Group Privacy Policy

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	27 Jul 2022	New – replaces the following: i) Aviva Ltd. Personal Data Protection Compliance Policy (full version) v1.3 dated 13 Apr 2020 ii) Aviva Ltd. Personal Data Protection Compliance Policy (abridged version) v1.9 dated 19 Jan 2021	Sharon Tan, Senior Manager	Edwin Ti, Director of Compliance; Michael Puhaindran, Group Head Legal & Compliance; Ashley Tan, Group Chief Risk Officer
1.1	27 Oct 2023	Key changes: • Updated Singlife logo • Expanded scope to include third parties • Defined “staff” • Added further clarity on DPIA requirements • Updated policy/standards document names and/or document owners	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 policy sets out the minimum requirements that the Singlife Group needs to comply with to fulfill its Privacy (also referred to as Data Protection obligations) and its commitments as reflected in the following to address Privacy risk:

Obligations under Data Protection

i) Accountability Obligation
ii) Notification Obligation
iii) Consent Obligation
iv) Purpose Limitation Obligation
v) Accuracy Obligation
vi) Protection Obligation
vii) Retention Limitation Obligation
viii) Transfer Limitation Obligation
ix) Access and Correction Obligation
x) Data Breach Notification Obligation
xi) Data Portability Obligation

1.2 Country laws and regulations may also establish Do Not Call or similar provisions ("DNC") which allow individuals to register their country-registered telephone numbers on the national DNC registry to opt out from receiving marketing phone calls, mobile text messages such as Short Message Service ("SMS") or Multi-media Messaging Service ("MMS"), and faxes from organizations and prescribes obligations for organizations in relation to the sending of specified messages to country-registered telephone numbers. The DNC provisions considered in this policy, where applicable to country, shall include:

Obligations under the DNC provisions

i) Duty to check the DNC Registry
ii) Duty to provide contact information of the sender and not conceal the sender's calling line identity

1.3 Also covered under these provisions is the prohibition of sending applicable messages to any telephone number generated or obtained using dictionary attack or address-harvesting software.

1.4 This policy is aligned with:

- The Personal Data Protection Act 2012 ("PDPA") in Singapore as the baseline for the Group;
- The Directions issued by the Monetary Authority of Singapore (being the financial regulatory authority for the Group company) under the Financial Holding Companies Act 2013;
- Recognised industry good practice;
- The Data Risk Governance Framework; and
- Group Risk Managment Framework.

1.5 Subject to country laws and regulations, Privacy laws or an appointed Data Protection Supervisory Authority may set out requirements to:

- govern the collection, use, disclosure and care of personal data in the country by organizations;
- recognize both the rights of individuals to protect their personal data, including the rights of access and correction, and the needs of the organization to collect, use or disclose personal data for legitimate and reasonable purposes; and
- govern the transfer of Personal Data outside the country.

1.6 For the purpose of this policy, the requirements apply to any organization (regardless of its country of incorporation or physical presence) that collects, uses or discloses personal data in the country and its data intermediaries that process personal data on behalf of and for the purposes of the organization.

2. SCOPE

2.1 This policy applies to:

- Singapore Life Holdings Pte. Ltd. and its group of companies (collectively labeled 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;
- third parties, including partners, agents and service providers, where applicable, who process Personal Data belonging to the Group;
- 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.

2.2 Unless otherwise specified, any reference to "Staff" in this policy includes employees and independent contractors as described in para 2.1.

3. ROLES AND RESPONSIBILITIES

3.1 **Privacy Compliance** is part of the Group Compliance function and is responsible for:

a) Being the Group Data Protection Officer and Subject Matter Expert for Privacy risk;
b) Reviewing all policies and standards / procedures related to Privacy;
c) Informing and advising the Group on its Privacy obligations, monitoring and reporting compliance with these obligations;
d) Providing advice and guidance on Privacy obligations in the Data Protection Impact Assessments escalated in line with the Data Protection Impact Assessment process; and
e) Providing advice and guidance on Personal Data Breaches escalated in line with the criteria set out in the Data Incident and Breach Management Standard

3.2 **Data Risk team** is part of the Group Risk Function and is responsible for:

a) Overseeing the management of critical data (which may include Personal Data) held within the Group's possession as set out in the Data Management Policy;

b) Providing advice and guidance on the requirements of the record of processing activities as set out in Data Inventories, Data Maps and Data Consumer Logs;
c) Providing advice and guidance on the retention and disposal of data as set out in the Records Retention and Records Disposal Schedules; and
d) Reviewing and handling Personal Data Breaches escalated in line with the criteria set out in the Data Incident and Breach Management Standard.

3.3 Each **Data Protection Officer** ("DPO") is a member of the Group Business / Function and is responsible for:
a) Informing and advising their respective Business / Function on its Privacy obligations;
b) Ensuring that relevant standards / procedures / manuals owned by their respective Business / Function are aligned with the requirements as set out in this policy and related standards;
c) Monitoring and reporting compliance with the Privacy obligations within their respective Business / Function to Group Privacy Compliance, being the Group DPO;
d) Providing advice and guidance on Privacy obligations in the Data Protection Impact Assessments ("DPIA") for their respective Business / Function and escalated in line with the DPIA process;
e) Providing advice and guidance on and handling Personal Data Breaches for their respective Business / Function escalated in line with the criteria set out in the Data Incident and Breach Management Standard;
f) Reporting to Group Privacy Compliance any Privacy risk which could cause a material impact on the Group;
g) Handling privacy related questions/complaints for their respective Business / Function from employees and anyone else covered by this policy;
h) Dealing with requests for their respective Business / Function from individuals to access the Personal Data or other information that the Group holds about them;
i) Reviewing and approving any contracts / agreements for their respective Business / Function with third parties that may handle Personal Data; and
j) Maintaining a list of the various Personal Data collection processes for their respective Business / Functions to ensure that all aspects of Personal Data processing are well monitored and addressed.

3.4 Each **Compliance Liaison Officer** ("CLO") is a member of the Group Business / Function who is responsible for working with their respective DPOs to:
a) Review, maintain and update documentation of their respective Business / Function's manner of compliance to applicable Privacy laws and regulations in their Functional Area Regulatory Obligation Mapping ("FAROM") template; and
b) Assist Compliance with the annual FAROM Attestation to applicable Privacy laws and regulations. The objective of the attestation is to provide assurance to Board and Senior Management of Singlife that necessary controls and procedures have been established within the functional units to comply with applicable Privacy laws and regulations.

3.5 **Group Heads of Business / Functions** are responsible for implementing this policy in their respective areas and should do so through their respective Data Protection Officers and Data Owners. The **Data Owner** is responsible for the First Line of Defense for data management within each Business / Function. The responsibilities include:

a) Knowing what Personal Data is processed, how and why, by / for their respective Business / Function so that Personal Data is processed in line with the requirements of this policy;
b) Determining the business purpose and lawfulness for any processing of Personal Data, and managing any new processing by the Business / Function, or changes to existing processing in accordance with this policy;
c) Taking reasonable steps to ensure that any processing of Personal Data by or on behalf of their Business / Function is compliant with this policy and developing procedures or department operating instructions to adopt this policy;
d) Understanding all Privacy risks applicable to their Business / Function and actively monitor, manage and mitigate these risks in accordance with the agreed Group risk appetite;
e) Validating that all employees and Third Party workers who work for their Business / Function have been appropriately trained on Privacy; and
f) Reporting any Personal Data Breach originating from their respective Business / Function in accordance with the requirements of this policy.

3.6 **Process Owners** are Business / Function managers in the First Line of Defense who are responsible for the end-to-end Business / Function processes. Process owners are responsible for any risks associated with or created by their process(es) regarding Privacy and must assess the applicability of this policy to their process(es) and comply with the requirements of this policy.

4. POLICY REQUIREMENTS

4.1 **Know what Personal Data you are Processing and why.**

a) Identify what Personal Data the Business / Function is processing and the business purpose for processing the data.
b) Determine the lawful basis for the business purpose identified and for the processing.
c) The processing of Personal Data (including, but not limited to, collection, use, disclosure, transfer, retention and disposal) should be limited only to the extent that it is necessary and reasonable to meet legitimate business purposes and based on the specific purpose for which individuals have given consent.

4.2 **Record what Personal Data you are using, why and how.**

Maintain an accurate Record of Processing Activities for the Business / Function, including any Cross Border Transfer of Personal Data within the Group and/or externally.

4.3 **Be transparent about your use of Personal Data**

a) Maintain accurate and up-to-date Privacy Notices, including but not limited to, Cookie Notices.
b) Provide a Privacy Notice to individuals whose Personal Data is collected.
c) Provide information to individuals on request about the process to receive and respond to Privacy-related complaints. This information may be made available as part of the Privacy Notice.

4.4 **Keep Personal Data accurate; destroy it securely when no longer required.**

a) Verify that Personal Data is accurate and kept up-to-date. The accuracy of Personal Data must be managed in accordance with the Data Management Policy.

b) Personal Data should be retained no longer than for the purpose it was obtained for and in accordance with applicable country laws and regulations. Identify the appropriate retention period for Personal Data (in accordance with the Records Retention and Records Disposal Schedules) and ensure that it is destroyed (or irreversibly anonymized, if appropriate) after the retention period has elapsed, unless required by law or other mandatory obligation to retain it.
c) All destruction of Personal Data must comply with the relevant applicable Information Security and Technology Management policies and standards.

4.5 **Embed Privacy into the Business' / Function's ways of working (i.e., Privacy by Design)**

a) Consider the Privacy implications and risks to individuals associated with the day-to-day operations, e.g., new product / service development, new process or project initiative, material changes to existing product / service, material changes to existing ways of working.
b) Conduct a Data Protection Impact Assessment ("DPIA"), where required, before Personal Data is processed within periodic review timeframes, i.e.,
   - when developing a new product / service, process or project initiative; or
   - when there are any material changes to the underlying product / service / process / project or supported Information System.
c) Conduct a security risk assessment of the product / service / process / project initiative, i.e., Information Security Risk Assessment ("ISRA"), where applicable, which will be processing Personal Data, in accordance with the relevant Information Security and Technology Management policies and standards.
d) All DPIAs must be logged and tracked till closure, i.e., agreed actions completed.

4.6 **Keep Personal Data Secure**

Reasonable steps must be taken to ensure that Personal Data is processed securely by adhering to the relevant Information Security and Technology Management policies and standards, which cover the technical and organizational security controls and measures.

4.7 **Manage Third Party Privacy Risks**

a) Consider the Privacy considerations and risks to individuals associated with the products/services provided by a Third Party.
b) Conduct a DPIA of the Third Party engagement ("TPDPIA") before sharing Personal Data with them.
c) Conduct a security risk assessment of the Third Party, i.e., Third Party Information Security Assessment ("TPISA") which the Business / Function is sharing Personal Data with, in accordance with the relevant Information Security and Technology Management policies and standards.
d) Ensure a legally enforceable written contract as approved by Legal is put in place before Personal Data is shared or transferred to a Third Party. At a minimum, the contract must include:
   - Appropriate data protection obligations on the Third Party as a Data Intermediary (Data Processor), Data Controller or Joint Data Controller where applicable. Where the Third Party is providing the Group with any Personal Data, this must also include appropriate contractual confirmation, and a right to receive supporting documentation, that the Personal Data processed and shared with the Group is in line with applicable Privacy laws and regulations.

- Any specific contractual provisions required to comply with applicable Privacy laws and regulations relating to Cross Border Transfer of Personal Data.
- Any obligation on the Third Party to report any Personal Data Breach to the Group without any undue delay and in line with the Data Breach requirements and timeframe.
- In relation to material outsourcing, appropriate representation from the Third Party about the location where Personal Data will be processed, including the requirement for the Third Party to give reasonable notice to the Group in advance on any proposal of location change.

e) Know which Third Parties Personal Data is shared with and what Personal Data is being shared, by:
   - Maintaining an updated list of Third Parties with which the Business / Function has contracted to provide services that involve the processing of Personal Data.
   - Documenting what Personal Data is shared with Third Parties, including the transfer mechanism used.

f) Maintain a procedure to identify, handle and address any instances of contractual non-compliance by any Third Party.

g) Take reasonable steps to minimize Personal Data shared with Third Parties, i.e., ensure that access to Personal Data is limited to what is required to provide the contracted service.

h) Upon termination of any arrangement, verify that any Personal Data that the Third Party processes on behalf of the Group is securely destroyed or repatriated in accordance with the relevant Information Security and Technology Management policies and standards.

4.8 **Manage Cross Border Transfers of Personal Data Appropriately**

a) Conduct a risk assessment of the factors related to the transfer of Personal Data to another country before commencing the processing of Personal Data. At a minimum, the following should be assessed:
   - Level of protection afforded to Personal Data against government surveillance and access in the importing country.
   - Assessment of the risk by reference to the format and nature of the Personal Data, including the length and complexity of the transfer.
   - If Personal Data is within the scope of intelligence and law enforcement activities.
   - The legal framework or applicable privacy and security standards in the country where Personal Data is transferred to, including any onward transfers.
   - The general human rights of the country.

   The assessment should be conducted before the commencing of Personal Data processing.

b) Ensure that there are legally enforceable obligations imposed on the recipient to provide to the transferred Personal Data a standard of protection that is at least comparable to that of the originating country under any applicable country law;
   - any contract which imposes such standard of protection;
   - any binding corporate rules;
   - any other legally binding instrument, or

   Ensure that the recipient organization holds a specialized certification, e.g., Asia Pacific Economic Cooperation Cross Border Privacy Rules (“APEC CBPR”) System Certification applicable to Data Controllers, or APEC CBPR Certification or Asia Pacific Economic Cooperation Privacy Recognition for Process (“APEC PRP”) System Certification.

c) Where legally enforceable obligations or specialized certifications cannot be relied on, ensure that one of the following circumstances apply:

- The individuals whose Personal Data are to be transferred have given their consent to the transfer of their Personal Data after being informed about how their Personal Data will be protected in the destination country;
- The transfer relates to the processing Personal Data under the lawful basis of contract;
- The transfer is necessary for a use or disclosure that is in the vital interests of individual or national interest, and the transferring organization has taken steps to ensure that the Personal Data will not be used or disclosed by the recipient for any other purposes;
- The Personal Data is data in transit; or
- The Personal Data is publicly available.

d) Know what Personal Data you are sharing within the Group and externally, by documenting the Cross Border Transfer of Personal Data for each process in the Record of Processing Activities.

e) Maintain appropriate contractual mechanisms for Cross Border Transfer of Personal Data, as approved by Group Legal.

4.9 **Handle Requests and Complaints from Individuals**

a) Respond to requests and complaints from individuals who may exercise any rights that they may have in relation to their Personal Data held by the Group. Requests may include:
- Requests to access Personal Data.
- Requests to opt out of, restrict or object to the processing of their Personal Data.
- Right to rectify Personal Data.
- Requests for Personal Data portability.
- Requests for removal or erasure of Personal Data.
- Complaints relating to Privacy matters, which could include complaints made directly to the relevant Data Protection Supervisory Authority.

b) Respond to requests from individuals to exercise any rights that they may have in relation to their Personal Data within 30 calendar days after receiving the request or within the applicable timeframe under applicable country laws and regulations (whichever is earlier).

c) The Group may reject the request if the information provided is insufficient to process the request, or if the request pertains to certain exceptions as stipulated by applicable country laws and regulations. In such cases, the applicant must be notified as per the timeframe set out in Para 4.9b with reasonable information.

d) Log, track and close all requests and complaints received within a reasonable timeframe or as stipulated by country laws and regulations.

4.10 **Manage Personal Data Breaches Appropriately**

a) Train all employees to understand the process to report any incident that may or may not result in a Personal Data Breach without delay (and no later than 24 hours of becoming aware of the incident).

b) Handle any potential or actual Personal Data Breach in accordance with the Data Incident and Breach Management Standard to enable any Personal Breach to be reported:
- By authorized staff as set out in the Regulatory Contact Standards, and
- By the applicable Business / Function to any affected individual in accordance with the applicable country requirements.

c) Report all Personal Data Breaches to the Data Protection Officer, Data Risk team and Group Privacy Compliance.

5. TRAINING AND AWARENESS

5.1 All employees, including independent contractors, must be made aware, through learning and development, of their roles and responsibilities relating to the Privacy obligations.

5.2 People leaders are responsible for ensuring that their staff completes all mandatory Privacy training.

6. GOVERNANCE AND MONITORING

6.1 A monitoring program of Privacy controls and practices, in accordance with the Integrated Assurance Framework process mandated by Group Operational Risk, must be maintained. At a minimum, it should include:

a) Defining monitors (such as key control indicators and control sample tests) and setting benchmark thresholds for key controls to provide early warning of potential problems and indicate where risk exposure may be elevated due to ineffective controls.
b) Performing monitoring activities.
c) Assessing the operating effectiveness of the Privacy controls using the outputs of the key control monitoring. Where a key control is deemed ineffective, assign and track actions to improve it.

6.2 Departments that handle Personal Data shall carry out periodic reviews to ascertain that the department's standards/procedures and guidelines in managing Personal Data are compliant with this Policy.

6.3 The DPO / CLO / designated staff shall conduct at least once every calendar year a review of the adequacy of related controls and processes against the Privacy obligations to ensure compliance with applicable Privacy laws and regulations, e.g., through the FAROM process.

7. DISPENSATION AUTHORITIES

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

8. RELATED POLICIES / STANDARDS

Document Name	**Document Owner**
Group Risk Management Framework	Board of Directors
Data Risk Governance Framework	Group Chief Risk Officer
Data Management Policy	Group Chief Risk Officer
Integrated Assurance Framework	Group Operational Risk
Data Incident and Breach Management Standard	Data Risk
Records Retention Schedule	Data Risk
Records Disposal Schedule	Data Risk
Information Security Policy	Group Chief Information Security Officer

Document Name	Document Owner
Technology Management Policy	Group Chief Information Security Officer
Information Security Standard	Group Chief Information Security Officer
Group Privacy Standard	Compliance
Regulatory Contact Standard	Compliance

9. GLOSSARY

Term	Definition
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 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.
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 Processor	Also known as Data Intermediary. See definition for "Data Intermediary".

Term	Definition
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 lifecycle of a project or process (product, system, service and activity).
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, e.g., Personal Data Protection Commission Singapore ("PDPC").
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 the Group.
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 possesses, e.g., name, national identification number, work pass number, passport number, mobile number, address, photo.

Term	Definition
	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.
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 lifecycle. 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, and 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,

Term	Definition
	erasing, obtaining, recording, organizing, retaining, retrieving, storing, transmitting, transferring, using or viewing.
Record of Processing Activities	A comprehensive documentation of all processing of Personal Data undertaken to fulfill 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 ● Criminal allegations, proceedings or convictions ● National Identity Card Number[1] ● Birth Certificate Number[1] ● Passport Number[1]
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 include 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.

[1] Specific to Singapore