Data Management Policy

Approved By	Group Chief Risk Officer
Document Owner	Group Chief Risk Officer
Document Author	Group Risk
Effective Date	1 May 2024

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.

Version Control

Version no.	Date issued	Key Revisions
1.0	28 July 2022	First issuance (Livia Aminah) Approved by the Group CRO on 28 July 2022 and notified to the ORC on 3 August 2022.
2.0	19 Dec 2022	Updates (Livia Aminah) Approved by the Group CRO on 19 Dec 2022 - Changes made to section 3.1 and 3.2 - New section 3.3. was added
3.0	25 May 2023	Annual refresh (Sarah Cheong) Approved by the Group CRO on 25 May 2023 - Aligned document format to Policy Document Template 2.1 Use – Updates/amendments: Issued Business Ethics Code; develop approval process for data extraction 2.1 Enhance - Updates: Issued AI Governance Policy 2.2 – added last point to align with framework 2.4 – added point to comply with Group Business Ethics Code. 3.2-Data Inventory, added list of related data inventory documents 4.0 – revised to Framework, Policy and related documents and updated document name and owners. 5.0 - Version control moved to page 2 and Section 5 replaced with 5.0 - Review 6.9 – Added section for M & E 7.0 – Added section for Non-compliance
4.0	1 May 2024	Updates (Daniel Heng) - Editorial changes across the Policy to improve clarity - 2.1 Data Lifecycle Management – Updates to Brief Description, Risks, Control Expectation - 2.3 Data Quality – Added Data Owner and Data Steward Responsibilities - 3.3 Approval for Data Request pertaining to Marketing or Servicing Purpose - 3.4 Other Important Roles – Updated Platform Owner Responsibilities, Removed Gatekeeper

Contents

1. Purpose and Scope

1.1. Purpose

This Data Management Policy (“Policy”) is one of the three pillars of the Data Risk Governance Framework (“Framework”). It provides requirements and guidance on key areas in the Framework relating to data management of **Critical Data**[1] and **Personal Data**[2].

1.2. Scope

This Policy applies to all companies within the Group, their operations, functions and employees.

2. Data Management

2.1 Data Lifecycle Management

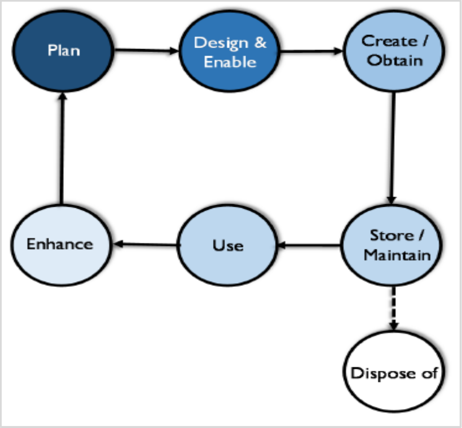

Figure 1: Data Lifecycle
(Extracted from DAMA DMBOK 2nd edition)

Effective data management includes understanding how data traverses throughout its life from the time it is created or obtained to its eventual disposal.

There are risks at all stages of the data lifecycle management. Key controls need to be put in place to manage the risks.

Refer to the table below for examples of key controls that should be implemented, wherever possible.

[1] **Critical Data** is 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 unauthorised access to such data per the Integrated Assurance Framework (“IAF”). Refer to the Group IAF’s impact parameters.

[2] **Personal Data** is a sub-set of Critical Data. The definition of Personal Data is in accordance with the Personal Data Protection Act 2012 (“PDPA”).

Stage	Brief Description	Risks	Key Control Expectation
Plan	Account for the movement of data across its lifecycle to effectively manage data assets.	• Poor planning would result in poor data quality and/or data breaches.	• Plan for system requirements, data architecture, costs and resources. • Perform Data Protection Impact Assessment (DPIA) and manage the identified risks/gaps. • Perform due diligence on vendor / external system – Third Party DPIA
Design & Enable	Develop data architecture and data design / modelling to achieve the company's objectives.	• Inadequate design of systems / processes to meet data privacy and data protection requirements eg requesting for data that are not required for fulfilling business purpose. • Data ownership is not properly defined.	• Implement Privacy by Design from inception. • Adopt data minimization strategy. • Perform comprehensive SIT and UAT. • Identify Data Owner.
Create / Obtain	Data is generated or obtained from various sources	• Data is created / modified without proper authorization. • Data is classified inaccurately resulting in lower level of security measures implemented.	• Proper access rights for manual input of data into the system. • Implement doer and checker to ensure completeness and accuracy. • Department's data inventory and data map is regularly updated to reflect new and/or changes to data assets.

Stage	Brief Description	Risks	Key Control Expectation
			• Staff awareness on Group Information Classification
Store / Maintain	Data to be stored and protected, with the appropriate level of security commensurate with the information classification. A robust backup and recovery process should also be implemented to ensure retention of data during the lifecycle.	• Data is kept for longer than necessary and beyond regulatory requirements. • Insufficient data security measures resulting in data breaches. • No back-up of data.	• Records retention and disposal schedule is updated and complied with. • Regular testing and/or audits on the company's security measures. • Ensure regular back-up of data and properly storage of back-up files. • Ongoing due diligence on cloud & system service providers.
Use	Data is used to support activities in the company.	• Data processing activities are not in compliance with the relevant privacy laws. Data is not being used for value adding purposes. • Unable to use the data collected due to poor data quality, systems limitation or wrong extractions. • Unauthorized and/or unethical use of data. • No proper approval process for data access and data extraction.	• Ensure compliance with the relevant Privacy laws & engage Group Risk team and Privacy Compliance. • Unused data to be destroyed. • Regular review of user access rights on systems and physical cabinets/rooms. • Ensure correct parameters / rules for data extraction. • Data Quality process to cleanse and validate data • Defined data related principles in the Business Ethics Code . • Develop approval process for data extraction.

Stage	Brief Description	Risks	Key Control Expectation
Enhance	Process of adding attributes to a data set to increase its quality and usability, e.g. psychographic information. Transformation of data to various formats & reports.	• Incorrect additional attributes tagged to source data resulting to inaccurate data set. • Inaccurate artificial intelligence (“AI”)	• Issued the Group AI Governance Policy. • Self-service / Automation of reports generation.
Dispose of	The process of removal of every copy of a data item from the company.	• Data is not destroyed completely and securely in all systems or physical storage.	• Maintain a register detailing data disposal method. • Department’s data inventory is regularly updated to reflect new and/or data storage to facilitate complete removal of data.

2.2 Data Security

Data security is expected to be managed throughout the data lifecycle to ensure that data is secure, and the risks associated at each data life stage are mitigated. It includes the planning, development, and execution of security policies and procedures to provide proper authentication, authorization, access, and auditing of data and information assets.

The implementation of technical safeguards is led by the Technology Owners. The responsibilities of the Technology Owner include:

- Design and regularly review the information security policy and data security standard.
- Implement appropriate technical safeguards to protect the confidentiality, integrity and availability of information asset and data.
- Manage data user access as prescribed and authorised by data owners (applies to systems managed by IT).
- Overall responsible for monitoring and managing data security to ensure that the IT operating environment is secured.
- Provide technical support for data management.

All staff are required to comply with the data security measures rolled out by the Technology Office.

2.3 Data Quality

Similar to data security, data quality is expected to be managed throughout the data lifecycle from creation through disposal. Data quality management is central to data management. It refers to the planning, implementation, and control of activities that apply quality management techniques to data, in order to assure it is fit for consumption and meets the needs of data consumers (i.e., high quality data).

Low quality data (inaccurate, incomplete, inconsistent or out-of-date) represents cost and risk, rather than value because its information is not accurate or complete, and may be misunderstood and misused. This is particularly risky if the low quality data was used for decision making that impacts the customers or the Group. It can damage the Group's reputation, resulting in fines, lost revenue, lost customers, and negative media exposure.

The data quality dimensions (i.e., the feature or characteristic of data) that should be considered throughout the data lifecycle are:

Data Quality Dimensions	Brief Description	Considerations
Completeness	Whether all required data is present.	• Whether sufficient information has been collected / obtained for fair decision making. • Indicate mandatory fields and detect blank values. • Ensure records are populated correctly and completely from where its collected to where its stored. • Complete parameters/rules used for data extraction or transfer.
Uniqueness	No entity[3] exists more than once within the data set.	• Identify the unique identifier to prevent duplication in systems.
Timeliness	The degree to which data represents reality from the	• Currency of data used for decision making (i.e., original record versus a later modified record)

[3] Briefly explained, the term 'entity' in the context of data/database refers to a thing, person, place, unit, object or any item about which the data is captured and stored. The 'Entity Attributes' identifies, describes, or measures an entity.
E.g. Jane is employee of a company. In this context:

Entity	Entity Instance	Entity Attributes
Employee	Jane	Employee first name Employee last name Employee ID number Employee DOB

Data Quality Dimensions	Brief Description	Considerations
	required point in time.	• Regulatory requirements on the frequency of updating certain data from customers. • Availability to obtain/extract latest information when required. • Audit trail on date or time the data was last updated or confirmed.
Validity	Data is valid if it conforms to the syntax (format, type, range) of its definition.	• Define the data type, format, and precision of expected values when defining data domain. • Implement automated rules check for the data fields (e.g., NRIC/FIN input cannot be < 5 characters). • Verify logical sequence of dates (e.g., Inception Date must be less than or equal to the Cover End Date)
Accuracy	The degree that data correctly represents ‘real-life’ entities.	• Verify against data source (e.g., verify identification number inputted against identification card). • Utilize government’s database (e.g., MyInfo). • Maker and checker control for edits of data.
Consistency	Same information that are stored in various places are consistent / matches.	• Implement data standardization, i.e. the conditioning of input data to ensure that data meets rules for content and forma (e.g. format for name, date, address) across all systems. • Consistency check across various systems, (e.g. HR system indicate Jane has left the company, but payroll system still transfer monthly salary to Jane)

Data Owner is responsible for ensuring data quality by leading the effort in the following

- Identify Critical Data Element (CDE) to be subject to Data Quality validation
- Define Data Quality rules for the measurement of various Data Quality dimensions
- Identify where Data Quality validation will take place
- Report Data Quality issues to Group Risk
- Review and approve Action plan proposed by Data Steward to remediate Data Quality issues

Data Stewards are appointed from the Data Science and Analytics (DSA) team to work with Data Owners to carry out their data quality responsibilities.

Details of each step are covered in March 24 DRF - 02. 25 Mar 24

2.4 Data Ethics

Data ethics are concerned with how data is procured, stored, managed, interpreted, analyzed / applied and disposed of in ways that are aligned with ethical principles, including community responsibility. This includes moral obligations and going beyond meeting Personal Data protection and technical or security standards or regulatory requirements.

The Group's data ethics principles that should be observed at all times are:

- **Impact on people**: Because data represents characteristics of individuals and is used to make decisions that affect people's lives, there is a moral obligation to manage its quality and reliability, as well as ensuring fairness across different demographic lines.
- **Potential for misuse**: Misusing data can negatively affect people and the Group's reputation, so there is an ethical imperative for the Group to implement sufficient controls and governance to prevent the misuse of data, including data breaches that potentially could result to the misuse of data by unauthorized third parties.
- **Economic value of data**: Data has economic value. Ethics of data ownership should determine how that value can be accessed and by whom. The Group must not sell our customers' data to any parties.

Unethical data handling can result in financial loss as well as loss of reputation and customers because it puts at risk people whose data is exposed. All data users in Singlife Group should be aware of the ethics of data collection, analysis, and use and comply with the data related principles in the Group Business Ethics Code.

Any unethical data handling practices in the Group should be escalated to the Group Risk team.

3. Data Risk Management

3.1 Data Protection Impact Assessment ("DPIA") Process

The DPIA Process helps to assess if the handling of Personal and Critical Data complies with the data protection regulations and data management best practices; and implement appropriate technical or organizational measures to safeguard against data protection risks.

The key tasks in the DPIA Process include:

1. Identifying the Critical Data and Personal Data handled by the system or process, as well as the reasons for collecting the data.
2. Identifying how the data flows through the system or process.

3. Identifying data related risks by analyzing the data handled and its data flows against applicable regulations (e.g., PDPA for Personal Data), data management practices (e.g., data quality) and appropriate technical / organizational measures (e.g., encryptions, user access controls, etc).
4. Addressing the identified risks and ensure they are adequately addressed before the system or process is in effect or implemented.
5. Checking to ensure that identified risks are adequately addressed before the system or process is in effect or implemented.

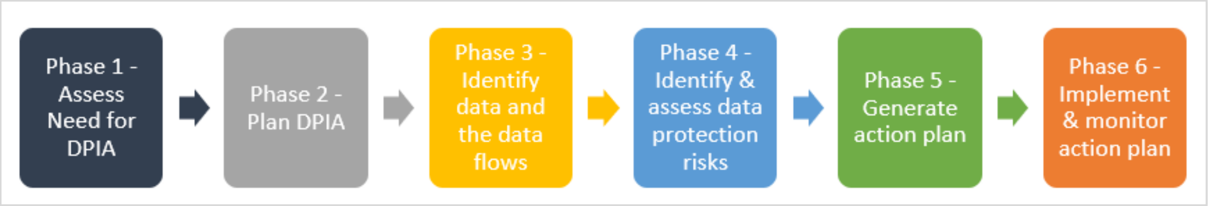
Phase 1 - Assess Need for DPIA
Phase 2 - Plan DPIA
Phase 3 - Identify data and the data flows
Phase 4 - Identify & assess data protection risks
Phase 5 - Generate action plan
Phase 6 - Implement & monitor action plan

Figure 2: DPIA Process

There are two impact assessment forms under the DPIA Process, and they should be used in different contexts:

Forms	Relevant Contexts	Trigger Points
Third Party Data Protection Impact Assessment **("TPDPIA") Form**	To be completed by Business Unit for the following instances: - Onboarding of new third parties that involve the processing of Critical Data and/or Personal Data; or - Material changes to how Critical Data and/or Personal Data is processed by the existing third parties.	The TPDPIA must be completed and reviewed by Group Risk and Privacy Compliance teams <u>before</u> the sign-off of the legal agreement, work order, etc.
Data Protection Impact Assessment **("DPIA") Form**	To be completed by Business Project Manager / Business Unit for the following instances: - New project or process (system, product, service or activity) involving the processing of Critical Data and/or Personal	The DPIA form should be <u>initiated at the earlier stages</u> of project/process lifecycle, where there is most room for shaping how the initiative is to be implemented, by integrating data protection considerations into all projects/processes right from the design stage and throughout its lifecycle.

	Data (includes new systems, applications or APIs allowing for data transfer); or - Material change to existing product or process (system, product, service or activity) relating to how Critical Data and/or Personal Data is processed.	The DPIA form must be completed and reviewed by Group Risk and Privacy Compliance teams before production implementation. Considering the required controls to address data management and privacy risks upfront helps to ensure compliance with regulatory obligations and not hinder production implementation which may likely lead to increased cost and effort.

Refer to the SharePoint link here for the latest version of TPDPIA form and DPIA form that are jointly developed by Group Risk and Privacy Compliance teams.

3.2 Data Inventory

Data Inventory and Data Map are documents that record the Critical and Personal Data collected and/or processed by the company as it moves across various systems throughout the data lifecycle from creation to disposal. The documents also include information on the business purposes for collection, use and disclosure of the data, the parties (including third parties) who handle the data, the classification of the data to manage user access as well as when and how the data should be retained or disposed. These documents help the company to assess the controls in place, identify risks / gaps and subsequently address the risks / rectify the gaps.

Each department will maintain a copy of their department's Data Inventory documents, which comprises the Data Inventory, Data Map, Records Retention Schedule, Disposal Schedule and Consumer Log. The regular annual exercise of updating the Data Inventory documents will be triggered by the Group Risk team. Nevertheless, the department should proactively update their Data Inventory documents in the event of major changes to their department activities that has impact to the collection and processing of Critical and Personal Data. The relevant department shall raise the identified risks / gaps in the GRC systems (i.e., MetricStream).

The Data Inventory is one of the requirements to obtain and/or maintain the Data Protection Certification Trustmark.

3.3 Approval for Data Request pertaining to Marketing Campaign or Servicing Campaign Purpose

Staff may be required to use Critical Data and/or Personal Data (collectively ‘Data’) in their line of work. The use of the data, for any purposes other than Marketing or Servicing, would require staff to seek approval from the respective Data Owner (Refer:

- Group Data Management Policy 3.4 Other Important Roles – Data User)
- Data Risk Governance Framework 2.2 Roles and Responsibilities – Data Owner)

This section outlines the process for seeking approval for data request pertaining to Marketing or Servicing purpose. All data extraction requests fulfilling the definition of Marketing and Servicing will follow this process.

Marketing Communication	Servicing Communication
• Include direct and obvious upsell messages, including the latest promotion and specific CTAs	• Does not include upsell of a Singlife Product • Informative by nature, anchoring either on latest statutory updates (i.e. changes to cancer coverage under IP plans) or useful stats (i.e. factual information about healthcare costs/claims/etc) leading to a message which encourages the consumer to rethink their coverage • No specific product or promotions can be mentioned

To drive consistency of messaging and branding, and prevent duplication or multiple communication targeting the same customers at the same time, all Marketing or Servicing campaigns will be driven centrally by Brand, Communications and Marketing (BCM)

Staff will therefore seek approval of the data extraction from Executive Director of Marketing or Group Head of BCM.

3.4 Other Important Roles

The Framework describes the roles and responsibilities for key data role holders, including data owner and data protection officer. However, besides the two data roles, there are other roles undertaken by various functions, teams or staff in the Group that impact how Critical Data is processed. They collaboratively contribute to good data management practice.

Platform Owner

The Platform Owners own the various collection points of Critical Data, e.g., the Singlife App has its own Platform Owner and the Singlife official website has its own Platform Owner.

The Platform Owner is responsible for the following:

- Collection of data in accordance with relevant data quality requirements. Data Quality Checklist can be used by the Platform Owner as the baseline standard
- Work collaboratively with Data Owners during initial design phase (by providing inputs and/or suggestions) and continually highlight any gaps found post implementation to improve processes.
- Restrict the use of customer data temporarily stored in the platform for following up with customers regarding their requested / aborted transactions or as per consent clause agreed to by customer.

  Purge data stored in the platform that is no longer relevant for business use in accordance with records retention schedule.

Data Engineer

The Data Engineer is the engineer that determines the architecture of how data flows from start to end, as well as where and how data is stored and safeguarded.

The Data Engineer is responsible for the following:

- Work closely with Data Owner to ensure protection, security and manage the data risks of the data assets within Singlife group.
- Data structure, pipeline, and correctness of data source to serve the needs of business users / Data Users (data science team, marketing data, etc.). For example, building the required validation rules/checks properly, etc.
- Maintain data on the IT applications in accordance with the business and Data Owner's requirements.
- Put in place a governance process on the handling and processing of data assets. For example:
  - Maintain and monitor user access rights that is regularly reviewed.
  - Monitor compliance of data processing through audit logs and trails in IT applications. Report any instances of non-compliance (not in accordance to approved use case) to Data Owners upon discovery.
  - Obtain Data Owners' feedback and approvals for changes made to the IT application that will impact on how the data within the application will be stored, maintained and/or processed.
  - Ensure that data within the IT application satisfies the data quality dimensions as described above.

Data User

The Data User is anyone in the company that processes or have access to the Critical Data.

The Data User is responsible for the following:

- Seek approval from respective Data Owner on any access, use and processing of data.
- Include clear purpose of data usage (including limitations of use), scope, storage and protection/retention parameters, user access and disposal plans.
- Ensure deletion of all data in possession once approved retention period is expired.
- Handle data in accordance with Singlife data protection policies and relevant legislations (e.g., PDPA).
- No modification of data is permitted unless approved by data owners and within authorized scope.
- Ensure the use of data is within the approved scope and parameters as stipulated in the data request. The data user is held fully accountable for any misuse of data.

4. Framework, Policies and related documents

This Policy should be read in conjunction with the Data Risk Governance Framework and the following policies:

Policies	Policies' Owners
Group Privacy Policy	Privacy Compliance
Singlife Information Security Policy	Group CISO

This Policy should also be read in conjunction with the following documents:

- Technology Risk Management Framework
- Data Incident and Breach Management Standard
- Data Inventory and related Documents
- Singlife Information Security Standard

5. Review

This Policy will be reviewed at least once annually or when there is a major change, with changes approved by the Group CRO and notified to the ORC. Where no changes to the Policy are proposed after the annual review, the ORC must still be informed that a review has been conducted.

The Policy will be made available in the intranet.

6. Modification and Exceptions

Modifications and exceptions should be sought from Document Owner and/or Document Approver for any deviation or non-compliance with the policy.

7. Non-compliance

Non-compliance or any identified issues that could lead to non-compliance must be:

- Notified to Group Risk team and Group CRO; and
- Rectified immediately or within a reasonable timeframe agreed with the Group CRO