for example, if the personal data relates to opinion data

kept solely for an evaluative purpose). These correction requests must be dealt with in a fair and prompt manner.

5.5. Notification of Correction Requests by Other Organisations

5.5.1. The Organisation may also in turn, receive correction requests from other organisations who have disclosed personal data to it. Where such a request has been received, the Organisation should correct the personal data in its possession or control accordingly, unless the Organisation is satisfied on reasonable grounds that the correction should not be made (see [**5.7**] below). For the avoidance of doubt, the Organisation does not have to in turn, send corrected personal data received through such correction requests from other organisations, to other organisation(s) to whom the Organisation has disclosed personal data.

5.6. Dealing with Correction Requests

5.6.1. The correction request made by an individual must be in writing and must include sufficient detail to enable the Organisation, with a reasonable effort, to identify -

(a) the applicant making the request; and

(b) in relation to a correction request, the correction requested by the applicant.

5.6.2. When acting on correction requests received by the Organisation, the Organisation will first have to determine whether any of the exceptions as set out in [**5.7**] below apply. Only if the Organisation determines that none of the exceptions apply should it then proceed to correct not only the personal data in its possession or control but also make preparations to send the corrected personal data to every other organisation to which the personal data was disclosed to within a year before the date of the correction request.

5.6.3. The Organisation must ensure that such other organisations receiving the corrected personal data do indeed require the corrected personal data for any legal or business purpose. In the event that the Organisation determines that any of these organisations do not require the corrected personal data for a legal or business purpose, then the Organisation will not be required to send the corrected personal data to such organisations.

5.6.4. Where the Organisation does not correct personal data pursuant to a correction request received from an individual or from another organization because the Organisation is satisfied that there are reasonable grounds for a correction not to be made as set out at paragraph **[5.7.1.(a)]**, the Organisation must annotate the personal data in its possession or under its control indicating the correction was requested but not made. As a matter of best practice, the Organisation may also wish to annotate the reasons and explain to the individual why the Organisation has refused the correction request.

5.6.5. For the avoidance of doubt, no annotation is required where the Organisation does not make any correction on the basis of any of the other grounds set out at paragraph from **[5.7.1(b) to (h)]**.

5.6.6. Pursuant to the requirements of PDPA, once the Organisation receives a correction request from an individual, the Organisation shall correct the personal data as soon as practicable and in any event, no later than thirty (30) calendar days from the time the request is made. The Organisation would need to complete the matters set out at paragraph [**5.4.1**] above.

5.6.7. Where a request cannot be complied with within the above 30-days' time frame, the Organisation would have to within the said 30-days' time frame inform the individual in writing of the soonest practicable time in which the Organisation will make the correction.

5.6.8. Should the Organisation fail to act upon the correction request or should such correction request be somehow overlooked by the Organisation, it would amount to a breach of PDPA. Note that the Organisation is not permitted to impose a charge or fee on the requesting individual for the correction of personal data or for dealing with this correction principle and obligation.

5.6.9. Please refer to **Annex E** for the process for approaching and responding to a correction request which includes the annotation process. Please consult your Data Protection Officer when in doubt on how to respond to a correction request. For existing clients who wish to update their personal data, please refer to the DocuShare under **PIAS Resource Library > Forms > PDPA forms > Consent from Existing Clients Listing for a copy of the Personal Data Update Form.

5.7. Exceptions to the Information to be Provided in response to a Correction Request

5.7.1. The Organisation is free to refuse to correct the personal data in respect of:

(a) where the Organisation is satisfied on reasonable grounds that such correction should not be made;

(b) where the personal data to be corrected is an opinion, including a professional or an expert opinion;

(c) opinion data kept solely for an evaluative purpose;

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

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

(f) 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;

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

(h) derived personal data.

6. ACCURACY OBLIGATION

6.1. Introduction

6.1.1. The Organisation must make a reasonable effort to ensure that personal data collected by it or on its behalf 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.

6.1.2. The policy underlying this Accuracy Obligation is to ensure that the personal data collected by the Organisation which may be used to make a decision that affects the individual concerned, is reasonably correct and complete to ensure that the decision is made taking into account all relevant parts of accurate personal data.

6.2. Compliance with the Obligation

6.2.1. In order to comply with the Accuracy Obligation, the Organisation must make a "reasonable effort" to ensure that:

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

(b) the personal data it collects includes all relevant parts thereof;

(c) it has taken the appropriate 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.

6.3. Requirement of Reasonable Effort

6.3.1. The 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).

6.4. Personal Data Provided Directly by the Individual

6.4.1. Even though the Organisation may presume that personal data provided directly by the individual is accurate in most circumstances, as a matter of best practice, the Organisation should consider requiring the individual to make a verbal or written declaration that the personal data provided is accurate and complete. This could be in the form of a written undertaking contained in the various forms the Organisation provides to the individual.

6.4.2. Where the currency of the personal data is important, the Organisation should take steps to ensure that the personal data it collects, uses and/or discloses is up to date. For example, the Organisation could request for an updated copy of the individual's personal data before making a decision that will significantly affect the individual. The currency of the personal data is likely to be an issue in the scenario where the Organisation had previously collected personal data from an individual, but is now required to make a decision that affects the individual after a significant and substantial amount of time subsequent to the time of first collection.

6.5. Personal Data Provided from a Third-Party Source

6.5.1. In general, the Organisation should be more careful when collecting personal data from a third-party source compared to collecting it directly from the individual himself. In that regard, the Organisation may consider obtaining warranties from its third-party sources that such third-party sources had verified the accuracy and completeness of the personal data they are forwarding to the Organisation. Depending on the circumstances, the Organisation may also wish to consider conducting further independent verification checks on the personal data provided by such third-party sources.

6.5.2. 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.

6.6. Accuracy of Derived Personal Data

6.6.1. The PDPC recognises that the Organisation may derive personal data from the raw personal data collected either directly from the individual or from third party sources. In such cases, the Organisation 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, the Organisation should ensure that the categorisation and selection criteria (i.e. business rules) are applied accurately at the data processing stage.

6.7. Where an employee is aware, or suspect that the personal data collected is inaccurate or incomplete and attempts to verify the personal data against the customer's documents such as NRIC or proof of address or ACRA etc. have been made, **THE EMPLOYEE MUST NOTIFY THE DATA PROTECTION OFFICER IMMEDIATELY.**

6.8. Where an adviser is aware, or suspect that the personal data collected is inaccurate or incomplete and attempts have been made to either contact customer or verify against the customer's documents such as NRIC or proof of address or ACRA etc., **THE ADVISER MUST NOTIFY THE DATA PROTECTION OFFICER IMMEDIATELY.**

7. PROTECTION OBLIGATION

7.1. Introduction

7.1.1. The Organisation must protect personal data in its possession or under its control (whether in physical or electronic form) by making reasonable security arrangements to prevent (i) unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks and (ii) the loss of any storage medium or device on which personal data is stored. The Organisation is required to put in place procedures and technologies to maintain the security of all personal data, from the point of collection, to the point of destruction.

7.2. Compliance with the Obligation

7.2.1. In order to comply with the Protection Obligation, in practice, the Organisation should:

(a) design and organize 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.

7.3. In addition, the Organisation can consider undertaking a risk assessment exercise to ascertain whether their information security arrangements are adequate by considering the following factors:

(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.

7.4. Security arrangements may take various forms such as administrative measures, physical measures, technical measures or a combination of these. Examples of such measures are as follow:

7.4.1. Administrative Measures

(a) Requiring employees to be bound by confidentiality obligations in their employment agreements;

(b) Implementing robust policies and procedures (with disciplinary consequences for breaches) regarding confidentiality obligations;

(c) 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

(d) 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.

7.4.2. Physical Measures

(a) Marking confidential documents clearly and prominently;

(b) Storing confidential documents in locked file cabinet systems;

(c) Restricting employee access to confidential documents on a need-to-know basis;

(d) Using privacy filters to minimise unauthorised personnel from viewing personal data on laptops;

(e) Proper disposal of confidential documents that are no longer needed, through shredding or similar means;

(f) 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);

(g) Providing a summary of the personal data contained in storage so that personal data is accessed only when necessary; and

(h) Confirming that the intended recipient of personal data is the correct recipient to avoid undue disclosure of personal data.

7.4.3. Technical Measures

(a) Ensuring computer networks are secure;

(b) Adopting appropriate access controls (e.g. considering stronger authentication measures where appropriate);

(c) Encrypting personal data to prevent unauthorised access;

(d) Activating self-locking mechanisms for the computer screen if the computer is left unattended for a certain period;

(e) Installing appropriate computer security software and using suitable computer security settings;

(f) Disposing of personal data in IT devices that are to be recycled, sold or disposed;

(g) Using the right level of email security settings when sending and/or receiving highly confidential emails;

(h) Updating computer security and IT equipment regularly; and

(i) Ensuring that IT service providers are able to provide the requisite standard of IT security

7.4.4. Where an employee or adviser discovers or suspects that there is an unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks of the personal data or a loss of any storage medium or device on which personal data is stored, **WITHOUT UNDUE DELAY, THE EMPLOYEE OR ADVISER MUST IMMEDIATELY NOTIFY THE LINE MANAGER AND THE DATA PROTECTION OFFICER.** For more details, you may also wish to refer to Paragraph 11 on Data Breach Notification Obligation**.**

8. RETENTION LIMITATION OBLIGATION

8.1. Introduction

8.1.1. The 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 the personal data no longer serves the purpose(s) for which it was collected, and retention is no longer required for business or legal purposes. For example, through methods such as destruction, deletion and/or anonymization.

8.2. Retention Period

8.2.1. Personal data should not be kept for longer than is necessary for the purposes it serve when they were collected and where retention is no longer necessary for legal or business purposes.

8.2.2. PDPA does not specify any specific duration of time for which the Organisation may legitimately retain personal data. Rather, the duration of time for which the Organisation can legitimately retain personal data is to be determined by the Organisation based on their own specific business needs, to be 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. Note that although PDPA does not prescribe a specific retention period for personal data, the Organisation would need to comply with any legal or specific industry-standard requirements that may still apply.

8.2.3. The Organisation should consider the following factors in determining the retention periods of documents:

(a) the purpose(s) for which the personal data was collected. In particular, note that:

(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 the Organisation "just in case" it may be needed for other purposes that have not been notified to the individual concerned;

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

(i) the personal data is required for an ongoing legal action involving the Organisation;

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

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

(iv) the personal data is used for the 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.

8.2.4. Therefore, personal data held by the Organisation should be reviewed regularly and consideration given in relation to each type of data, as to how long those data will need to be kept for the relevant purposes or if at all. Where personal data is required to be kept for extensive periods of time, the reasons for such extended retention periods should be documented. The Organisation may also have to implement varying retention periods for the different types of personal data as appropriate.

8.2.5. All financial institutions in Singapore are required to keep the documents for:

8.2.5.1. A period of at least 5 years following the termination of business relations for customer identification information, and other documents relating to the establishment of business relations, as well as policy files and business correspondence; and

8.2.5.2. A period of at least 5 years following the completion of the transaction for records relating to a transaction, including any information needed to explain and reconstruct the transaction.

8.2.6. The Organisation's retention policy is to keep the documents, which are required by law or regulations, for 7 years where the trigger may be following the termination of business relations, the completion of the transaction or any other trigger (whichever that is applicable). This is unless otherwise specified in the Organisation's Records Retention Schedule and Disposal Schedule.

8.2.7. For any other documents/records that do contain personal data but do not fall in Paragraphs [**8.2.5**], Paragraph **[8.2.6]** and are not specified in the Organisation's Records Retention Schedule and Disposal Schedule, it should not be kept for longer than is necessary for the purposes it serve when they were collected and where retention is no longer necessary for legal or business purposes.

8.2.8. No documents/records containing personal data shall be retained beyond the retention periods stated above. To retain documents beyond its prescribed retention period based on the respective department's business or legal need, prior written approval must first be obtained from the Data Protection Officer. The approval must specify the type of document and the intended purpose for which an extension of the applicable retention period is being sought. Once the approval is granted, the employee shall indicate at or within the document the specific purpose for which the document is being retained and the estimated date of disposal or deletion or destruction for the document. The responsibility lies with the employee to ensure the disposal date is being strictly adhered to.

8.3. Retention Procedure (Physical Copies of Documents)

8.3.1. Employees and adviser shall ensure that, at the end of each day, all physical copies of documents are neatly arranged in an orderly manner and stored in the physical cabinets allocated to them. Employees and advisers shall also ensure that such physical cabinets are properly secured at the end of each day and that the keys to such physical cabinets are stored in a secure location when they leave the office premises.

8.3.2. An employee or adviser who has no operational necessity to refer to physical copies of documents on a day-to-day basis should consider archiving such documents in the following manner:

8.3.2.1. As far as possible, employees and advisers should ensure that physical copies of documents are grouped together based on similar retention periods. Once grouped, such physical copies of documents should be neatly arranged into files, separated by appropriate tabs and given appropriate labels to ensure ease of reference.

8.3.2.2. Employees and advisers shall, on an appropriate file label, provide a general description of the type of documents contained within the file, as well as provide an estimated range of the retention periods for the documents contained within the file.

8.3.2.3. Employees and advisers shall ensure that the afore-mentioned files and/or boxes are securely stored in accordance with the PIAS's guidelines.

8.3.2.4. Employees and advisers shall be responsible for indexing and/or maintaining a record of the files which have been archived.

8.4. Retention Procedure (Electronic Copies of Documents)

8.4.1. Employees and advisers must not send, upload, remove on portable media or otherwise transfer externally any information that is designated as 'Secret' or 'Confidential', or they should reasonably regard as being confidential to PIAS.

8.4.2. An employee and adviser who has no operational necessity to refer to electronic copies of documents on a day-to-day basis should consider archiving such electronic copies of documents.

8.5. Ceasing to Retain

8.5.1. The Organisation must promptly destroy or anonymize documents containing personal data as soon as the purpose for which the data was collected is no longer being served by its retention and retention is no longer necessary for legal or business purposes. The Organisation must ensure that such destruction or anonymization is carried on all of the Organisation's repositories. This includes any copies of documents which have been archived and/or stored as back-ups.

8.5.2. The Organisation will be deemed to have ceased to retain documents containing personal data when it, its agents and its data intermediaries no longer has access to the documents and the personal data they contain.

8.5.3. The Organisation may cease to retain documents containing personal data by ensuring that it (including its advisers and its data intermediaries):

(a) returns the documents to the individuals concerned;

(b) transfers the documents to another person on the instructions of the individual concerned;

(c) destroys the documents by shredding or disposing them in an appropriate manner; or

(d) anonymizes the personal data.

8.5.4. The following circumstances will NOT be deemed to be ceasing to retain documents containing personal data:

(a) Merely filing of documents in a locked cabinet;

(b) Warehousing of documents;

(c) Transferring of documents to a party who is subject to the Organisation's control; and/or

(d) Archival of electronic documents.

8.5.5. The Organisation should cease to retain documents containing personal data in a manner which renders the documents irretrievable or inaccessible to the Organisation. However, it is recognised that there are certain circumstances where the personal data would still remain within reach of the Organisation or within the Organisation's systems in some form. This may include shredded documents in the disposal bin, or deleted personal data in an un-emptied recycling bin in the computer or within the Organisation's systems. In this regard, the following factors should be considered when considering if the Organisation has ceased to retain personal data:

(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.

8.6. The 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. For more details, refer to the chapter on Anonymisation in the Advisory Guidelines on the PDPA for Selected Topics.

8.7. Disposal Procedures

8.7.1. The following processes and procedures shall be observed by all employees and advisers of the PIAS:

8.7.1.1. Regular disposal exercise to be conducted in a proper and secure manner to ensure that records/documents containing personal data are not retained in perpetuity where it does not have legal or business reasons to do so and to prevent the risk of recovery of, accidental disclosure of or unauthorized access to such records/documents. Examples include:

(a) destroy hard-copy documents by shredding or disposing using PIAS secure bin,

(b) destroy storage device by crushing, drilling or degaussing

(c) delete, erase or purge electronic records/documents, or

(d) anonymise personal data found in documents/records.

9. TRANSFER LIMITATION OBLIGATION

9.1. Introduction

9.1.1. The Organisation must not transfer personal data to a country or territory outside Singapore except in accordance with the requirements prescribed under PDPA. This is to ensure that the Organisation provide a standard of protection to personal data so transferred that is comparable to the protection under PDPA.

9.1.2. PDPA limits the ability of the Organisation 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. For further explanation of Data Intermediary, please refer to Section **[12.5].** In situations where personal data transferred or situated overseas remains in the possession or control of the Organisation, it has to comply with all the Data Protection Provisions. Such situations include where an employee travels overseas with customer lists on his notebook; the Organisation owns or leases and operates a warehouse overseas for archival of customer records; or the 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.

9.1.3. The Transfer Limitation Obligation is a manifestation of the Accountability Obligation as when the Organisation discloses personal data to another organisation, and both are in Singapore, the receiving organisation is subject to PDPA and has to protect the personal data that it thereby receives. Likewise, when the 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 the Organisation transfers personal data to another organisation that is outside Singapore, the recipient organisation is not subject to 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.

9.2. Transferring Personal Data outside of Singapore

9.2.1. Before transferring personal data outside of Singapore, the Organisation must take 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 as specified in the Personal Data Protection Regulations 2021.

9.2.2. 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 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 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 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.

9.2.3. 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 Obligation if:

(a) it is receiving the personal data as an organisation 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.

9.2.4. The Organisation's transfer of personal data outside of Singapore must be in a manner that is consistent with the Organisation's obligations under PDPA and pursuant to a legally binding instrument that contains the appropriate safeguards (i.e. contracts between the Organisation and third-party recipients or binding corporate rules for group companies). 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 PDPA, the legally binding instrument must contain provisions that implement the following obligations:

(a) Specifics:

i. In the case of the contract, specify the countries to which the personal data may be transferred under the contract;

ii. In the case of the binding corporate rules, specify the recipients of the transferred personal data to which the binding corporate rules apply; the countries to which the personal data may be transferred under the binding corporate rules; and the rights and obligations provided by the binding corporate rules;

(b) Purpose of use and disclosure:

i. The receiving organisation shall not use or disclose transferred personal data for any purpose other than the purposes specified in the instrument (and such purposes shall be consistent with the purposes for which the Organisation may use and disclose the personal data in accordance with PDPA);

ii. The receiving organisation shall only use and disclose transferred personal data in a manner and to the extent permitted in the instrument (and such use and disclosure shall be consistent with the ability of the Organisation to use and disclose the personal data in accordance with PDPA); and

iii. The receiving organisation shall limit disclosure of such transferred personal data to its employees or authorised personnel on a need-to-know basis and only for the purposes specified in the instrument;

(c) Accuracy: The receiving organisation shall make a reasonable effort to ensure that the transferred personal data in its possession or control remain or is otherwise accurate and complete, if the personal data is likely to be (i) used by the receiving organisation to make a decision that affects the individual to whom the transferred personal data relates; or (ii) disclosed by the receiving organisation to another organisation;

(d) Protection: The receiving organisation shall protect the transferred personal data in its possession or under its control by making reasonable security arrangements to prevent unauthorised or accidental access, collection, use, disclosure, copying, modification, disposal or destruction of personal data, or other similar risks; and the loss of any storage medium or device on which personal data is stored;

(e) Retention Limitation: The receiving organisation shall cease to retain its documents containing transferred personal data, or remove the means by which the transferred personal data can be associated with particular individuals, as soon as it is reasonable to assume that (i) the specified purposes are no longer being served by retention of the transferred personal data; and (ii) retention is no longer necessary for legal or business purposes;

(f) Data Breach Notification: The receiving organisation shall notify in writing as soon as reasonably practicable should it be aware of, or reasonably suspect, a data breach has occurred and shall promptly take all steps necessary to remedy the event and prevent its re-occurrence;

(g) General: The receiving organisation shall ensure that its employees, agents and sub-contractors who may receive or have access to any of the transferred personal data are aware of the obligations specified above and agree to abide by the same.

(h) Others: There should be provisions touching on the policies on personal data protection, access and correction obligations.

9.2.5. As evidenced from the above paragraphs, the transfer obligation would apply equally regardless of whether the overseas recipient is a group company or a third-party organisation. Be aware that transferring personal data out of Singapore is not limited to the physical transfer of personal data outside of Singapore. Below are some common examples of situations in which personal data may be transferred out of Singapore to group companies or a third-party organisation:

(a) internal reporting between group companies to head office. For example, a Singapore branch sending employee salary details to its head company located overseas;

(b) sending emails/letters/facsimile messages containing personal data to individuals overseas;

(c) storage of personal data in servers overseas. These may be for purposes such as backups and/or disaster recovery. The storage can be automatic or manually configured;

(d) having a common database containing personal data (where the server is hosted in Singapore) which is shared with other group companies located overseas, such that these group companies are able to access the personal data and store it locally on their servers and systems;

(e) passing physical files/documents containing personal data to persons located overseas;

(f) passing a physical storage device (such as a thumb drive, CD, hard drive etc.) containing personal data to a recipient overseas; and

(g) verbally providing personal data to a recipient of a phone call who is located overseas at the time of the call, including leaving a voice mail/recording of such personal data on a voice recording machine.

9.2.6. The obligation in paragraphs [**9.2.2] or [9.2.3**] is deemed or assumed to be satisfied in certain limited situations. As such situations are specific in nature, please consult your Data Protection Officer when:

(a) you are transferring personal data out of Singapore;

(b) there is no contract in place dealing with such transfer between the Organisation and the foreign recipient party; and

(c) you are wondering whether such transfer would fall within such limited situation. For now, one such limited situation would be where the personal data that is to be transferred out of Singapore is publicly available in Singapore – in such a case, no contract dealing with such transfer between the Organisation and the recipient party would be needed for such personal data.

9.2.7. If you are unsure whether the legally enforceable obligations or specified certifications are adequate to meet PDPA requirements prescribed, always consult the Data Protection Officer first before transferring any personal data outside of Singapore.

10. ACCOUNTABILITY OBLIGATION

10.1. Introduction

10.1.1. In data protection, the concept of accountability refers to how the Organisation discharges its responsibility for personal data in its possession or which it has control over. The Organisation is responsible for personal data under its possession which it has collected or obtained for processing or under its control.

10.1.2. Under PDPA, the Organisation must implement the necessary policies and procedures in order to meet its PDPA obligations and shall make information about its policies and procedures publicly available.

10.1.3. The Organisation must designate one or more individuals to be responsible for ensuring that the Organisation complies with PDPA. This individual is typically referred to as a Data Protection Officer (DPO).

10.2. Appointing a Data Protection Officer (DPO)

10.2.1. The individual designated by the Organisation may delegate to another individual the responsibility conferred by that designation.

10.2.2. The designation of an individual by the Organisation does not relieve the Organisation of any of its obligations under PDPA. Hence, the legal responsibility for complying with PDPA remains with the Organisation and is not transferred to the designated individual(s).

10.2.3. The designated individual(s) should be (a) sufficiently skilled and knowledgeable and (b) amply empowered, in order to discharge their duties as a DPO. The Organisation should ensure that individuals appointed as a DPO are trained and certified.

10.2.4. Ideally, the individual(s) designated by the Organisation should 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.

10.2.5. The Organisation must make available to the public the business contact information of at least one of the individuals designated by Organisation and 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.

10.2.6. 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 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.

10.2.7. The Organisation's Senior Management has appointed a trained and certified Data Protection Officer. The DPO's business contact information has been made available to the public via PIAS' corporate website at https://www.proinvest.com.sg/pdpa.

10.2.8. If any individual, including yourselves, has any concern or query on the Organisation's data protection related policies and practices, please contact the Data Protection Officer via pias.dataprotection@singlife.com.

10.3. Developing and Implementing Data Protection Policies and Practices

10.3.1. PDPA sets out four (4) additional key requirements which form part of the Accountability Obligation. In general, the 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 the Organisation manages personal data protection risks.

10.3.2. The Organisation is required to develop and implement data protection policies and practices, both internal and external facing, to meet its obligations under PDPA and must be made easily accessible to the intended reader. The Organisation 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. The Organisation should put in place monitoring mechanisms and process controls to ensure the effective implementation of these policies and practices.

10.3.3. The Organisation must develop a process to receive and respond to complaints that may arise with respect to the application of PDPA. 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.

10.3.4. The Organisation is required to staff training and communicate to its staff information about its policies and practices. Such communication efforts could be incorporated in the Organisation's 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 is sensitive and alert to data protection issues and concerns.

10.3.5. The Organisation must make information about its data protection policies, practices and complaints process available on request by applicable parties. This is to ensure that individuals are able to find the necessary information and have the means of raising any concerns or complaints to the Organisation directly.

10.3.6. On top of the 4 key PDPA requirements, the Organisation also implement and adhere to Singlife Group's Data Protection related policies such as Data Risk Governance Framework, Data Incident and Breach Management Standard, Group Privacy Policy and Group Privacy Standard etc. As a result, governance structures have been established and processes are designed to operationalise policies.

10.4. Other Provisions related to the Accountability Obligation

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

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

(b) the Organisation has to notify the PDPC and/or affected individuals when a data breach is likely to result in significant harm or is of a significant scale;

(c) the Organisation has 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 PDPC and the PDPC may review or investigate the Organisation's conduct and compliance with PDPA;

(e) the PDPC may, if satisfied that the Organisation has contravened the Data Protection Provisions, give directions to the Organisation to ensure compliance including (amongst others) imposing a financial penalty of up to $1 million (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 PDPA by the Organisation may commence civil proceedings against the Organisation.

11. DATA BREACH NOTIFICATION OBLIGATION

11.1. Introduction

11.1.1. PDPA sets out the requirements for the Organisation to assess whether a data breach is notifiable, and to notify the affected individuals and/or the PDPC 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.

11.1.2. Data breach is the unauthorized access, collection, use, disclosure, copying, modification or disposal of personal data; or the loss of any storage medium or device on which personal data is stored in circumstances where the unauthorized access, collection, use, disclosure, copying, modification or disposal of personal data is likely to occur.

11.2. Duty to Conduct Assessment of Data Breach

11.2.1. Once the Organisation has credible grounds to believe that a data breach has occurred, the Organisation is required to take reasonable and expeditious steps to assess whether the data breach is notifiable under PDPA.

11.2.2. 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 Data Breach Notification (DBN) Obligation and the PDPC can take enforcement action.

11.2.3. The Organisation should generally establish the facts of a data breach and determine whether it is notifiable within 30 calendar days. Otherwise, to be prudent, the Organisation shall be prepared to provide an explanation to the PDPC for the time taken to carry out the assessment.

11.2.4. 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. Refer to Paragraph **[11.11.]**

11.2.5. For any suspected or discovered data breaches, please refer to **Group Risk's Data Incident and Breach Management Standard** as it defines the process and expectation for all businesses to ensure the effective and consistent management of data incident and breaches and to fulfill the Data Breach Notification Obligation stipulated in PDPA.

11.3. Data Breaches within the Organisation

11.3.1. A data breach that occurs within the Organisation is not a notifiable data breach as it is contained within the Organisation.

11.4. Data Breaches Discovered by a Data Intermediary

11.4.1. 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. This ensures the organisation is informed of data breaches in a timely way, able to decide on the immediate actions to take to contain the data breach; and able to assess whether the data breach is a notifiable data breach. For further details of a Data Intermediary, please refer to Section [**12.5].**

11.4.2. 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 PDPC. 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 PDPC on its behalf.

11.4.3. As a good practice, the Organisation should establish clear procedures for complying with the DBN obligation when entering into service agreements or contractual arrangements with their data intermediaries. The agreements should consider 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 harm that may result from a data breach.

11.5. Data Breaches Involving more than one Organisation

11.5.1. 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.

11.5.2. 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.

11.5.3. Where a data breach is notifiable to the PDPC, each organisation has to notify the PDPC. As a matter of administrative convenience, the Organisations may use the same information where relevant to individually submit the notification. Where the data breach is notifiable to affected individuals, the PDPC 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 minimize confusion.

11.6. Criteria for Data Breach Notification

11.6.1. A data breach is notifiable data breach if the data breach — (a) results in, or is likely to result in, significant harm to an affected individual; or (b) is, or is likely to be, of a significant scale.

11.6.2. Significant harm to affected individuals

11.6.2.1. The Organisation is required to assess whether a data breach is notifiable as it is likely to result in significant harm 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).

11.6.2.2. 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.

11.6.2.3. Under Personal Data Protection (Notification of Data Breaches) Regulations 2021, it 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.

11.6.2.4. The personal data (or classes of personal data) prescribed include:

(a) Individual's full name or alias or full national identification number **in combination with** any of the following personal data in categories listed in (b) to (h):

(b) financial information which is not publicly disclosed

(c) Identification of vulnerable individuals

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

(e) Specified medical information

(f) Information related to adoption matters

(g) Private key used to authenticate or sign an electronic record or transaction

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

11.6.2.5. Please note that the above list is neither exhaustive nor specific. For more details, refer to Personal Data Protection (Notification of Data Breaches) Regulations 2021.

11.6.2.6. The prescribed personal data or classes of personal data, or other prescribed circumstances excludes any personal data that is publicly available and any personal data that is disclosed under any written law.

11.6.2.7. Where different categories of personal data are lost or compromised at different times, the affected Organisation must notify the PDPC 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.

11.6.3. Significant scale of breach

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

11.6.3.2. 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 PDPC, even if the data breach does not involve any prescribed personal data listed in Personal Data Protection (Notification of Data Breaches) Regulations 2021.

11.6.3.3. If the Organisation is unable to determine the actual number of affected individuals in a data breach, the Organisation should notify the PDPC 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 PDPC of the actual number of affected individuals when it is established.

11.7. Timeframes for Notification

11.7.1. Upon determining that a data breach is notifiable, the Organisation must notify the respective parties following the table below:

Party to Notify	Timeframe
PDPC	As soon as practicable but no later than 3 calendar days[1], starting from the day the Organisation makes the determination that there is a notifiable breach
Affected Individuals[2]	As soon as practicable at the same time or after notifying PDPC.
MAS	(a) Concurrently notify MAS of data breaches that are required to be notified to PDPC (b) Based on the timelines indicated within MAS Notice 127 and MAS Guidelines on Outsourcing if the data breaches meet the criteria stated within these instruments. (c) For data breaches that fall outside (a) and (b), to consolidate and notify MAS within 3 weeks from the last day of each quarter.

[1] If the Organisation notifies PDPC of the notifiable data breach after the expiry of the period specified above, the Organisation must additionally 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.

[2] If the Organisation does not intend to notify any affected individual affected by the notifiable data breach of the occurrence of that data breach, the notification to the PDPC must additionally specify the grounds for not notifying the affected individual.

11.7.2. Any unreasonable delays in notifying the relevant parties will be a breach of the DBN Obligation.

11.8. Exceptions to the DBN Obligation

11.8.1. Under PDPA, the Organisation does not need to notify the affected individuals if:

(a) on or after assessing that the data breach is a notifiable data breach, takes any action, in accordance with any prescribed requirements, that renders it unlikely that the notifiable data breach will result in significant harm to the affected individual; or

(b) had implemented, prior to the occurrence of the notifiable data breach, any technological measure that renders it unlikely that the notifiable data breach will result in significant harm to the affected individual.

11.8.2. The PDPC may, on the written application of the Organisation, waive the requirement to notify an affected individual subject to any conditions that the PDPC thinks fit.

11.8.3. The 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. For further explanation of a Data Intermediary, please refer to Section [**12.5]**.

11.8.4. Such remedial actions need not necessarily be taken before notifying the PDPC. Remedial actions (or further remedial actions) may also be taken after notifying the PDPC and receiving guidance from them. In the event that, after notifying the PDPC, 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.

11.8.5. 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.

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

11.8.7. As with the general nature of exceptions, **DO NOT RELY ON ANY OF THE EXCEPTIONS SET OUT ABOVE BEFORE CONTACTING THE DATA PROTECTION OFFICER.**

11.9. Prohibition and Waiver of the Requirement to Notify Affected Individuals

11.9.1. The Organisation is 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. The Organisation is also prohibited from notifying the affected individuals if the PDPC so directs them.

11.9.2. In addition, the PDPC may, on the written application of the Organisation, waive the requirement for the 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 where such investigations are not publicly known. This application to the PDPC to waive the requirement to notify an affected individual may be submitted together with the notification to the PDPC.

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

11.10. Mode of Notification of Data Breach

11.10.1. Where the Organisation is required to notify affected individuals of a data breach, it should ensure that the mode of notification used is appropriate and effective in reaching the affected individuals in a timely way. The Organisation may employ their regular mode of communication with the affected individuals to send the notification.

11.10.2. 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, the Organisation may determine the most efficient and effective mode of notification to inform affected individuals.

11.11. Information to be Provided in Notification of Data Breach

11.11.1. The Organisation notifying affected individuals and/or the PDPC 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. The Organisation may provide their notification on the PDPC's website.

11.11.2. Under the Personal Data Protection (Notification of Data Breach) Regulations, the notification by the Organisation to the PDPC of a notifiable data breach must include all of the following information:

(a) the date on which and the circumstances in which the Organisation first became aware that the data breach had occurred;

(b) 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 PDPA that the data breach is a notifiable data breach;

(c) information on how the notifiable data breach occurred;

(d) the number of affected individuals affected by the notifiable data breach;

(e) the personal data or classes of personal data affected by the notifiable data breach;

(f) the potential harm to the affected individuals as a result of the notifiable data breach;

(g) information on any action by the Organisation, whether taken before or to be taken after the Organisation notifies the PDPC of the occurrence of the notifiable data breach —

(i) to eliminate or mitigate any potential harm to any affected individual as a result of the notifiable data breach; and

(ii) to address or remedy any failure or shortcoming that the Organisation believes to have caused, or enabled or facilitated the occurrence of, the notifiable data breach;

(h) information on the Organisation's plan (if any) to inform, on or after notifying the PDPC of the occurrence of the notifiable data breach, 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;

(i) the business contact information of at least one authorised representative of the Organisation.

11.11.3. 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, the Organisation should notify parents or guardians of young children whose personal data has been compromised

11.11.4. Where the Organisation does not have the contact details of the child's parent or guardian, the Organisation should ensure that the data breach notification to the child is in a language that is readily

understandable by the child so that the child may understand the consequences of the data breach. The Organisation should also consider advising the child to inform his/her parent or guardian about the data breach.

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

11.11.6. Under the Personal Data Protection (Notification of Data Breach) Regulations, the notification by the Organisation to an affected individual affected by a notifiable data breach must contain all of the following information:

(a) the circumstances in which the Organisation first became aware that the notifiable data breach had occurred;

(b) the personal data or classes of personal data relating to the affected individual affected by the notifiable data breach;

(c) the potential harm to the affected individual as a result of the notifiable data breach;

(d) information on any action by the Organisation, whether taken before or to be taken after the Organisation notifies the affected individual —

(i) to eliminate or mitigate any potential harm to the affected individual as a result of the notifiable data breach; and

(ii) to address or remedy any failure or shortcoming that the Organisation believes to have caused, or enabled or facilitated the occurrence of, the notifiable data breach;

(e) the 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;

(f) the business contact information of at least one authorised representative of the Organisation.

11.11.7. The Organisation 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.

11.11.8. Where the 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 PDPC and affected individuals (if required) according to the timeframes for data breach notification under PDPA. The Organisation is not regarded to have fulfilled the DBN Obligation under PDPA just by fulfilling any other breach notification requirements set out under other written laws.

11.12. If you discover or suspect that a data breach has occurred, **PLEASE NOTIFY YOUR LINE MANAGER AND THE DPO IMMEDIATELY.**

11.13. If you are unclear on whether the case or situation constitutes as a data breach (be it notifiable or not) or you discover or suspect that a data breach has occurred, **PLEASE NOTIFY THE DPO IMMEDIATELY** at pias.dataprotection@singlife.com.

12. EXCLUSIONS & EXCEPTIONS UNDER PDPA

12.1. Introduction

12.1.1. This sub-section details the various exclusions as set out under Section 4 of PDPA.

12.1.2. **ALWAYS CLARIFY AND CHECK WITH THE DATA PROTECTION OFFICER PRIOR TO RELYING ON ANY OF THESE EXCLUSIONS**. No employee is allowed to determine on their own whether the exclusions apply to any activity relating to personal data.

12.2. Personal Data of an Individual Contained in a Record that has been in Existence for At Least 100 Years

12.2.1. The entirety of PDPA (including the DNC obligations) would not apply to the personal data of an individual where such personal data has been contained in a record that has been in existence for at least 100 years or more.

12.3. Business Contact Information (BCI)

12.3.1. The Organisation does not have to comply with Parts 3, 4, 5, 6 and 6A of PDPA with regard to any personal data that is classified as business contact information except where BCI is expressly mentioned. Please note that the DNC obligations would still apply to business contact information. For further information on how business contact information can be identified, please refer to [**3.10.2**].

12.4. Personal Data of Deceased Individuals

12.4.1. The entirety of PDPA (including the DNC obligations) would not apply to the personal data of deceased individuals who have been deceased for more than 10 years from the date of death.

12.4.2. However, if the deceased individual has been deceased for 10 years or less, then PDPA obligations would still apply but only to a limited extent. To be clear, this includes the following obligations:

(a) notification of purposes for disclosure of personal data;

(b) obtaining consent for disclosure of such personal data for the specific purposes of the disclosure;

(c) ensuring that the purpose is one which a reasonable person would consider appropriate in the circumstances;

(d) ensuring reasonable efforts have been taken that such personal data is accurate; and

(e) having reasonable security arrangements to protect such personal data.

12.4.3. When complying with their obligations under PDPA, the Organisation 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.

12.5. Data Intermediary

12.5.1. Under PDPA, a "data intermediary" refers to an organisation which processes personal data on behalf of another organisation but does not include an employee of that other organisation.

12.5.2. Under PDPA, "processing" refers to 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) organization, adaptation or alteration; (d) retrieval; (e) combination; (f) transmission; (g) erasure or destruction. Items

(a) to (g) above represent an indicative but non-exhaustive list of activities which could be considered processing.

12.5.3. If the data intermediary processes personal data on behalf of and for the purposes of another organisation pursuant to a contract which is evidenced or made in writing, PDPA obligations will apply only to a limited extent to the data intermediary. In this case, the data intermediary would be statutorily required to comply with only three of PDPA obligations; namely, the Protection, Retention and Data Breach Notification obligations. It does not need to comply with the obligations in Parts 3, 4, 5, 6 (except sections 24 and 25), 6A (except sections 26C(3)(a) and 26E) and 6B.

12.5.4. The 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 organization pursuant to a contract which is evidenced or made in writing.

12.5.5. The Organisation has the same obligations in respect of personal data processed on its behalf and for its purposes by a data intermediary as if the personal data were processed by the Organisation itself.

12.5.6. This effectively means that, in using a data intermediary, the Organisation remains primarily responsible for the actions and omissions of its data intermediary when the data intermediary is processing personal data for the Organisation. Similarly, where the Organisation is a data intermediary, then the organisation that the data intermediary is processing data for will remain primarily responsible.

12.5.7. In this regard, to protect itself, the Organisation will have to contractually impose obligations on its data intermediaries to process personal data in accordance with PDPA so as to ensure the Organisation's compliance with and to limit its liability under PDPA. It is good practice for the Organisation to undertake an appropriate level of due diligence to assure itself that a potential data intermediary is capable of complying with PDPA.

12.5.8. When engaging a data intermediary, the 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.

12.5.9. Where the 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.

12.5.10. The Transfer Limitation Obligation requires that the 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.

12.6. Requirements of Other Written Law

12.6.1. PDPA provides that in the event of any inconsistencies between PDPA and the provisions of other written law, the provisions of such other written law shall prevail, but only to the extent of the inconsistency in any provisions of Parts 3, 4, 5, 6, 6A and 6B.

12.6.2. PDPA provides that nothing in Parts 3, 4, 5, 6, 6A and 6B affects 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 is not an excuse for contravening PDPA.

12.7. Exceptions for Collection, Use and Disclosure

12.7.1. The Organisation may collect, use or disclose personal data without the individual's consent in circumstances that fall within the scope of the exceptions listed in the First Schedule and Second Schedule of PDPA.

12.8. Exceptions from Access and Correction Requirements

12.8.1. Please refer to the exceptions listed in the Fifth Schedule and Sixth Schedule of PDPA for the exceptions from access and correction requirements respectively.

12.9. Exclusion from Meaning of "Specified Message"

12.9.1. Please refer to the exclusions listed in the Eighth Schedule of PDPA.

13. OFFENCES

13.1. Offences

13.1.1. Offences under PDPA include:

(a) disposing of, altering, falsifying, concealing or destroying, or directing another person to dispose of, alter, falsify, conceal or destroy a record containing personal data or information about the collection, use or disclosure of personal data, with an intent to evade an individual's access or correction request;

(b) obstructing or hindering the PDPC, an inspector or an authorized officer in the performance of any function or duty, or in the exercise of any power under PDPA;

(c) without reasonable excuse, neglects or refuses to provide any information or produce any document which the organisation or person is required by or under the PDPA to provide or produce to the PDPC or an inspector

(d) without reasonable excuse, neglects or refuses to attend before the PDPC or an inspector as required by or under PDPA;

(e) makes a statement, or provides any information or document, to the PDPC, an inspector or an authorised officer under PDPA which the organisation or person knows, or ought reasonably to know, to be false or misleading in any material particular.

(f) knowing or reckless unauthorised disclosure of personal data;

(g) 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

(h) knowing or reckless unauthorised re-identification of anonymised information.

13.2. Penalties Relating to the Organisation

13.2.1. In relation to the offence listed in 13.1.1.(a), an organization may be fined up to $50,000.

13.2.2. In relation to the offences listed in 13.1.1.(c) and 13.1.1.(f), an organization may be fined up to $100,000.

13.2.3. In relation to contravention of Data Protection Provisions, an organization may face a financial penalty of up to $1 million or 10% of the Organisation's annual turnover in Singapore, whichever is higher.

13.3. Penalties Relating to Individuals

13.3.1. The individual may be fined up to $5,000 or to imprisonment for a term not exceeding 2 years or to both for the following offences:

(a) In relation to the unauthorised disclosure of personal data where the individual discloses, or the individual's conduct causes disclosure of, personal data in the possession or under the control of any organisation or a public agency to another person, the disclosure is not authorized by the organisation or public agency, and the individual does so (i) knowing that the disclosure is not authorised by the organisation or public agency or (ii) reckless as to whether the disclosure is or is not authorised by the organisation or public agency;

(b) In relation to the improper use of personal data, where the individual makes use of personal data in the possession or under the control of an organisation or a public agency, the use is not authorised by the organisation or public agency, the individual does so (i) knowing that the use is not authorised by the organisation or public agency or (ii) reckless as to whether the use is or is not authorised by the organisation or public agency and the individual, as a result of that use, (i) obtains a gain for the individual or another person; (ii) causes harm to another individual or (iii) causes a loss to another person;

(c) In relation to the unauthorised re-identification of anonymised information, if the individual takes any action to re-identify or cause re-identification of the person to whom anonymised information in the possession or under the control of an organisation or a public agency relates; the re-identification is not authorised by the organisation or public agency and the individual does so (i) knowing that the re-identification is not authorised by the organisation or public agency or (ii) reckless as to whether the re-identification is or is not authorised by the organisation or public agency

13.3.2. The individual may be fined up to $5,000 or to imprisonment for a term not exceeding 12 months or to both for the following offences:

(a) In relation to obtaining access to or changing another individual's personal data without the authorization of that individual;

(b) In relation to the offence of giving a porting organisation a data porting request to transmit personal data about another individual to a receiving organisation without the authority of that other individual; or

(c) In relation to the offence listed in 13.1.1.(a)

13.3.2.1. The offence for 13.3.3.(b) does not apply to an individual who gives a data porting request, in the individual's personal or domestic capacity, to transmit any user activity data or user-provided data about the individual even though the user activity data or user-provided data (as the case may be) includes personal data about another individual.

13.3.3. The individual may be fined up to $10,000 or to imprisonment for a term not exceeding 12 months or to both for the following offences:

(a) in relation to the offences listed in 13.1.1.(c) and 13.1.1.(f).

13.3.4. The individual may be fined up to $5,000 or to imprisonment for a term not exceeding 6 months or to both for the following offences:

(a) In relation to the offences listed in 13.1.1.(d) and 13.1.1.(e).

13.4. Offences by Corporations

13.4.1. In a proceeding for an offence under PDPA, it is necessary to prove the state of mind of a corporation in relation to a particular conduct, evidence that –

(a) an officer, employee or agent of the corporation engaged in that conduct within the scope of the actual or apparent authority of the officer, employee or agent, and

(b) the officer, employee or agent had that state of mind,

is evidence that the corporation had that state of mind.

13.4.2. Where a corporation commits an offence under PDPA, a person -

(a) Who is –

(i) an officer of the corporation; or

(ii) an individual involved in the management of the corporation and in a position to influence the conduct of the corporation in relation to the commission of the offence; and

(b) Who –

(i) consented or connived, or conspired with others, to effect the commission of the offence;

(ii) is in any other way, whether by act or omission, knowingly concerned in, or is party to, the commission of the offence by the corporation; or

(iii) knew or ought reasonably to have known that the offence by the corporation (or an offence of the same type) would be or is being committed, and failed to take all reasonable steps to prevent or stop the commission of that offence,

shall be guilty of that same offence as is the corporation and shall be liable on conviction to be punished accordingly.

13.4.3. A person mentioned in Paragraph 13.4.2. may rely on a defense that would be available to the corporation if it were charged with the offence with which the person is charged and, in doing so, the person bears the same burden of proof that the corporation would bear.

13.4.4. Under PDPA, any act done or conduct engaged in by an employee shall be treated for the purposes of PDPA as done or engaged in by the Organisation as well as by the employee, whether or not it was done or engaged in with the employer's knowledge or approval.

13.4.5. In any proceedings for an offence under PDPA brought against any person in respect of an act or conduct alleged to have been done or engaged in by an employee of that person, it is a defense for that person to prove that the person took such steps as were practicable to prevent the employee from doing the act or engaging in the conduct, or from doing or engaging in, in the course of his or her employment, acts or conduct of that description.

13.5. Civil Claims

13.5.1. Third parties who suffer losses or damages as a result of a breach of PDPA by the Organisation of any provision of Part 4, 5, 6, 6A or 6B or by a person of any provision of Division 3 of Part 9 or section 48B(1), can file civil claims.

13.5.2. If the claim is successful, the court may grant such third parties relief by way of injunction or declaration, damages, or any other relief as the court thinks fit.

13.5.3. Investigations require significant time, resources and management input that can be disruptive to business and may also have a negative impact on general repute.

13.5.4. **ALL EMPLOYEES AND ADVISERS ARE THEREFORE EXPECTED TO BE FULLY AWARE OF THE DOS AND DON'TS FOR COMPLIANCE WITH PDPA. FURTHER, SHOULD THE ORGANISATION SUFFER ANY LOSS OR DAMAGE OR BE IMPOSED WITH A FINANCIAL**

PENALTY, A CIVIL CLAIM, OR FINE FOR BREACHES OF PDPA AS A RESULT OF AN ACTION OR OMISSION OF ANY EMPLOYEE OR ADVISER, THE ORGANISATION RESERVES ITS RIGHT TO CLAIM COMPENSATION AND DAMAGES FROM THAT EMPLOYEE.

14. DO NOT CALL (DNC) PROVISIONS

14.1. Introduction

14.1.1. The Organisation sending marketing messages to Singapore telephone numbers are required to comply with the Do Not Call (DNC) provisions in PDPA. DNC provisions apply when:

14.1.1.1. Sender of message is in Singapore when message is sent; or

14.1.1.2. Recipient of message is in Singapore when message is accessed.

14.1.2. The DNC Provisions apply equally to all means by which a sender may send a specified message to a Singapore telephone number. For example, voice calls, SMS, or any data applications (such as 'WhatsApp', 'iMessage' or 'Viber') which use a Singapore telephone number.

14.1.3. For specified messages which are not sent to a Singapore telephone number, e.g. location-based broadcasts that are pushed to mobile phones though data-enabled smart phone applications or data applications that do not use a Singapore telephone number to send messages, the Do Not Call Provisions do not apply but the Data Protection Provision may still apply.

14.1.4. The DNC Provisions do not apply if both the sender and the recipient are not in Singapore when the specified message is sent and accessed respectively. The DNC Provisions would apply if the recipient is travelling in another country and the sender is in Singapore. It would also apply where one of the senders is located overseas while another is located in Singapore.

14.1.5. With reference to Group Marketing and Social Media Materials Standards, the Organisation sending marketing materials via mail or email to the general public, where DNC provision does not apply, is required to comply with the following:

(a) Spam Control Act 2007 and PDPA;

(b) Every message shall contain a title in the subject field (where there is a subject field), and this title shall not be false or misleading and must be relevant to the content of the message;

(c) It should also include an accurate and functional email or telephone number by which the sender can readily be contacted;

(d) Where applicable, include <ADV> to clearly identify that the message is an advertisement;

(e) Where applicable, include <T&C apply> if the information on any offer or promotion in the content is subject to specific requirements or restrictions that may not be adequately addressed in the main text; and

(f) Where applicable, include <UNSUB> to provide an option to the recipient to opt out from receiving further marketing materials. Please ensure proper documentation for unsubscribed records.

14.2. Definitions of "Send", "Message" and "Specified Message"

14.2.1. The term "send" is referred to (a) the sending of the message, (b) causing or authorizing the sending of the message, or (c) the making of a voice call containing the message, or causing or authorizing the making of such a voice call.

14.2.2. Note: A person who caused or authorized the sending of the message or the making of the call is also a sender under the DNC Provisions and must comply with the provisions.

14.2.3. The term "message" includes a message in sound, text, visual or other form.

14.2.4. A "specified message" is if the purpose, or one of the purposes, of the message is:

(a) to advertise, promote, or offer to supply or provide (i) goods or services, (ii) land or an interest in land; or (iii) a business opportunity or an investment opportunity;

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

(c) any other prescribed purpose related to obtaining or providing information.

14.2.5. An invitation to an event, seminar or course could be considered as a purpose which falls within the meaning of a specified message. Example: An event could offer to supply a good or service, or a seminar could promote or advertise a supplier.

14.2.6. For exclusions of specified messages, please refer to Eighth Schedule of PDPA. **When in doubt, please contact the Data Protection Officer.**

14.3. Duty to Check the DNC Register

14.3.1. Before a person sends a specified marketing message addressed to a Singapore telephone number, the person must check with the DNC Registry to confirm that the number is not listed on a DNC Register established by the PDPC as part of the DNC Registry. This is only applicable when sending marketing messages addressed to Singapore telephone numbers of prospects/non-PIAS clients.

14.3.2. In order to ascertain the above, the person must:

(a) Have made an application to the PDPC within 21 days, before sending the specified message, to confirm whether the Singapore telephone numbers is listed in the DNC Register; and received confirmation from the PDPC that the Singapore telephone number is not listed in the relevant register; or

(b) Have obtained from a checker information that the Singapore telephone number is not listed in the relevant register ("relevant information") and has no reason to believe that –

(i) the relevant information was obtained more than 21 days ago; or

(ii) the relevant information is false or inaccurate.

14.3.3. The prescribed duration within which a person must check with the DNC Registry before sending a specified message to a Singapore telephone number has been prescribed as 21 days.

14.3.4. The "prescribed duration" for the validity of the DNC check has been prescribed as 21 days from receipts of results.

14.3.5. There are three separate DNC Registers covering: Voice calls, Text Messages and Fax Messages

14.4. The Organisation must not send a marketing message addressed to a Singapore telephone number unless they had:

14.4.1. For Prospects/non-PIAS clients, checked the relevant DNC register within the "prescribed duration" before sending the message and received information that the telephone number is not listed in the register; or

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

14.5. Duty to Identify the Sender of a Message

14.5.1. When sending a specified marketing message, the person must include information identifying the sender and how the recipient can readily contact the sender. This information must be reasonably likely to be valid for at least 30 days after the message is sent.

14.5.2. Examples of contact information would be an operational Singapore telephone number which can receive incoming calls or text messages, or a valid email address which can receive incoming emails.

14.5.3. For voice calls, do not conceal or withhold from the recipient the sender's calling line identity.

14.6. Obtaining Clear and Unambiguous Consent

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

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

(b) whether the user or subscriber gave consent to receive specified messages through some form of positive action. Clear and unambiguous consent is unlikely to be construed to have been obtained from a mere failure to opt out through inaction on the part of the user or subscriber.

14.7. Consent Evidenced in Written or Other Form

14.7.1. Written form may include documents or other form of records in physical or electronic form. The requirement to obtain consent in evidential form applies to both online and offline situations.

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

14.7.3. Where consent was obtained through electronic means, you should retain documentation or system logs capturing the following information:

(a) the individual's choice (i.e. whether the individual provided consent or not);

(b) date and time when the individual expressed his choice;

(c) the webpage / pop-up / online form (or equivalent) which the relevant individual was looking at when providing consent; and

(d) the clauses which the individual consented to (including the terms and conditions applicable to the consent which the individual provided).

14.8. Retention Period for the Documentary Evidence of Clear and Unambiguous Consent

14.8.1.1. To retain evidence of clear and unambiguous consent from an individual for as long as they intend to rely on such consent to send specified messages to that individual's Singapore telephone number.

14.9. Requirement to Provide Clear and Accurate Information Identifying the Sender

14.9.1. Persons may choose to use their website address as identification information if the recipient can easily locate and identify the sender using the information provided within the text of the website address itself, within the contents of the landing page of the relevant website address or on the "Contact Us" or equivalent page.

14.9.2. The PDPC recognizes that in certain circumstances, persons who send specified messages may wish to identify themselves using a name other than their own which is more closely related to the goods or services offered ("related names") or if the related name would be more familiar to the recipient. Examples of such related names could be the names of a person's brands, retail outlets, buildings or property developments.

14.9.3. Do not attempt to obscure or conceal identity by using related names as identification information.

14.9.4. Identification information must be provided in the form of a name or alias that is able to identify the sender. The sender would not be considered to have provided identification information if that information is provided solely in the form of generic pronouns, e.g. "me" or "us", informal nicknames, or fictitious names.

14.10. Requirement to Provide Clear and Accurate Information about how the Recipient can Readily Contact the Sender

14.10.1. The PDPC consider this requirement to be met so long as the contact information enables the recipient to directly contact the sender in a reasonably convenient manner.

14.10.2. The most straightforward way to provide contact information would be to provide an operational Singapore telephone number which can receive incoming calls or text messages, or a valid email address which can receive incoming emails.

14.10.3. Note: Short codes and "No-Reply" email addresses are not considered as contact information as they do not allow the recipient to readily contact the sender. Provision of a physical address by itself does not allow the recipient to readily contact the sender as it requires more time and effort to either make a trip to the location or write a letter and send it by post to the sender.

14.10.4. As good practice, any contact information provided should be readily accessible from Singapore and operational during Singapore business hours. In considering whether the contact information provided enables the recipient to readily contact the sender, the PDPC will consider the actual outcome when the contact information is used.

14.11. Prohibition on Use of Dictionary Attacks and Address-Harvesting Software

14.11.1. The Organisation must not send, cause to be sent, or authorize the sending of any message, insofar as the recipient telephone number is obtained by dictionary attack or address-harvesting.

14.11.2. The Organisation must not send 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.

14.11.3. "Dictionary attack" means the method by which the telephone number of a recipient is obtained using an automated means that generates possible telephone numbers by combining numbers into numerous permutations. For instance, this would include randomly generating strings of 8-digit numbers, in running sequence or otherwise.

14.11.4. "Address-harvesting software" means software that is specifically designed or marketed for use for (a) searching the Internet for telephone numbers and (b) collecting, compiling, capturing or otherwise harvesting those telephone numbers.

14.11.5. The primary responsibility lies with the organisation that sends the messages and employees are not liable if they are merely acting in the course of their employment. However, directors, partners or other officers of similar level of seniority may also be held liable for their organisation's actions.

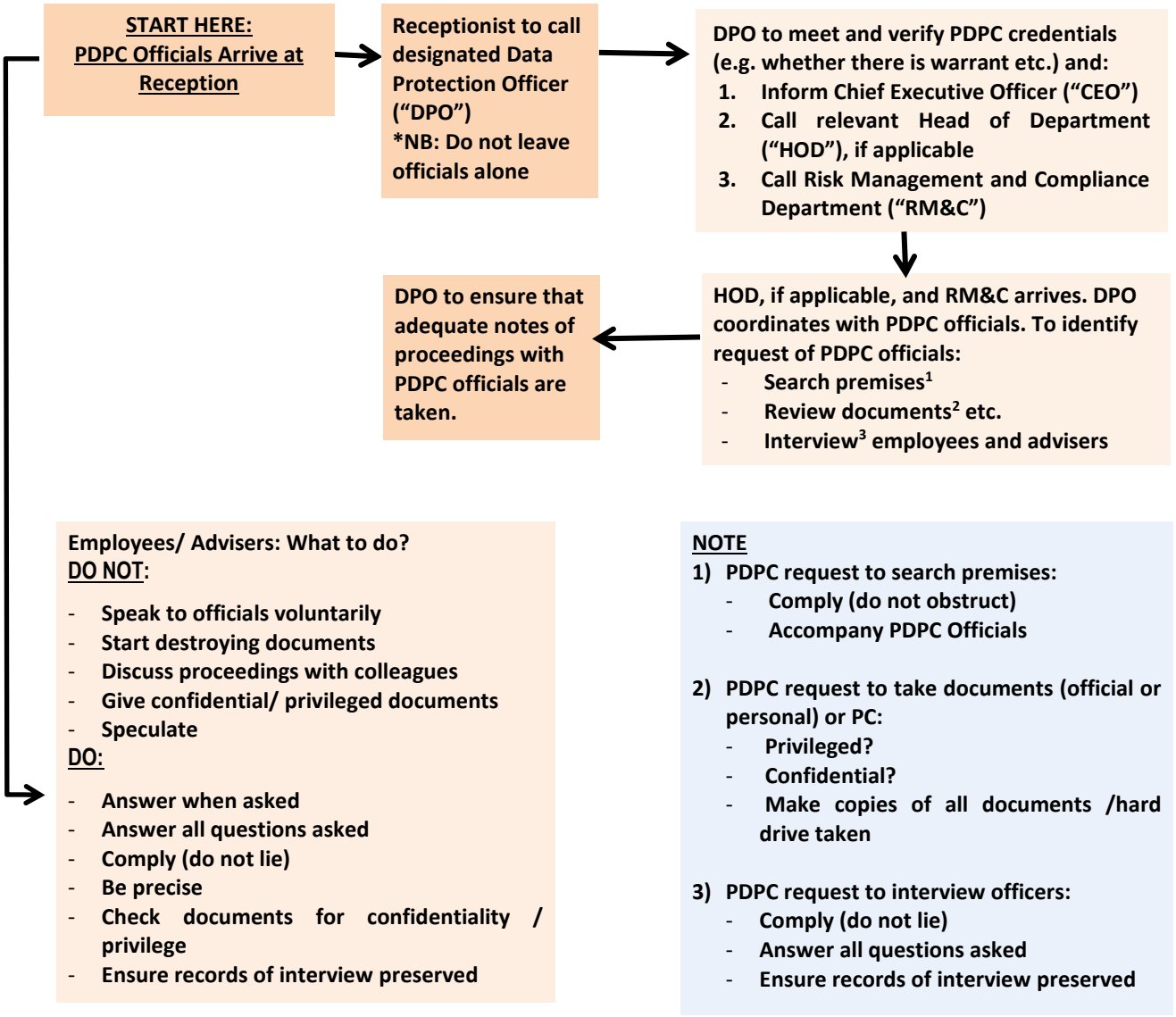
14.12. DNC Registry Related Breaches Penalties

14.12.1. Any organisation who contravenes the DNC Provisions of PDPA shall be issued directions, including paying a financial penalty of up to $1 million. For more egregious cases, the financial penalty amount may be up to 5% of the organisation's annual local turnover. Individuals in breach shall pay a financial penalty of up to $200,000.

15. WHAT TO DO IF THERE IS AN INVESTIGATION/RAID BY THE PDPC

15.1. Before and During the Investigation/Raid

15.1.1. A detailed flowchart is provided below on the appropriate steps to take during an investigation. Employees are expected to be familiar with the flowchart and to refer to it as and when necessary.



16. RELATED POLICIES/STANDARDS/RESOURCES

16.1. This Handbook should be read in conjunction with the following policies, standards and resources:

Document Name	Document Owner	Impacted Users
Group Privacy Standard	Group Compliance	PIAS Corporate Staff and FARs
Group Privacy Policy	Group Compliance	PIAS Corporate Staff and FARs
Data Risk Governance Framework	Group Chief Risk Officer	PIAS Corporate Staff
Data Management Policy	Group Chief Risk Officer	PIAS Corporate Staff
Data Incident and Breach Management Standard	Group Data Risk	PIAS Corporate Staff and FARs
PIAS Records Retention Schedule	PIAS DPO	PIAS Corporate Staff - Data Owners and Action Owners
PIAS Disposal Schedule	PIAS DPO	PIAS Corporate Staff - Data Owners and Action Owners
PIAS Data Inventory	PIAS DPO	PIAS Corporate Staff - Data Owners and Action Owners
PIAS Data Maps	PIAS DPO	PIAS Corporate Staff - Data Owners and Action Owners
PIAS Consumer Log	PIAS DPO	PIAS Corporate Staff - Data Owners and Action Owners

Annex A - COLLECTION, USE AND DISCLOSURE OF PERSONAL DATA

1. COLLECTION, USE AND DISCLOSURE OF PROSPECTS OR CUSTOMER PERSONAL DATA

1.1. Introduction

1.1.1. The Organisation collects, handles and retains personal data about its current, past and potential customers.

1.2. Obtaining Consent

1.2.1. Before collecting, using or disclosing personal data of an individual, you must seek his prior consent. Be sure to use the issued forms and wordings provided by the Data Protection Officer when doing so. Do not use forms or wordings which have not been certified by the Data Protection Officer.

1.2.2. When obtaining consent from individuals, it is the Organisation's policy to refer the individual to the full set of purposes for which the Organisation is collecting, using and disclosing personal data, as set out in the Organisation's Personal Data Notice and Consent Policy before obtaining the consent from the individuals. Please ensure that the individuals must have had an opportunity to review the Organisation's Personal Data Notice and Consent Policy and indeed have had reviewed the same before their provision of consent. For your ease of reference, the full version of the Organisation's Personal Data Notice and Consent Policy can be found at https://www.proinvest.com.sg/pdpa.

1.2.3. If you are in a front-facing department, that is you collect personal data from sources outside your Organisation, be sure to check to make sure that all required fields are completed and in order. Be sure to keep a record of the date at which the personal data is received by you.

1.2.4. Should any field be incomplete or otherwise unacceptable, immediately inform the Data Protection Officer and set that personal data aside. The notification to the Data Protection Officer must contain:

(a) why the consent is unacceptable;

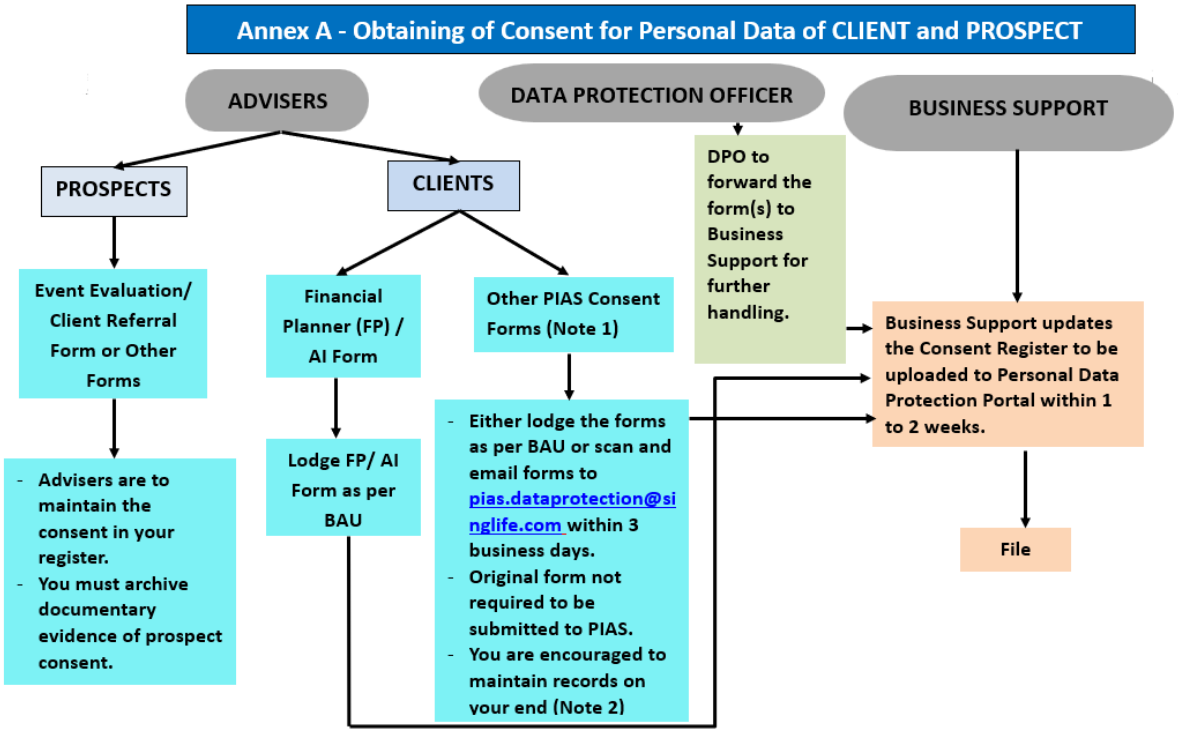
(b) the form or other manner in which the consent was collected on

(c) whether any action has been taken on the personal data (e.g. keying it into the system or otherwise using it) including which other departments or persons it was passed to or shared with; and

(d) the date at which such action was taken.

1.2.5. While waiting for the direction from the Data Protection Officer, cease all activity concerning that personal data.

1.3. Please refer to the below illustration for the Process of Obtaining Personal Data Consent from Clients and Prospects.



Note 1
Other PIAS Consent Forms are:
- Personal Data Notice & Consent Form
- Personal Data Update Form
- Event Evaluation Form

Note 2
Any individual who has given consent can withdraw consent anytime. Always check status of consent via the Personal Data Protection Portal to ensure consent is not withdrawn.

2. COLLECTION, USE AND DISCLOSURE OF ADVISERS AND EMPLOYEES PERSONAL DATA

2.1. Introduction

2.1.1. In addition to customer data, the Organisation collects, handles and retains personal data about its current, past and potential advisers and employees. The data protection principles described above in this Handbook must be considered and the suggested methods of compliance must be followed, whenever such advisers' and employees' personal data is being collected, or subsequently used, stored or disclosed in any way.

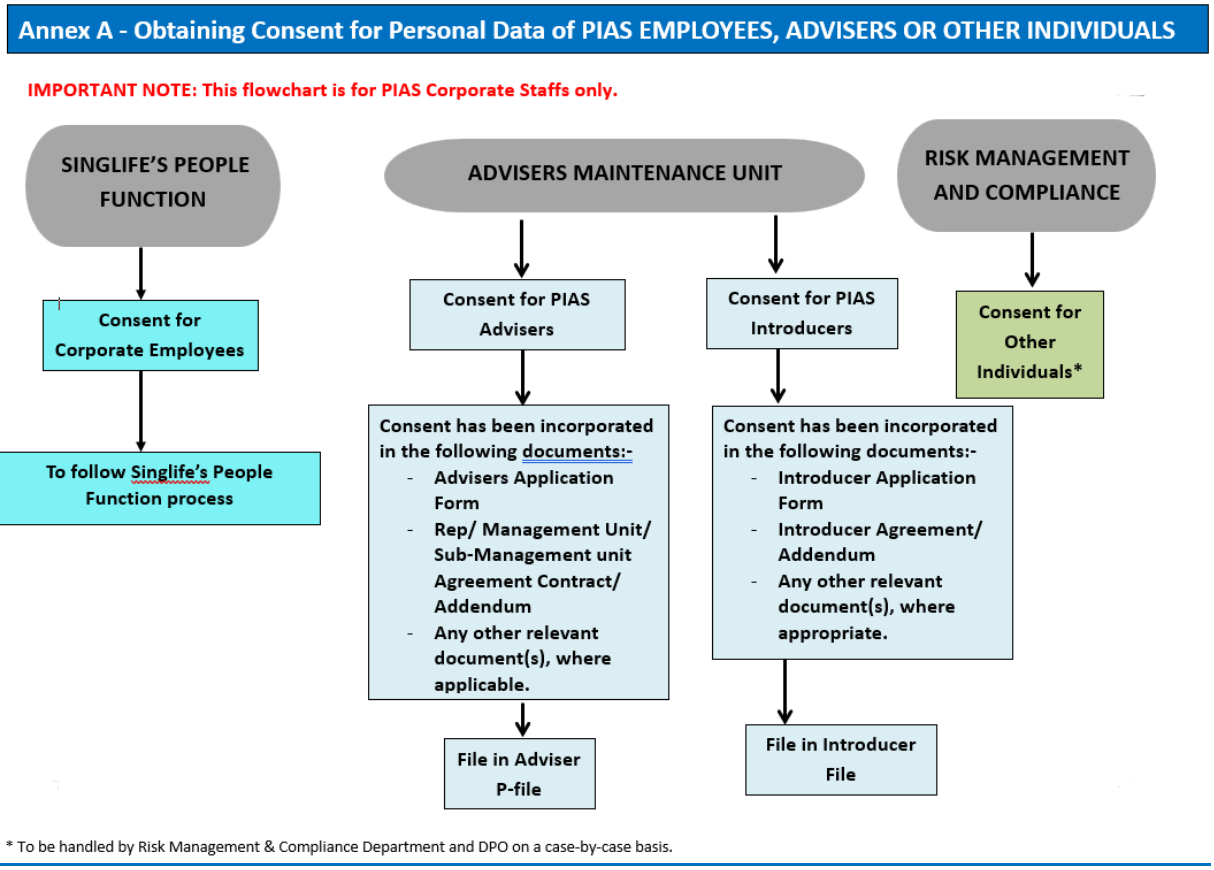
2.2. Obtaining consent

2.2.1. Before collecting, using or disclosing personal data of the potential advisers and employees, you must seek his prior consent.

2.2.2. For advisers related, be sure to use the issued forms and wordings that have been reviewed by the Data Protection Officer. Do not use forms or wording which have not been reviewed by the Data Protection Officer. For

2.2.3. For corporate employees related, be sure to use the issued forms and wordings provided by Singlife's People Function. Do not use forms or wording which have not been approved by Singlife's People Function.

2.3. Please refer to the below illustration for the Process of Obtaining Personal Data Consent from Advisers and Employees.



Annex B – OBTAINING CONSENT OF AN INDVIDIUAL FROM THIRD PARTIES WHERE INDVIDIUAL IS UNABLE TO PROVIDE CONSENT

1. SPECIAL CASES OF CONSENT

1.1 Minors / Children

1.1.1. The issue here is whether consent pursuant to the consent principle, can be given by an individual who is a minor (i.e. below 21 years of age) or a child (i.e. 18 years of age or below).

1.1.2. There are 2 ways to deal with this. They are referred to as Option A or Option B. You may choose to proceed with either Option A or Option B. When in doubt, you must seek the guidance of the Data Protection Officer.

Option A

This is where, when you or the Organisation deals with anyone who is below 13 years of age, consent would need to be obtained from that individual's parent or legal guardian.

Option B

This is where you proceed as follows:

Where the individual is below 21 years of age but 13 years or older, you or the Organisation may treat consent given by that individual as valid so long the policies on the collection, use and disclosure of the minor's personal data as well as the withdrawal of consent are readily understandable by them. However, if you have reason to believe or it can be shown that the minor does not have sufficient understanding of the nature and consequences of giving consent, you must then proceed by way of Option A.

1.2. Obtaining Consent from a Deceased Individual

1.2.1. PDPA protects deceased individuals' personal data to a limited extent and this is only for individuals who have been deceased for 10 years or less. For such personal data, only the provisions relating to the protection and disclosure of personal data would apply. For the latter, this would entail notification of purposes of disclosure of personal data, obtaining consent for disclosure of such personal data for the specific purposes of the disclosure, ensuring that the purpose is one which a reasonable person would consider appropriate in the circumstances, ensuring reasonable efforts have been taken that such personal data is accurate, and having reasonable security arrangements to protect such personal data. All other data protection principles do not apply. Once the individual has been dead for more than 10 years, none of the data protection principles would apply.

1.2.2. With regard to the personal data of a deceased individual who has been dead for 10 years or less, you must not disclose his personal data without the necessary consent. However, as the individual is deceased, the question then is from whom such consent should be obtained. In such a case, consent can be obtained, in the following order, from:

(a) firstly, the personal representative to the extent specified in the deceased's will or otherwise to the extent required for the administration of the deceased's estate; and

(b) secondly, if there is no such personal representative then the nearest relative of the deceased individual. The nearest relative is determined as the first living individual as determined in

accordance with the priority below (note that these stated individuals below must be of sound mind, not be legally incapable of exercising the right and not be subject to any legal instrument which limits their authority):

(i) Spouse at the time of death;

(ii) Child including child by adoption;

(iii) Parent;

(iv) Brother or Sister, including a brother or sister by adoption; and

(v) Other relation by birth or adoption.

1.2.3. Note that this is different from the priority in the Intestate Succession Act (Cap. 146).

1.2.4. Where two or more of the abovementioned individuals highlighted in (i) to (v) above share equal priority, then priority passes to the individual who is eldest. Where an individual who has higher priority is unable or unwilling to exercise the rights and powers of the deceased under PDPA, the priority shall pass to the individual who is next in priority.

1.2.5. Note that the individuals highlighted at paragraph [1.2.2(a) and 1.2.2(b)] above have the right to give consent and to also withdraw consent for the deceased individual. They also have the right to bring a private action against the Organisation or bring a complaint under PDPA.

ANNEX C - WITHDRAWAL POLICY

1. WITHDRAWAL POLICY

1.1. Introduction

1.1.1. Generally, the withdrawal of consent shall be handled using the standard clauses and forms. In accordance with PDPA, the Organisation must not restrict or prevent individuals from withdrawing consent. Hence, if an individual is communicating his/her withdrawal of consent outside the prescribed means, you must still act on such withdrawal request.

1.1.2. Section 2 below sets out the process which you are to follow when dealing with an individual's withdrawal of consent.

1.1.3. If you receive any withdrawal enquiry from an individual seeking to withdraw his/ her consent for the collection, use or disclosure of personal data, you must refer the individual to contact DPO at pias.dataprotection@singlife.com.

1.1.4. If you receive any withdrawal of consent via email (e.g. unsubscribed from receiving marketing materials via email), you must immediately notify DPO by forwarding the email to pias.dataprotection@singlife.com. It is highly encouraged to provide the following information:

(a) name of the individual;

(b) NRIC or passport no. of the individual (for client only);

(c) contact number of the individual;

(d) date of email that individual withdrew his consent, where applicable; and

(e) summary of the instructions given by the individual, where applicable.

1.1.5. If you receive any withdrawal of consent via any other mode of communication, such as a letter, you must immediately notify and forward that communication to DPO at pias.dataprotection@singlife.com.

1.1.6. If you receive some form of communication from an individual (such as an email) that is vague and you are unclear on whether that individual is seeking to withdraw his consent but you have in any case an impression (even if it is a weak impression) that the individual appears to be seeking to withdraw his consent, you must clarify with the individual and advise the individual to contact DPO at pias.dataprotection@singlife.com.

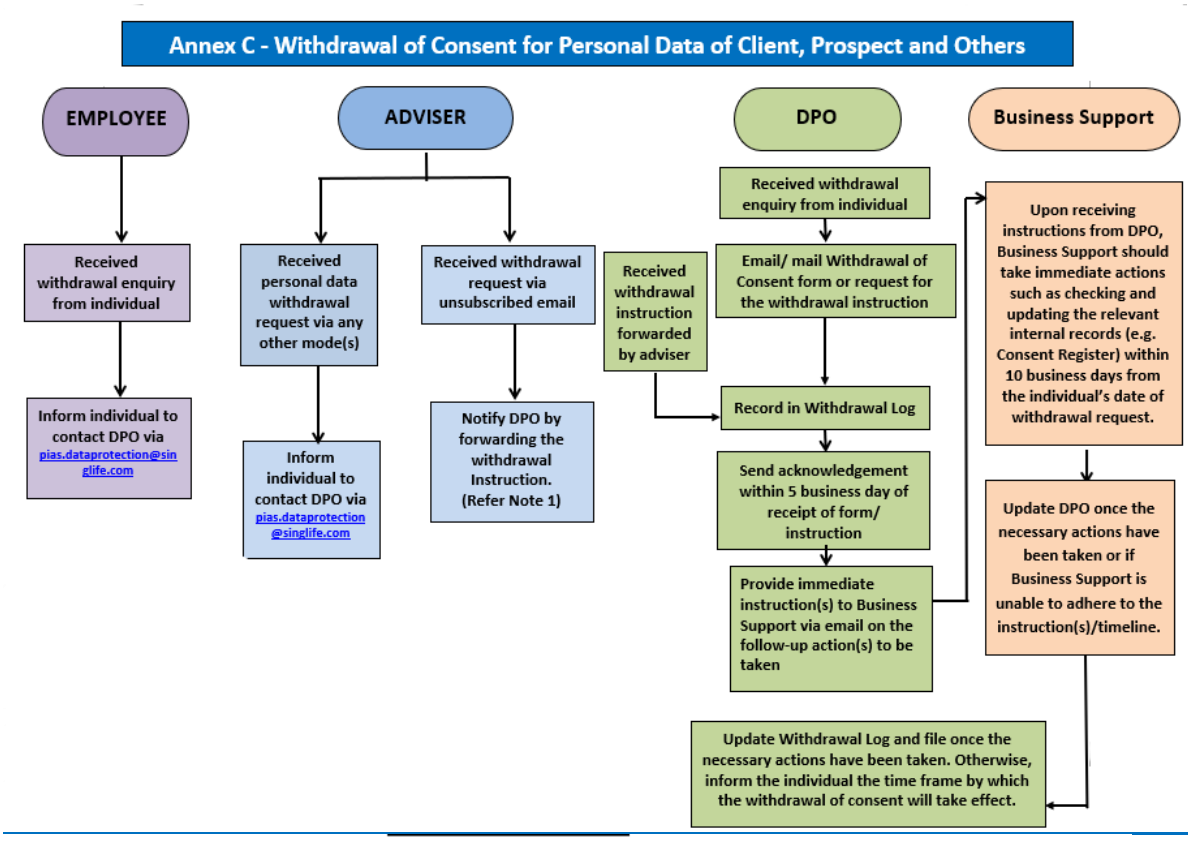
1.1.7. If the DPO receives any withdrawal enquiry from an individual, the DPO must email or mail the Withdrawal of Consent form or request for the withdrawal instruction. The DPO is to record in the Withdrawal Log for any withdrawal instruction either from the individual directly or through the adviser. The DPO is to send acknowledgement within 5 business day of receipt of form/ instruction. The DPO must provide immediate instruction(s) to Business Support via email on the follow-up action(s) to be taken. Upon receiving instructions from the DPO, Business Support should take immediate actions such as checking and updating the relevant internal records (e.g. Consent Register) within 10 business days from the individual's date of withdrawal request. Business Support is to update DPO once the necessary actions have been taken or if they are unable to adhere to the instruction(s)/timeline. The DPO is to update the Withdrawal Log and file the necessary supporting document(s), if any, once the necessary actions have been taken. Otherwise, the DPO is to inform the individual the time frame by which the withdrawal of consent will take effect.

1.1.8. Ignoring any communication from an individual where he is seeking to withdraw his consent or to act slowly in dealing with any such communication is conduct that is not accepted by the Organisation and will be viewed by the Organisation as a breach of your employment contract with the Organisation and subject you to disciplinary proceedings as well as possible termination of your employment with the Organisation.

1.1.9. Where an individual has been made aware of the consequences of his withdrawal and nonetheless proceeds to withdraw his consent, you must ensure that you cease collecting, using or disclosing the individual's personal data. The data intermediaries must be informed about the withdrawal and ensure that they cease collecting, using or disclosing the personal data for the various purposes.

2. PROCESS OF WITHDRAWAL OF CONSENT FOR PERSONAL DATA OF CLIENT, PROSPECT AND OTHER INDIVIDUALS

2.1. Please refer to the below illustration for the process of withdrawal of consent for personal data of client, prospect and other individuals.



Note 1

Submit withdrawal instruction as soon as possible, within 3 working days to DPO (pias.dataprotection@singlife.com) with the following information:

a. Name of individual;
b. NRIC/ Passport No (for client only);
c. Contact Number of individual;
d. Date of unsubscribed email; and
e. Summary of the withdrawal instruction.

A General Reminder to All Advisers

Always check the Personal Data Protection Portal prior to using or disclosing of Personal Data as consent can be withdrawn anytime.

3. WITHDRAWAL OF CONSENT FORM (CLIENT & PROSPECT)

3.1. Please refer to the Docushare under **PIAS Resource Library > Forms > PDPA forms Listing folder for a copy of the Withdrawal of Consent Form.

ANNEX D – PROCEDURES FOR ACCESS REQUEST

1. ACCESS REQUEST POLICY

1.1. Introduction

1.1.1. Generally, all information that is to be provided to individuals seeking access to their personal data are to be handled by using the standard forms. An access request may be received by many means. For example, through websites, email, faxes, SMS, letters, in-person notification or otherwise. The Organisation must respond to each access request as accurately and completely as necessary and reasonably possible. If an individual is communicating his/her access request outside the prescribed means, you must still act on such request.

1.1.2. Please refer Section 2 of this Annex for the request process that is being communicated to individuals.

1.1.3. If you receive an email from an individual making an access request, you must immediately forward that email to the DPO at pias.dataprotection@singlife.com.

1.1.4. If you receive any access requests by any other mode of communication, such as a letter, you must immediately notify and forward that communication to the DPO at pias.dataprotection@singlife.com.

1.1.5. If you receive some form of communication from an individual (such as an email) that is vague and you are unclear on whether that individual is making an access request but you have in any case an impression (even if it is a weak impression) that the individual appears to be making an access request, you must err on the side of the action and immediately notify and forward that communication to the DPO at pias.dataprotection@singlife.com.

1.1.6. If the DPO receive any access requests, the DPO must mail/email the individual the Access Request Form and inform the individual of the fee. The DPO to ensure sufficient information to identify the individual and the personal data being sought have been provided. Within 3 business days upon receipt of completed Access Request Form, NRIC copy, letter of authorisation (if applicable) & payment, the DPO to send acknowledgement to the individual. The DPO should refer to Section **[5.1 to 5.3.20.2.2.]** in tandem with this Annex D.

1.1.7. If the individual is neither a prospect nor a client, the DPO should forward the request by email to relevant business unit(s) for handling immediately after acknowledgement is sent to individual. The business unit(s) is to collate the personal data information as requested by individual in Part B and C of the Access Form and mail the collated information via registered mail within 30 days from the date of receipt of the completed Access Request Form and the fee from the individual. If the business unit is unable to comply with the request within the timeline, the business unit must inform the individual in writing of the reasonably soonest time in which the business unit will respond. The business unit to forward the collated information including the supporting documents(s) if any, to DPO for record-keeping and the DPO is to update the Access Log and file the supporting document(s).

1.1.8. If the individual is a prospect, the DPO to immediately email the adviser indicated in the Part A of the Access Form to collate personal data information requested in the Part B and C of the Access Form. The DPO must mail the collated information via registered mail within 30 days from the date of receipt of the fee and the completed Access Request Form from the individual. If the DPO is unable to comply with the request within the timeline, the DPO must inform the individual in writing of the

reasonably soonest time in which the DPO will respond. The DPO should update the Access Log and file the supporting document(s), if any.

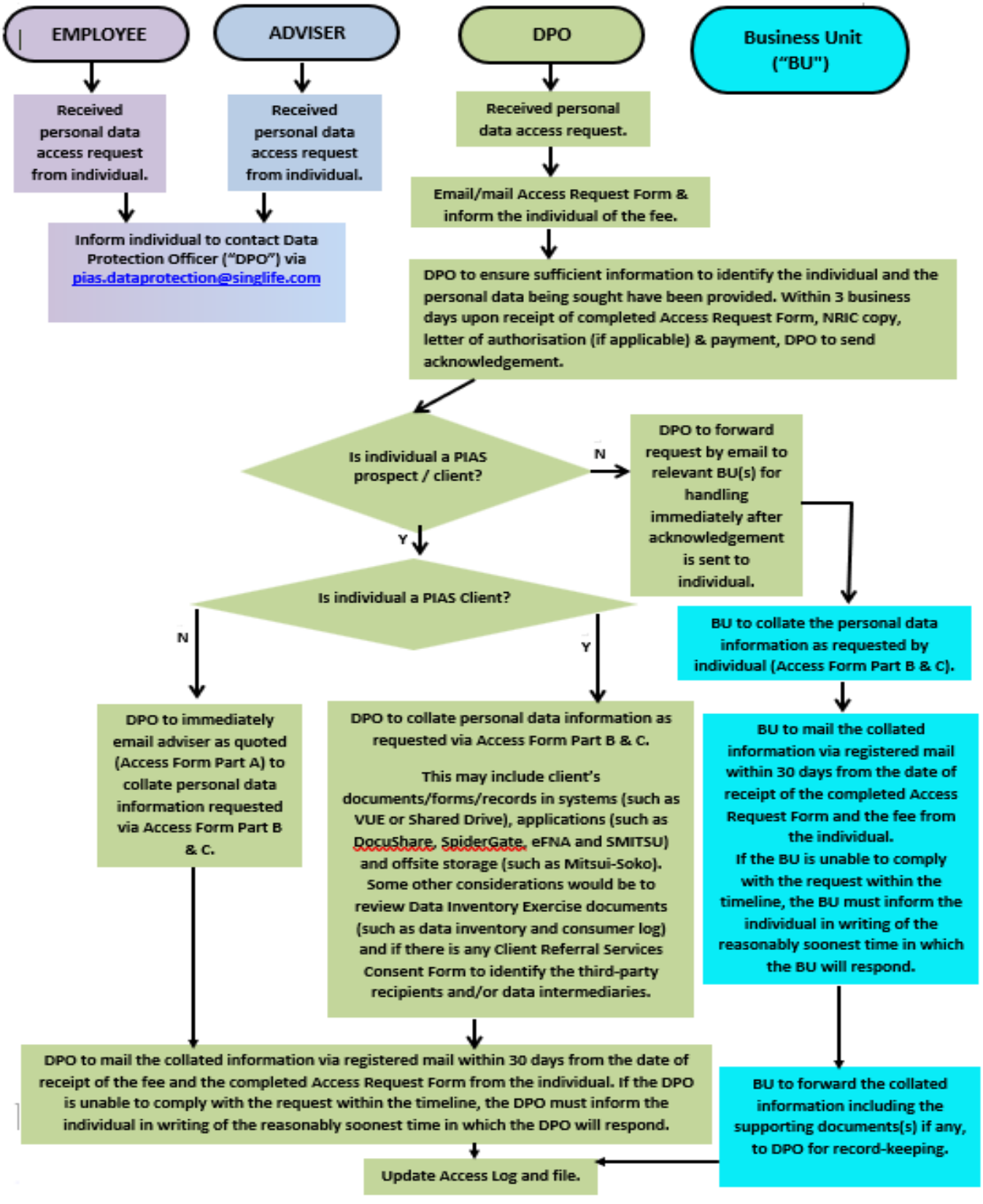
1.1.9. If the individual is a client, the DPO to collate personal data information as requested in the Part B and C of the Access Form. This may include client's documents/forms/records in systems (such as VUE or Shared Drive), applications (such as DocuShare, SpiderGate, eFNA and SMITSU) and offsite storage (such as Mitsui-Soko). Some other considerations would be to review Data Inventory Exercise documents (such as data inventory and consumer log) and if there is any Client Referral Services Consent Form to identify the third-party recipients and/or data intermediaries. The DPO must mail the collated information via registered mail within 30 days from the date of receipt of the fee and the completed Access Request Form from the individual. If the DPO is unable to comply with the request within the timeline, the DPO must inform the individual in writing of the reasonably soonest time in which the DPO will respond. The DPO should update the Access Log and file the supporting document(s), if any.

1.1.10. Ignoring any communication from an individual where he is seeking to make an access request or to act slowly in dealing with any such communication is not accepted by the Organisation and will be viewed by the Organisation as a breach of your employment contract with the Organisation and subject you to disciplinary proceedings as well as possible termination of your employment with the Organisation.

2. PROCESS FOR ACCESS REQUEST RECEIVED FROM PROSPECTS, CLIENTS AND INDIVIDUALS

2.1. Please refer to the below illustration for the process for access request received from client, prospect and other individuals.

Annex D - Access Request received from Prospects, Clients and Individuals



3. ACCESS REQUEST FORM

3.1 Please refer to the Docushare under **PIAS Resource Library > Forms > PDPA forms Listing folder for a copy of the Access Request Form

ANNEX E – PROCESS FOR DEALING WITH CORRECTION REQUEST

1. CORRECTION REQUEST POLICY

1.1. Introduction

1.1.1. Generally, all correction requests are to be handled by using the standard clauses and forms. A correction request may be received by many means, and from either individuals or other organisations. For example, through websites, email, SMS, letters, in-person notification or otherwise. If the communication of the correction request is outside the prescribed means, you must still act on such request.

1.1.2. Please refer Section 2 of this Annex for the request process that is being communicated to individuals.

1.1.3. If you receive a telephone call from an individual or a representative from another organization seeking to make an correction request or are informed by the individual or representative of another organisation in person, you must immediately refer the individual to contact DPO at pias.dataprotection@singlife.com

1.1.4. If you receive an email from an individual or representative of an organisation making a correction request, you must immediately refer the individual to contact DPO at pias.dataprotection@singlife.com .

1.1.5. If you receive any correction requests by any other mode of communication, such as a letter, you must immediately refer the individual to contact DPO at pias.dataprotection@singlife.com.

1.1.6. If you receive some form of communication from an individual (such as an email) or representative of another organization that is vague and you are unclear on whether that individual or the representative is making an correction request but you have in any case an impression (even if it is a weak impression) that the individual or representative appears to be making an correction request, you must err on the side of the action and immediately refer the individual to contact DPO at pias.dataprotection@singlife.com .

1.1.7. As an adviser, if you receive any personal data update request from your client, do provide the client with the Personal Data Update Form. Either lodge the completed form as per BAU or submit the completed form and necessary supporting document(s) to Data Protection Officer (“DPO”) within 3 business days upon receipt, via pias.dataprotection@singlife.com.

1.1.8. As an adviser, if you receive any correction request from your prospect, you are to (1) correct* prospect’s records in your possession as soon as practicable, no later than 30 calendar days from the time the request is made, (2) update other relevant parties that you had disclosed the personal data to within the past year, the personal data to be corrected within 30 calendar days from the date of receipt of request and (3) email the DPO the name of prospect, NRIC (optional), correction request receipt, completion date and reason if correction not made.

1.1.9. * Prior correction, please consider if there is a business and/ or legal reason for the correction to be made. If not, document the reason why the correction should not be made on the Personal Data Update Form and reject the correction request, within 30 days from the date of receipt. Send the completed form to the DPO for filing to complete the process.

1.1.10. If the adviser is unable to comply with the request within the time frame, the adviser must inform the individual in writing of the soonest practicable time in which the adviser will make the correction.

1.1.11. If the DPO receives a correction request from a prospect, the DPO must request for PIAS adviser's name from the prospect and forward the request via email to the adviser within 3 business days upon receipt of request. The DPO is to update the Correction Log.

1.1.12. If the DPO receives a correction request from an individual that is not a prospect, the DPO must provide the Personal Data Update Form to the individual.

1.1.13. Upon receipt of completed form and necessary supporting document(s) either from the individual directly or through the adviser, the DPO is to update the Correction Log.

1.1.14. If the individual is neither a prospect nor a client, the DPO must forward the request via email, to relevant business unit(s) within 3 business days upon receipt of completed form and necessary supporting document(s). The business unit is to correct* individual's records in its possession as soon as practicable, no later than 30 calendar days from the time the request is made. The business unit is to update other relevant parties that it had disclosed the personal data to within the past year, the personal data to be corrected within 30 calendar days from the date of receipt of request. If the business unit is unable to comply with the request within the time frame, the business unit must inform the individual in writing of the soonest practicable time in which the business unit will make the correction. The business unit is to provide completion status update to the DPO for record-keeping and the DPO is to update the Correction Log and file the supporting document(s), if any. For the asterisk (*), please refer to Section **[1.1.9**].

1.1.15. If the individual is a client, within 3 business days upon receipt of completed form and necessary supporting document(s), the DPO must: (1) instruct the relevant business unit(s) to correct* client's records within PIAS, (2) instruct AMU/BD to forward the request via email, to the specified PIAS adviser indicated in the form so that they can correct the record as well and (3) update other relevant parties that PIAS had disclosed the personal data to within the past year, the personal data to be corrected within 30 calendar days from the date of receipt of request. If PIAS is unable to comply with the request within the time frame, the DPO must inform the individual in writing of the soonest practicable time in which PIAS will make the correction. The DPO is to update the Correction Log and file the supporting document(s), if any. For the asterisk (*), please refer to Section **[1.1.9].**

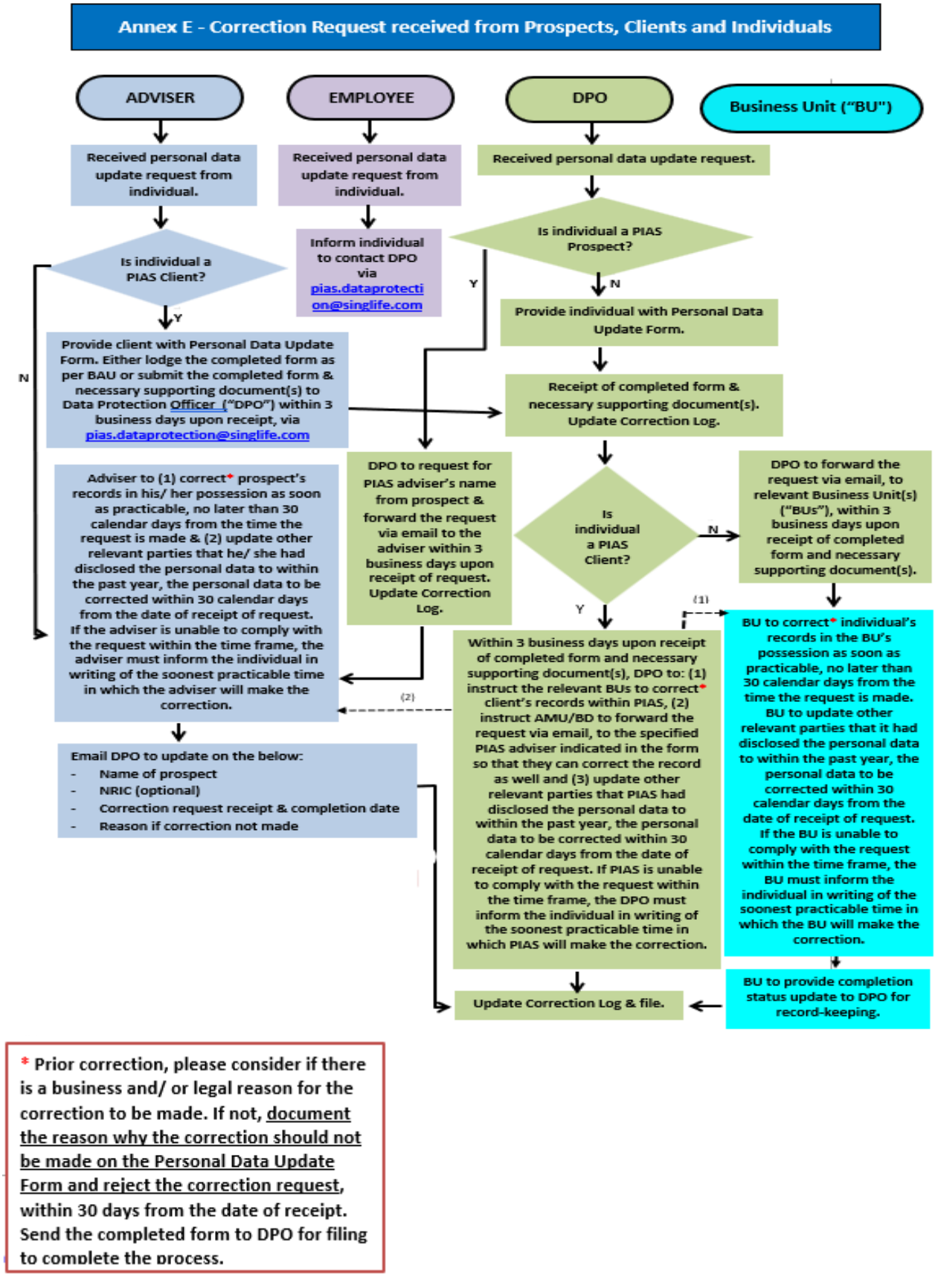
1.1.16. Section 2 sets out the process which you are to follow when dealing with an individual's or representative or another organisation's correction request.

1.1.17. Ignoring any communication from an individual or a representative of another organization where he is seeking to make a correction request or to act slowly in dealing with any such communication is not accepted by the Organisation and will be viewed by the Organisation as a breach of your employment contract with the Organisation and subject you to disciplinary proceedings as well as possible termination of your employment with the Organisation

2. PROCESS FOR CORRECTION REQUEST RECEIVED FROM PROSPECTS, CLIENTS AND OTHER INDIVIDUALS

2.1. Please refer to the below illustration for the process for correction request received from prospects, clients and other individuals.

Annex E - Correction Request received from Prospects, Clients and Individuals



* Prior correction, please consider if there is a business and/ or legal reason for the correction to be made. If not, document the reason why the correction should not be made on the Personal Data Update Form and reject the correction request, within 30 days from the date of receipt. Send the completed form to DPO for filing to complete the process.

3. PERSONAL DATA UPDATE FORM

3.1. For existing clients who wish to update their personal data, please refer to the DocuShare under **PIAS Resource Library > Forms > PDPA forms > Consent from Existing Clients Listing for a copy of the Personal Data Update Form.