Group Privacy Standard

Version: 1.1

Document owner:
Compliance – Privacy

INTERNAL USE ONLY

If it may be necessary to disclose this document in part, or in full, to a third party, approval must be obtained from the document owner prior to disclosure.

Change Control

Version	Date	Description	Changed by	Reviewed / Approved by
1.0	3 Aug 2022	New	Sharon Tan, Senior Manager	Edwin Ti, Director of Compliance; Michael Puhaindran, Group Head Legal & Compliance
1.1	28 Dec 2023	Key Changes: • Updated Singlife logo • Updated policy/standards document names and/or document owners • Section 5 - included additional consideration for collection of fresh consent • Section 9 - included additional considerations on access requests to Personal data	Maisarah Mohamed, Analyst; Sharon Tan, Senior Vice President	Edwin Ti, Head, Compliance; Michael Puhaindran, Group Head of Legal, Compliance and Secretariat

TABLE OF CONTENTS

1. INTRODUCTION

1.1 This Standard is mapped to the Group Privacy Policy and defines the standards for compliance with the Group Privacy Policy to address Privacy risk.

1.2 It should be read and applied in conjunction with the Group Privacy Policy. Where a conflict exists between the requirements of the Group Privacy Policy and this Standard, the Group Privacy Policy shall prevail. Where a conflict exists between this Standard and any related Business-owned Policy / Standard, this Standard shall prevail.

1.3 Where there are local legal or regulatory requirements, industry best practice or regulatory expectations that provide higher or stricter requirements than those set out in this document, these should be adopted and incorporated for local application, and where appropriate, documented by way of a Country / Business Segment Addendum to this Standard.

2. SCOPE

This Standard applies to:

- Singapore Life Holdings Pte. Ltd. and its group of companies (collectively labelled as the "Group") that process Personal Data;
- all employees (whether on a part-time, temporary or full-time basis), outsourced staff, interns and trainees (collectively, "employees") working at or attached to the Group who process any Personal Data;
- independent contractors, including representatives who are contracted to financial advisers which are subsidiaries within the Group, who process any Personal Data;
- all processing of Personal Data; and
- any records that contain Personal Data, regardless of their format or whether they are maintained or managed within the Group (i.e., internally) or by an external Third Party on behalf of the Group.

3. PERSONAL DATA

3.1 Personal Data refers to any data or information that enables an individual to be identified, either from this data itself or when combined with other data.

3.2 Sensitive Personal Data is a subset of Personal Data. As the name suggests, it needs to be treated with extra care because, if it falls into the wrong hands or is otherwise misused, the risk of harm or its severity caused to a person is much higher. It includes information about an individual's:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Genetic data
- Biometric data (where this is used for identification purposes)
- Health (mental or physical)

- Sexual orientation or sex life
- Criminal allegations, proceedings or convictions
- Minors' data[1]
- Financial and insurance information[1]
- National identity card number[1]
- Birth certificate number[1]
- Passport number[1]
- Work permit number[1]

3.3 By individual, we mean any of the following (usually) living people / persons:

- A current, past or prospective customer
- The officers, directors or shareholders of corporate customers
- A current, past or potential colleague or member of staff
- A supplier, vendor or business partner (if they are a person, not a legal entity/company/corporation)
- Any visitor to the Group's premises
- Any visitor to or user of the Group's websites or applications

3.4 The number of potential combinations of data means there is no exhaustive list of examples of what constitutes Personal Data, and an element of judgement is required in some situations.

3.5 Where the data is truly anonymized, i.e., it is not possible to identify the individual from the details or by combining it with other data or information held by the Group, then it is not Personal Data.

3.6 Where the data is pseudonymized, it is still Personal Data. Data or information that has had identifiers removed or replaced to pseudonymize the data is still considered as Personal Data.

3.7 Business Card Data or Business Contact Information is Personal Data, especially when used in a non-business context. However, depending on specific country laws and regulations, e.g., in Singapore, such information may be excluded from being deemed as Personal Data when it is provided by an individual for use for a business (not personal) purpose.

3.8 To determine if something is Personal Data, ask yourself:

- Can an individual be identified from this data?
- Can a person be singled out or a person be treated differently based on this data (either on its own or in combination with other data the Group holds)?

If the answer is Yes to at least one of those questions, then it is likely to be Personal Data.

4. PROCESSING OF PERSONAL DATA

4.1 Processing of Personal Data is defined as any operation or set of operations (or activity) which is performed on Personal Data. It includes (but is not limited to) adapting, blocking, collecting, combining, consulting, destroying, disclosing, disseminating, erasing, obtaining, recording, organizing, retaining, retrieving, storing, transmitting, transferring, using or viewing.

[1] Specific to Singapore

4.2 It is basically anything that is done with Personal Data, so it covers every type of operation whether carried out via manual or automated means. Some examples (not an exhaustive list) include:

- Screening of candidate / staff
- Administering payroll
- Sourcing Personal Data from Third Parties
- Conducting surveys or research
- Creating application forms which will be used to collect Personal Data
- Setting up of client accounts or policies
- Reviewing candidates' job applications and resumes
- Processing onboarding documentation of employees
- Using a contacts database containing Personal Data
- Issuing content or social media marketing
- Conducting helpline activities
- Archiving documents containing Personal Data
- Deleting documents containing Personal Data
- Posting a photo of an individual on the website
- Storing IP or MAC addresses, which are unique identifiers assigned to network devices
- Use of cookies and other tracking mechanisms
- Use of geo-location (tracking and location) devices
- Use of CCTV or other video surveillance
- Conducting internal investigations

4.3 Personal Data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

4.4 The collection of Personal Data must be assessed to be reasonably suitable and necessary to fulfil the specified purposes of the collection. When different types of Personal Data can be used to achieve the same purpose, collect the least sensitive types of Personal Data.

4.5 Personal Data or documents containing Personal Data must only be retained for a reasonable period deemed necessary to serve its business and/or legal purposes.

4.6 Documents containing Personal Data should be disposed of or Personal Data that can be associated with particular individuals should be removed (e.g., via anonymization), as soon as it is reasonable to assume that the purpose for which it was collected is no longer being served by the retention of the Personal Data, and the retention is no longer necessary for legal or business purposes. For example, subject to relevant country law / regulation, transactional data (which may contain Personal Data) may be retained for 7 years post the end of the customer relationship, while marketing communications (where Personal Data is used) may be retained for 1 year (to address the requirement to respond to access requests for information relating to how Personal Data was used or have been disclosed within the past year).

5. LAWFUL BASIS

5.1 Before commencing to process Personal Data, a valid purpose for doing so must first be determined. This is referred to as a "lawful basis". Without having determined a lawful basis, the processing of the Personal Data would not be deemed lawful and thus, the processing of the Personal Data should cease.

Note that there are different lawful bases and hence different applications accorded under different country Privacy laws. Hence, please consult your Data Protection Officer ("DPO") or Group Privacy Compliance at the first instance.

5.2 Lawful bases available for processing Personal Data may be referred to from the following perspective:

	Lawful Basis	**Description**
a)	Consent	• Refers to any freely given, specific, informed and unambiguous indication of the individual's wishes by which he/she by a statement or by clear affirmative action, signifies agreement to the Processing of his/her Personal Data. • May be in the form of explicit consent, deemed consent by conduct, deemed consent by contractual necessity or deemed consent by notification. Example: to receive marketing communications; for participation in lucky draws, competitions, events and activities; to process applications for products or services.
b)	Legal obligation	Where the processing is required to comply with the law. Example: for reporting obligations; to conduct identity verification, government sanctions screening and due diligence checks.
c)	Vital interest	Where the processing is necessary to protect someone's life, health or safety.
d)	Public interest	Refers to data obtained or disclosed to a public agency.
e)	Matters affecting the public	Refers to data that is publicly available, necessary for performance of task in national or public interest, solely for artistic or literary purposes, archival or historical purposes.
f)	Legitimate interest	Where the processing is necessary for: • Evaluation purposes • Any investigation or proceeding • For the Group to recover or pay a debt

	Lawful Basis	Description
		• Provision of legal services • Confer an interest or a benefit on the individual under a private trust or benefit plan • Produced in the course of an individual's employment, business or profession • Managing or terminating an employment relationship • Legitimate interest of the Group outweighs any adverse impact on the individual A Legitimate Interest Assessment (refer to Appendix A) must be conducted. The assessment consists of a Purpose test (to identify the legitimate interest you are relying on), a Necessity test (to show that process the Personal Data is absolutely necessary to achieve it) and a Balancing test (balancing the processing against the individual's rights and freedom). Example: Employee and customer satisfaction surveys; enforcement of legal claims including debt collection via out-of-course procedures; certain types of employee monitoring (to ensure the individual is acting appropriately in accordance with the employment contract) via CCTV monitoring and email/chat surveillance for safety or management purposes.
g)	Business improvement purposes	Where the processing is necessary for: • improving, enhancing or developing new products or services, or new methods of processes for business operations in relation to the Group's products and services • learning or understanding the behavior and preferences of individuals, including groups of individuals segmented by profile • identifying products or services that may be suitable for individuals or personalizing or customizing any such products or services for individuals Subject to conditions: • The purpose cannot reasonably be achieved without using the Personal Data in an individually identifiable form; and • The Group's use of personal data for purposes is one that a reasonable person would consider appropriate in the circumstances.
h)	Research purposes	To conduct broader research and development that may not have any immediate application to the Group's products, services, business operations or market.

	Lawful Basis	Description
		Subject to conditions: • the research purpose cannot reasonably be accomplished unless the Personal Data is used in an individually identifiable form; • there is a clear public benefit to using the personal data for research purpose; • the results of the research will not be used to make any decision that affects the individual; • in the event that the results of the research are published, the Group publishes the results in a form that does not identify the individual; and • provided that it is impracticable for the Group to seek the consent of the individual for the disclosure.

5.3 Consent may be obtained in the following ways:

a)	Express / Explicit Consent	An individual is clearly presented with an option to agree or disagree with the processing of his/her Personal Data. Explicit consent can be provided verbally or in writing. Explicit consent is usually required when clear, documentable consent is required, and the purposes for which it is being provided is sensitive, poses serious data protect risk, and a higher level of control is required over the processing of Personal Data, e.g., • when processing sensitive Personal Data, • when transferring data to third countries or international organizations in the absence of appropriate safeguards, • on automated individual decision-making, including profiling.
b)	Deemed consent by conduct	An individual is deemed to consent to the processing of Personal Data about the individual by the Group for a purpose if: a) the individual voluntarily provides the personal data to the Group for that purpose; and b) it is reasonable that the individual would voluntarily provide the data.
c)	Deemed consent by contractual necessity	An individual is deemed to have consented to the disclosure of his/her Personal Data in situations for the necessary conclusion or performance of a contract or transaction between the individual and the Group, e.g., deemed consent for processing of payment.

d)	Deemed consent by notification	An individual may be deemed to have given consent for a purpose when the individual is notified of the processing of his/her Personal Data and how he may opt-out, but he does not opt-out within a specified period. Note: Deemed consent by notification does not apply to, amongst other things, the sending of direct marketing messages.

5.4 For consent to be valid, the following must be present:

a) It must be given freely, i.e., giving the individual a genuine ongoing choice and control over how their Personal Data is processed.
b) It must identify the purpose of the processing, types of processing activity and the right to withdraw at any time.
c) There must be unambiguous indication of consent and no room for doubt that consent has been given, i.e., clear signal/sign that the individual had agreed. For example:
    - Explicit consent must be expressly confirmed in a clear statement, such as signing (their name) or ticking a checkbox next to it.
    - Opt-in consent, i.e., checkbox, must not be pre-ticked.
d) Consent requests must be prominent and unbundled / separate from other terms and conditions.
e) Consent requests must be clear, concise, easy to understand and user friendly.

5.5 The Group shall not:

a) As a condition to providing a product or service, require an individual to consent to the processing of Personal Data beyond what is reasonable to provide the product or service to that individual, or
b) Obtain or attempt to obtain consent for the processing of Personal Data by providing false or misleading information with respect to the processing of Personal Data or using deceptive or misleading practices.

However, where the collection of Personal Data is necessary (mandatory) for the administering of the product or service where otherwise the product or service cannot be provided / performed for the said purpose, the Group may choose not to avail the product or service to the individual. Example: collection of Personal Data for job applications, product application, etc.

5.6 The Group shall notify the individual and obtain fresh consent when there are new purpose(s) for the collection, use and disclosure of Personal Data. If the Personal Data collected is to be used or disclosed for different purpose(s) from what it was previously consented for, the Group shall notify the individual of the new purpose(s) of use and disclosure when obtaining fresh consent.

5.7 Before proceeding with any marketing communications with individuals, where the communication mode is via phone and related messaging platform, the Group shall:

a) unless the Group has the recipients' clear and unambiguous consent in written or other accessible form for sending the marketing message, additionally check if the individual's telephone number is registered on the national Do Not Call ("DNC") Registry; and
b) provide information sufficient for the recipient to identify and contact the sender.

5.8 The Group shall not send, cause to have sent or authorize the sending of a message sent to any telephone number, an electronic mail address or Instant Message ("IM") account which is generated through the use of a dictionary attack or address-harvesting software.

5.9 The processing of individual's National Identity Card number (or copies of the national identity card) should not be allowed except for the following specified circumstances:

a) Required under applicable country laws and regulations

b) Necessary to accurately establish or verify the identities of the individuals to a high degree of fidelity in the following situations:

- Where the failure to accurately identity the individual to a high degree of fidelity may pose a significant safety or security risk, or
- Where the inability to accurately identify an individual to a high degree of fidelity may pose a risk of significant impact or harm to an individual and/or the Group (e.g., fraudulent claims).

The treatment of the National Identity Card number applies to Birth Certificate numbers, Foreign Identification Numbers, Work Permit numbers and Passport Numbers (collectively "Other identification numbers").

c) An individual's physical National Identity Card and other identification documents (containing National Identity Card number or other identification numbers) should not be retained unless required by applicable country laws and regulations.

d) The suitability and reasonableness of alternatives to the National Identity Card number and other identification numbers must be assessed based on business and operational needs.

6. RECORD OF PROCESSING ACTIVITIES

6.1 The record of processing activity is a comprehensive internal documentation of all records of processing of Personal Data that the Group undertakes, to fulfil the Accountability obligation. It should list what data is used, how the data is processed, who the data is about, how long the data is held, where the data is shared and how the data is protected. It is used for documentation and analysis purposes.

6.2 It is a basic requirement, good practice and good business sense to keep proper, accurate and up-to-date documentation as mandated by every related law and international standard. It may be in a form of a single document or interconnected documents, e.g., data inventory map, data flow map, data consumer log, data transfer log, retention and disposal schedule.

6.3 It is a living document that is updated as and when necessary. Regular reviews should be conducted, at least annually, of the information to ensure that the documentation remains accurate, relevant and kept up to date.

6.4 The Record of Processing Activities is a legal responsibility of every Business and Function as it reflects the importance of the Accountability obligation and the Group's obligation to ensure and demonstrate that what we do with people's Personal Data is in accordance with applicable country Privacy laws and regulations.

6.5 Documenting the processing of Personal Data activities:

a) Is a Legal requirement

It helps the Group ensure and demonstrate compliance with other aspects of Privacy laws by providing inputs to the drafting of Privacy notices to individuals, responding to access requests by individuals, evaluating the Group's processing activities, and provides an overview of data transfers / flows.

b) Improves data governance and increase business efficiency

Such documentation provides management, regulator and our clients the assurance as to the quality, completeness and governance of Personal Data. Knowing what and how Personal Data is held and processed within the Group allows the development of more effective and streamlined business processes.

6.6 As required by Privacy laws, and depending on the applicability to Business / Function, the following information should be documented in the Record of Processing Activities:

	Data Fields	**Description**
a)	Name and Contact details of the Group entity	Identity and contact details of the organization
b)	Name and contact details of Data Protection Officer ("DPO")	Identity of the DPO with which the data falls under the remit of
c)	Process name, where available	Include process owner, where available, and other details as deemed necessary to link the processing activity
d)	Purpose of the processing	Explain the use of the Personal Data, e.g., marketing, client onboarding.
e)	Describe / Depict the processing activity	To enable linkage of fields
f)	Categories of individuals	To whom the Personal Data relates to, e.g., client, employee, third party.
g)	Categories of Person Data processed	Type of Personal Data, e.g., contact details, health data, financial data.
h)	Recipients of Personal Data	To whom Personal Data is shared with, e.g., service providers, regulators, agencies.
i)	Details of transfer to other country	Name of other countries or intra-Group entities to ensure legal, technical and organizational safeguards are in place.

	Data Fields	Description
j)	Processing with third parties	Identity third parties with whom data is transfer to / from.
k)	Retention schedules	How long data is to be kept for.
l)	Description of technical and organization controls	Document the safeguards to protect Personal Data.
m)	Source of Personal Data	Document where Personal Data is obtained from.
n)	Existence of automated decision-making, where available	Yes / No, logic involved and envisaged consequences.

7. PRIVACY NOTICE

7.1 A Privacy Notice is defined as a notice or statement setting out information on what Personal Data the Group obtains, why and how it is used. It is an artefact that seeks to inform the individual (e.g., client, staff, third parties) on what the Group does with their Personal Data, including what Personal Data you process, why are you processing it (i.e., purpose), what you do with it, where it came from, who you share it with and how long you will be keeping it for.

7.2 A Privacy Notice helps to demonstrate compliance with the Accountability, Notification and Purpose Limitation obligations. The Group must be open and upfront to individuals about the processing of their Personal Data, i.e., how is the data processed, why and with whom the data is shared with, how long it is retained, etc. It also includes informing the individual of what other rights are available to them.

7.3 Being open and transparent will allow the Group to discharge its legal obligation but also ensure that individuals are able to exercise their rights (refer to **Section 9 Individual Rights**). In being transparent, we are being fair to individuals when processing their Personal Data in a way that people would reasonably expect and helps you consider what effects it may have on them. Providing Privacy information that is clear and concise helps the Group meet the Purpose Limitation obligation, i.e., the Group must have specified, explicit and legitimate purpose for what the Group does with Personal Data, and any further use of the data must be compatible with those purpose.

7.4 Privacy information refers to the information that is required (by Privacy Laws) to be included in a Privacy Notice. The requirement differs for when Personal Data is collected directly from an individual, and when Personal Data has not been collected directly form the individual but from other sources, e.g., third parties.

	Information to provide	What should be told
a)	Name and contact details of the Group entity	• Who you are (e.g., entity name) • Contact details (e.g., address, phone, email)
b)	Name and generic contact details of DPO	Say how to contact the DPO (e.g., provide generic email address of DPO)
c)	Purpose of processing	Explain why you use their Personal Data. Typical purposes include marketing, application, staff administration
d)	The lawful basis for the processing	• Explain which lawful basis you are relying on in order to collect and use their Personal Data and/or Sensitive Personal Data where applicable • Explain what legitimate interests for the processing are, if appliable
e)	Categories of Personal Data obtained (from other sources) *Not applicable to direct collection*	Mention what types of information you collect about them (e.g., contact details, health history.)
f)	Recipients or categories of recipients, if applicable	Who you share their Personal Data with, including anyone that processes on your behalf; names of organizations or the categories that fall within such as regulators, credit reference agencies, service providers, etc.
g)	Details of transfers to any other countries, if applicable	• Tell them if you transfer their Personal Data to any other countries • Give brief information of safeguards put in place (cross border transfer rules may apply)
h)	Retention period	• State how long you will keep the Personal Data for • If no specific period, disclose the criteria you use to decide how long you will keep their data for
i)	Rights available to individuals in respect of the processing	• Indicate what rights they have in relation to your use of their Personal Data (e.g., access, rectification, erasure, restriction, objection, right to withdraw consent) and data portability • The rights will differ depending on the lawful basis for processing

	Information to provide	What should be told
j)	Right to withdraw consent (if consent is used as the lawful basis for processing), if applicable	• Inform them that they can withdraw their consent for your processing at any time (consent must be as easy to withdraw as it is to give) • Tell them how they can withdraw consent
k)	Right to lodge a complaint with the Data Protection Supervisory Authority	Tell them that they can complain to the Data Protection Supervisory Authority and provide the contact details and the process the Group takes to receive and respond to Privacy-related complaints.
l)	Source of the Personal Data *Not applicable to direct collection*	• Tell them where you obtained their information from, be as specific as possible and name the individual source(s). If don't know, provide more general information. • If it was from a publicly accessible source, you must mention it
m)	Details of whether individuals are under a statutory or contractual obligation to provide the Personal Data, if applicable *Not applicable to indirect collection*	Tell them if they are required by law or under contract to provide Personal Data to you, and what will happen if they don't provide it
n)	Details of the existence of automated decision-making including profiling, if applicable	• Tell them whether you make decisions based solely on automated processing, including profiling, that have legal or similarly significant effects on individuals • Give them meaningful information about the logic involved in the process • Explain the significance and envisaged consequences of the processing for the individual • How they can access details of the information used to create profiles about them • How they can object to any profiling (including for direct marketing purposes) • Based on lawful basis, do they have the right not to be subject to a decision based solely on automated processing

7.5 Privacy Notices must be in clear and plain language, be concise, transparent, intelligible, and easily accessible to the individual.

7.6 When a Privacy Notice should be provided:

a) Direct collection

A Privacy Notice should be provided at the time of collection of the individual's Personal Data

- Directly from the individual, i.e., when a client applies for a policy, we collect their data for Know Your Customer ("KYC") and policy setup purposes;
- By observation, i.e., when you use CCTV (relevant notices must be displayed); or
- Tracking people online using cookies – information can be provided via a cookie policy.

b) Indirect collection

A Privacy Notice should be provided within a reasonable period no later than 1 month

- From another individual or organization, e.g., when you buy leads or it is shared with you
- From a publicly accessible source, e.g., from social media, public websites
- If there are plans to use the Personal Data obtained to communicate with the individual it relates to or to disclose to someone else, the latest point at which the Notice must be provided is when you first communicate with the individual or disclose their data to someone else
- The specific circumstances of the use of Personal Data must be considered in deciding when it would be reasonable to provide Privacy information to the individual, i.e., as soon as possible after obtaining their Personal Data where:
  - The use of their Personal Data is likely to be unexpected or unwelcome;
  - The use of their Personal Data is likely to have a significant effect on the individual; or
  - Sensitive Personal Data has been obtained.

7.7 Privacy Notice can be provided in a range of ways, not just restricted to a single notice or page on the website, e.g.,

- Orally, i.e., face to face or when you speak on the telephone (do document the call log)
- In writing, i.e., printed media, application forms
- Signage, i.e., information poster in a public area
- Electronically, i.e., in text messages, websites, emails, mobile apps or smart device functionalities

7.8 It is preferable to use the same medium that is used to collect the Personal Data, to deliver the Privacy Information. For example,

- If information is collected through an online form, provide the notice on the form as the individual fills up the form
- Combine this with more detailed information on our website, by including a clear and prominent link on the form which the individual can access

Always focus on the individual when making decisions about the way to deliver the Privacy Information.

8. DATA PROTECTION IMPACT ASSESSMENT ("DPIA")[2]

8.1 A DPIA is a mechanism to help identify and manage privacy risks arising from the processing of Personal Data throughout the life cycle of projects and processes (systems, products, services, activities).

8.2 DPIAs help to demonstrate that privacy risks have been considered and mitigated, and thus are one of the ways to fulfil the Accountability obligations in accordance with country laws and regulations around Data Protection.

8.3 DPIAs also ensure that stakeholders embed Privacy by Design, i.e., think about Privacy and how to incorporate Privacy considerations at the earlier stages of project/process life cycles, when there is the most scope for shaping how the initiative is to be implemented. Privacy by Design is essentially about integrating Data Protection into all projects and processes (systems, products, services or activities) right from the design phase and throughout its life cycle. This will enable the Group to address our clients' expectations around how their Personal Data is used and protected. Considering Privacy risks upfront helps the Group to comply with regulatory obligations.

8.4 When an individual's Personal Data is processed, we expose that individual to several potential risks, e.g., identity theft, service unavailability, data breaches, financial or reputational damage. As such, the objective of conducting a DPIA is to:

a) Identify the Personal Data to be processed and the purpose for the processing
b) Identify and assess the privacy risks arising from the process
c) Address and mitigate identified risks by modifying the processing operations or implementing controls

8.5 A DPIA should be conducted prior to carrying out any processing of Personal Data. By conducting a DPIA, it helps the Group demonstrate that we have considered and mitigated privacy risks. Other than being one of the ways to fulfil our Accountability obligation, it is driven by regulatory requirement to provide clear documentary evidence that privacy risks have been appropriately evaluated and mitigated where appropriate.

8.6 It is important to conduct a DPIA at the early stages of project and process design, i.e., Privacy by Design, as it incorporates Privacy compliance at the initial stages when there is the most scope of shaping how the initiative is implemented. Consistent and correct use of DPIA will also improve the Privacy awareness across the Group.

8.7 A DPIA is required in the following instances:

a) New projects or processes (systems, products, services or activities) involving Personal Data, includes applications or APIs allowing for data transfer
b) Material change to existing product or processes (systems, products, services or activities) relating to how Personal Data is processed
c) New Third party engagement involving the processing of Personal Data

[2] Note that while the scope of DPIA that is rolled out by the Group covers both Critical and Personal Data, this Standard focuses on the Privacy obligations that pertains to Personal Data only. As such, references to DPIA in this Standard pertain only to Privacy obligations. For further coverage of Critical Data, refer to the Data Management framework and policy documents.

d) Change of Third party or change to the scope of processing of Personal Data by the Third party

8.8 Specific to 8.7b) above, material change triggering a DPIA review or a reassessment of an existing DPIA may include, but is not limited to:

- Significant change to how Personal Data will be processed
- Increase or decrease in the amount of Personal Data
- Change in the purpose for the processing Personal Data
- New technology/system/API will be used which may affect how Personal Data is processed, secured or transferred
- New/additional categories of Personal Data to be shared with Third Party
- Change in service and purpose of processing Personal Data by Third Party
- Change in location from where the Third Party service is provided or servers located
- Change/addition of sub-contractor

8.9 DPIA is dynamic and is a continuous exercise. It should be reviewed and reassessed periodically to ensure new identified risks are minimized. Controls identified in DPIAs to mitigate risk should be tested on a regular basis to ensure they are effective and remain appropriate.

8.10 Generally, a DPIA is not required when the processing of Personal Data is unlikely to result in material privacy risks to the rights and freedom of individuals. This would include:

a) Where there is no processing of Personal Data;
b) Where there is no material change to the existing scope or purpose of Personal Data in relation to renewals of third-party contracts (where a DPIA had previously been conducted), and updates to existing products, system processes or activities; or
c) Intra-Group outsourcing arrangements, e.g., annual reviews of intra-group Service Level Agreement.

8.11 The DPIA generally should include at a minimum:

a) Description of the impacted project or process (product, service, system, activity)
b) Personal Data impacted and related details (data source, who it relates to, collection purpose)
c) Data flows
d) Supported technology and any related security risk assessment conducted, e.g., Information Security Risk Assessment (“ISRA”)
e) How individuals are notified of the processing of Personal Data
f) How individuals have consented to the processing of Personal Data
g) Location of processing
h) Data accuracy controls implemented
i) Data security / protection controls implemented
j) Data retention and disposal control implemented
k) Third party Risk assessment, where applicable

8.12 The DPIA for Third Party engagement (“TPDPIA”) focuses mostly on the privacy risks and controls related to the third party and makes sure any privacy risks arising due to processing Personal Data are identified and mitigated early in the lifecycle of the engagement. Thus, it should include at a minimum:

- The nature of the Personal Data to be shared with them or processed by them on behalf of the Group
- The type of processing that they will conduct on the Group's behalf
- The location of processing
- Due diligence of the Third Party's Privacy framework
- Periodic monitoring of the Third Party
- Results of the Third Party Information Security Assessment ("TPISA"), as covered under the relevant Information Security and Technology Management policies and standards, may be used as references in the TPDPIA.

9. INDIVIDUAL RIGHTS

9.1 Right to be informed about the collection and use of Personal Data

a) Where Personal Data is obtained directly, the individual must be immediately informed, meaning at the time the data is obtained.

b) If Personal Data is not obtained from the individual, he/she must be provided the information within a reasonable period of time, but at latest after 1 month. In cases where the gathered information is used to directly contact the individual, he/she has the right to be informed immediately upon being approached. In addition to the required content as when the data is obtained directly, the Group has the obligation to inform from what sources the Personal Data originated and whether it was publicly available. Notification must be in a precise, transparent, comprehensible and easily accessible form. The right to inform can be fulfilled in writing or electronic form. So-called "standardized image symbols" may be used in order to convey a meaningful overview of the intended processing in an easily comprehended, understandable and clear form.

c) In the case that the personal data is not gathered from the individual, in exceptional cases there is no obligation to inform. This applies, if providing the information is either impossible or unreasonably expensive, the gathering and/or transmission is required by law, or if the data must remain confidential due to professional secrecy or other statutory secrecy obligations.

9.2 Right of access to their Personal Data

a) Upon request by an individual, the Group shall provide the individual with the following as soon as reasonably possible:
   - Personal Data about the individual that is in the possession or under the control of the organisation; and
   - information about the ways in which that personal data has been or may have been used or disclosed by the organisation within a year before the date of the individual's request.

b) Exceptions to access to Personal Data are as follows:
   - Where the access to Personal Data:
     - Causes immediate or grave harm to the individual's safety or physical / mental health
     - Threatens the safety or physical / mental health of another individual
     - Reveals Personal Data about another individual
     - Reveals the identity of another individual
     - Be contrary to national interest

- Where the Personal Data relates to:
  - An opinion kept solely for an evaluative purpose
  - Personal Data about the beneficiaries of a private trust kept solely for the purpose of administering the trust
  - Personal Data kept by an arbitral institution or mediation center solely for the purposes of arbitration or mediation proceeding
  - Documents related to a prosecution where related proceedings have not been completed
- Repetitious requests that would unreasonably interfere with the operations of the Group
- Requests where the burden or expense of granting access would be unreasonable to the Group or disproportionate to the individual's interest
- Requests for information that does not exist or cannot be found
- Requests for trivial information
- Frivolous or vexatious requests

c) Before responding to an access request, the Group should exercise due diligence and adopt appropriate measures to verify the individual's identity.

d) The Group should ask the applicant to be more specific as to what type of personal data he requires, the time and date the personal data was collected, to facilitate the processing of the access request or to determine whether the request falls within one of the prohibitions.

e) If there are any associated fees to be imposed on access request related to the provision of access to Personal Data, the Group shall provide a written estimate of the associated fees imposed upon receipt of such access request. The fee should be assessed based on the request and effort needed to retrieve the information.

f) When assessing an access request, the Group should consider the purpose of the applicant's access request to determine the appropriate manner and form in which access to the personal data should be provided. If the individual is unable or unwilling to provide more details, the Group should make an attempt to respond to the access request as accurately and completely as reasonably possible.

g) If the Group is unable to respond to an access request within 30 days after receiving the request, the Group shall inform the individual in writing within 30 days of the time by when it will be able to respond to the request.

h) When an access request cannot be fulfilled, the Group shall respond to the individual providing the reason for rejection. The Group shall also annotate that an access request to the Personal Data has been made but rejected.

9.3 Right to rectify / correct inaccurate or incomplete Personal Data

a) An individual may request the Group (in writing and must include sufficient detail to enable the Group, with reasonable effort, to identify the applicant making the request, and the correction requested by the individual) to correct an error or omission in his/her Personal Data that is in the Group's possession or control.

b) Unless the Group is satisfied on reasonable grounds that a correction should not be made, the Group shall:
   - Correct the Personal Data as soon as practicable; and
   - Send the corrected Personal Data to:
     - Every other organization to which the Personal Data was disclosed by the Group within a year before the date the correction was made, unless the other

organization does not need the corrected Personal Data for any legal or business purpose; or
    - Specific organizations to which the Personal Data was disclosed by the Group within a year before the date the correction was made, if the individual consents.

c) When the Group is notified (by the organization which the Personal Data had been collected from) of a correction of Personal Data, the Group shall correct the Personal Data in its possession or control unless the Group is satisfied on reasonable grounds that the correction should not be made.
d) If no correction is made, the Group shall annotate the Personal Data in its possession or under its control with the correction that was requested but not made.
e) Exceptions to correction are as follows:
    - An opinion kept solely for an evaluative purpose
    - Personal Data about the beneficiaries of a private trust kept solely for the purpose of administering the trust
    - Personal Data kept by an arbitral institution or mediation center solely for the purposes of arbitration or mediation proceeding
    - Documents related to a prosecution where related proceedings have not been completed

9.4 Right to erasure / removal of their Personal Data

a) Upon request, the Group shall delete the Personal Data in the Group's possession or control without undue delay. Subject to country laws and regulations around data retention, deletion may apply to where:
    - The Group no longer needs the data for the original reason it was collected or used
    - An individual withdraws consent to the Group's processing of their Personal Data
    - An individual objects to the Group's use and there are no legitimate grounds for the Group to continue to process their data
    - Data has been collected or used unlawfully (see **Section 5 Lawful Basis**)
    - The Group has a legal obligation under country laws and regulations to delete the data
b) The right to erasure may not apply if the processing is necessary:
    - To exercise the right of freedom of expression and information
    - To comply with a legal obligation
    - For the performance of a task carried out in the public interest or in the exercise of official authority
    - For archiving purposes in the public interest, scientific research, historical research or statistical purposes where erasure is likely to render impossible or seriously impair the achievement of that processing
    - For the establishment, exercise or defense of legal claims
    - If the request is manifestly unfounded or excessive

9.5 Right to data portability of their Personal Data

At the request of the individual, the Group shall transmit the individual's data that is in the Group's possession or under its control, to another organization in a commonly used machine-readable format.

9.6 Right to opt out of, restrict or object to the processing of their Personal Data

a) On giving reasonable notice, an individual may at any time withdraw any consent given, or deemed to have been given, with respect to the processing of Personal Data for any purpose, and the Group shall not prohibit the individual from withdrawing the consent.
b) On receipt of the withdrawal of consent notice, the Group shall:
    - Inform the individual of the likely consequences of withdrawing his/her consent, and
    - Cease (and cause its data intermediaries and agents to cease) the processing of the Personal Data within the timeframe as stipulated by applicable country laws and regulation, unless such processing without the consent of the individual is required or authorized under applicable country laws and regulation.

10. DISPENSATION AUTHORITIES

Dispensations to this Standard must be approved by the Standard Owner or delegate.

11. RELATED POLICIES / STANDARDS

Document Name	**Document Owner**
Data Risk Governance Framework	Group Chief Risk Officer
Data Management Policy	Group Chief Risk Officer
Data Incident and Breach Management Standard	Data Risk
Records Retention Schedule	Data Risk
Records Disposal Schedule	Data Risk
Group Privacy Policy	Compliance

12. GLOSSARY

Term	**Definition**
Anonymization	It refers to the conversion of Personal Data into data that cannot be used to identify any individual.
Automated Decision-Making	It refers to the process of making a decision by automated means without any human involvement. These decisions can be based on factual data, as well as on digitally created profiles or inferred data.
Cookie Notice	It is a form of Privacy Notice that sets out information on what cookies is being used, how they are used, the types of cookies used and details on how to manage cookie preferences. It is a technology that enables an “online memory” of an individual’s activity and actions performed while they browse web pages using their device. It may collect and store Personal Data about the individual operating the device, including but not limited to, a unique identification code, Internet Protocol (“IP”) address, geolocation, website preferences, previous web pages visited and log-in information.

Term	Definition
Cross Border Transfer	Occurs when Personal Data can be or is stored, accessed from, viewed from, sent to or otherwise processed to another country.
Data Controller	Also known as Organization See definition for “Organization”
Data Intermediary	Also known as Data Processor It refers to an organization that processes personal data on behalf of another organization but does not include an employee of that other organization. Only the Protection, Retention Limitation and Data Breach Notification Obligations apply to the Data Intermediary in relation to the personal data processed on behalf and for the purposes of another organization. The other organization is still responsible for complying with all the Privacy obligations for the Personal Data processed on its behalf and for its purposes by a Data Intermediary.
Data Protection Impact Assessment	A mechanism used to help identify, assess and minimize the potential impact on and the privacy risks to an individual resulting from the processing of Personal Data throughout the life cycle of a project or process (product, system, service and activity).
Data Processor	Also known as Data Intermediary See definition for “Data Intermediary”
Data Protection Supervisory Authority	It refers to an independent public authority that supervises the application of the data protection law, handles data breach reports and protects the fundamental rights and freedoms of individuals (data subjects) related to the processing of Personal Data.
Data Subject	Also known as Individual See definition for “Individual”
Do not Call (“DNC”) Registry	It refers to the national registers of telephone numbers set up by the relevant Data Protection Supervisory Authority for subscribers to add or remove his/her telephone number for organizations to check and perform the filtering out of the registered telephone numbers before they send any marketing messages.
Entity	Refers to an individual, partnership, joint venture or organization that has a separate identifiable existence.
External Third Party	Refers to a third party that is not part of Group

Term	Definition
Individual	Also known as Data Subject It refers to a natural person, whether living or deceased.
Joint Data Controller	It refers to where 2 or more data controllers jointly decide why and how to process Personal Data.
Organization	Also known as Data Controller It refers to any individual, company, association or body of persons regardless of whether it is or is not formed or recognized under the applicable country law and whether it is or is not resident or has a place of business, in the country. It excludes: • An individual acting in a personal or domestic capacity; • An employee acting in the course of his employment; and • A public agency or an organization acting on behalf of a public agency in relation to the collection, use or disclosure of the personal data.
Personal Data	Data about an individual who can be identified from that data on its own; or when that data is combined with other information the organization (in this case, the Group) possesses, e.g., name, national identification number, work pass number, passport number, mobile number, address, photo. It includes personal data in electronic and non-electronic forms, e.g., paper documents, computer systems, audio recordings, video recordings, images. Specific to Singapore: a) It includes: • personal data that is false or true • personal data of deceased individuals for 10 years after the date of death. b) It excludes: • business contact information, i.e., information about an individual that is typically printed on a business name card and is provided by the individual for a business purpose and not for personal purposes.
Personal Data Breach	Relates to: • 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. This includes breaches of both accidental and deliberate causes.

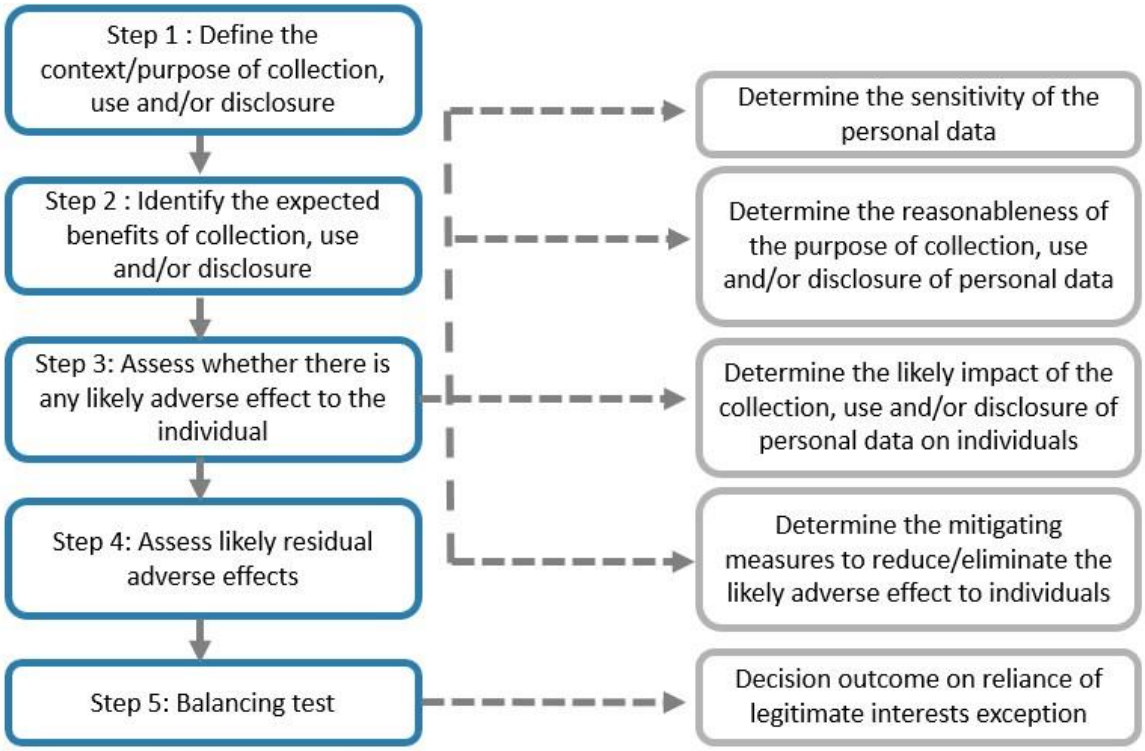
Term	Definition
	Refer to Data Incident and Breach Management Standards for Personal Data Breach handling requirements.
Privacy by Design	A data privacy concept that calls for the incorporation of data privacy protection into all projects and processes (systems, products, services or activities) from the design phases and throughout its life cycle. The goal of Privacy by Design is to prevent data privacy breaches and protect the privacy of individuals by proactively incorporating data privacy safeguards into systems and processes. It is rooted in the principle that data privacy should be built into systems and processes from the ground up, rather than being tackled as an afterthought or overlooked altogether.
Privacy Notice	A notice or statement setting out information on what Personal Data the Group obtains, why and how it is used.
Privacy Risk	The risk of failing to process Personal Data in a manner that is respectful, appropriate, secure and limited to the minimum necessary for the intended purpose may lead to a breach of personal data protection laws and regulations, resulting in censure, fines and/or penalties and damage to branding.
Processing of Personal Data	It refers to any operation or set of operations (or activity) that is performed on Personal Data. It includes, but is not limited to, adapting, blocking, collecting, combining, consulting, destroying, disclosing, disseminating, erasing, obtaining, recording, organizing, retaining, retrieving, storing, transmitting, transferring, using or viewing.
Pseudonymization	A technique that involves replacing information that are easily attributable to identifiable individuals (e.g., name) with, e.g., reference number.
Record of Processing Activities	A comprehensive documentation of all processing of Personal Data undertaken to fulfil the Group's Accountability obligation.
Sensitive Personal Data	Categories of Personal Data considered to be sensitive in nature and which therefore require a higher level of protection. They include: • Racial or ethnic origin • Political opinions • Religious or philosophical beliefs • Genetic data • Biometric data • Health data • Sexual orientation or sex life

Term	Definition
	• Criminal allegations, proceedings or convictions • National Identity Card Number[3] • Birth Certificate Number[3] • Passport Number[3] • Work Permit Number[3] • Minor's data[3] • Financial and insurance data[3]
Third Party	Refers to a legal entity that has entered in a business relationship or contract with the Group to provide goods, products or services. Also includes relevant sub-contractors.
Vendor	Refers to an external third party that has a commercial arrangement with the Group for the provision of goods, products or services.

APPENDIX A – ASSESSMENT FOR LEGITIMATE INTEREST EXCEPTION

(Adapted from: https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Advisory-Guidelines/AG-on-Key-Concepts/Annex-C--Assessment-Checklist-for-Legitimate-Interests-Exception-1-Feb-2021.pdf?la=en

Figure 1: The flow for conducting legitimate interest exception assessment



[3] Specific to Singapore

Assessment for
Legitimate Interest Ex