Singlife with AVIVA

Data Inventory Guide

15 August 2022

Group Risk

Table of contents

Data Inventory Guide

Overview

Data is an important asset for an organization. To have a clear understanding of the data under their care, each function will maintain the Data Inventory and related documents for their Critical Data (which may be Personal Data or non-Personal Data). The documents to be maintained are listed below.

S/N	Document	Scope	Document Description	Action Owner
1	Data Inventory	Critical Data (personal & non personal)	List of Critical Data Assets.	Data Owner
2	Data Map	Critical Data (personal & non personal)	Data Flow diagrams showing the data flow of Critical Data Assets, including control points. Data Flow includes the flow of Critical Data from data collection source, transfers within the organization, and transfers out of the organization. Controls include controls put in place to ensure data accuracy, consistency, integrity, ethical use of AI (new) and security during the transfer between data repositories.	Data Owner
3	Records Retention Schedule	All Records with data (includes records with Critical Data).	List of all records with data (including Critical Data) and their respective retention policy, by function.	Records Owners (Data Risk Forum members or nominees)
4	Disposal Schedule	Critical Data (personal & non personal)	List of data repositories with Critical Data and their respective disposal methods.	Business Application Owners, with Data Owners and Data Protection Officers
5	Data Consumer Log	Critical Data (personal & non personal)	List of third parties that Critical Data is disclosed or transferred to, with details of the disclosure / transfer	Vendor Owners, with Data Owners and Data Protection Officers

02 Data Inventory

Data Inventory

I. The Data Inventory is a list of all the Critical Data Assets in the Group.

II. Each function is responsible for identifying Critical Data under their care.

III. Each function will document the Data Assets identified as Critical Data in their department Data Inventory.

IV. Data Risk function will consolidate the Critical Data in their department Data Inventories into the Entity / Group level Data Inventory.

Critical Data

- Critical Data are data assets that are important for the efficient and effective operation of the organization with the potential of moderate and above risk impact to the business in the event of adverse events.

- 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.

Personal Data

- 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").

- Under the Personal Data Protection Act (PDPA) of Singapore, Personal Data means data, whether true or not, about an individual who can be identified
  i. from that data; or
  ii. from that data and other information to which the organization has or is likely to have access

- By default, all Personal Data should be considered as Critical Data. If there are data elements containing personal data that is deemed to be of such low risk and/or volumes that it should not be considered Critical Data, this should still be documented in the Data Inventory as a Non-Critical Data together with supporting evidence of Data Owner & Data Protection Officer assessment and approval for the Non-Critical Data classification.

Data Priority

- Critical Data identified is further prioritized based on the Data Criticality.

- There are three levels of data criticality

  i. Highly Critical Data is any data that poses a Major or Very Severe risk

  ii. Critical Data is data that could pose a Moderate risk

  iii. Non-critical Data is data that could pose a Low or Minor risk.

- The Integrated Assurance Framework (IAF) sets out impact scales and guidance that can help determine data criticality using five risk ratings classed as Very Severe, Major, Moderate, Minor or Low across Financial Loss/Misstatement, Conduct and Reputation or Operational Disruption.

Ownership and Responsibilities

- For each Critical Data, a Data Owner (“DO”) is to be appointed.
- For each Critical Data that is also Personal Data, a Data Protection Officer (“DPO”) is to be appointed.
- The DO is accountable for the management of the Critical Data and to maintain the Critical Data information in the Data Inventory and related documents.
- The DPO is accountable for the management of the Critical Data in compliance to PDPA.
- Where data is held in an IT asset, the Technology team (specifically the respective IT Application Owner) will be the Data Custodian (“DC”).
- The roles and responsibilities of the DO, DPO and DC is available in the Data Risk Governance Framework, Privacy Policy and Data Management Policy.

Relationship with other Data Inventory Documents

Data Map

- For each Critical Data Asset in the Data Inventory, a Data Map is developed to show the data flow of the Critical Data Asset

Records Retention Schedule

- For Records with Critical Data, the Critical Data Asset held as well as the Data Owner of the Critical Data will be identified in the Records Retention Schedule.

Disposal Schedule

- For each data repository identified as holding Critical Data in the Data Inventory, the disposal solution is documented in the Disposal Schedule.

Consumer Log

- For Critical Data Assets with “EXTERNAL DATA TRANSFERS” = Yes, the third parties to whom Critical Data is disclosed or transferred to are listed in the Consumer Log.

Relationship with other Documents

DPIA

- Critical Data identified in a DPIA should exist in the Data Inventory. If not, the Critical Data Identified is to be added to the Data inventory.

ISBIA

- If data is identified as Critical Data in the ISBIA, the Critical Data should exist in the Data Inventory. If not, the Critical Data Identified is to be added to the Data inventory

03 Data Map

Data Map

- The Data Map is a data flow diagram that
  1. identifies the original source of a data asset as it enters the organisation [Source of Data];
  2. documents its movement through the organisation [Data Flow within the BU]; and
  3. records how it exits the organisation [Data Flow out of the BU].

- The Data Owner is responsible to develop Data Maps for all the Critical Data under their care.

- The objective of data mapping is to enable the business and the Data Owner to visually identify the movement of their critical data from end to end, providing an effective tool for identifying, managing, controlling and protecting their data assets.

Components of the Data Map

i. Source of Data
- This is the initial point the data asset enters the organisation or is collected by the organisation/function.

ii. Data Flow within the Organisation
- This is how the data asset transfers within the organisation, including to other functions. It identifies the movement of the data asset, captures the various systems and applications or physical storage facilities where the data is stored, where it is replicated and how the data is transferred, whether through manual intervention or automated feeds and processes.

iii. Data Flow outside the Organisation
- This is where the data asset exits the Organisation. This may be a transfer to a related entity or to an external party, such as an outsourced function, customer, broker or supplier.

iv. For data disposal, please refer to the Disposal Schedule

Control Points

a) Following the creation of the data map, Data Owners can then identify key data controls that are already in place or are required to be implemented to control and manage the data asset.

b) Key data controls are layered over the data map and help to ensure the accuracy, integrity, consistency and security of the data as they transfer from one data repository to another or out of the organisation, namely:

Data Quality reconciliation	Reconciliation to show that the data in the downstream system has been consistently applied
Data Quality system control	A built-in control mechanism that identifies whether data is accurate or complete (e.g. validation rules, exception reports etc)
Data Quality manual control	A business process control that ensures data manually entered is accurate and complete (e.g. maker-checker, sample check, reasonableness check)
Artificial Intelligence (AI) control (new)	Document steps taken to ensure that AI has been deployed in a responsible manner, namely AI solutions should be human-centric (the interests of human beings, including their well-being and safety is protected), and the decision-making process is explainable, transparent and fair.
Data Security control	An appropriate security control such as encryption required when the data asset is transferred outside the Organisation
External Transfer control	A legal data sharing agreement or supplier contract is in place when data is shared with a related entity or external supplier.

Ownership

For each Critical Data, the Data Owner ("DO") is responsible to create and maintain the Data Map for the Critical Data under their care.

04 Records Retention Schedule

Records Retention Schedule

- The Records Retention Schedule is an inventory list of records with data held by each function, together with the corresponding retention policy and disposal method for the record.
- The Records Owner is responsible to update the Records Retention Schedule.
- The objective of the Records Retention Schedule is for functions to identify their records with data and document the retention policy and disposition for records with data in order to ensure that the records are maintained for an appropriate time, and destroyed after a reasonable period, considering its legal, regulatory, fiscal and operational requirements.
- The Retention policy defined must consider:
  i. retention requirements (the minimum period required for the records to be retained);
  ii. retention limitation requirements (the maximum period for the records to be retained).
- Where there is a conflict between regulatory obligations, risk based decisions relating to retention or deletion periods must be justifiable and documented.
- Clear trigger points and retention period should be clearly defined so that records with data (particularly, records with Critical Data) are disposed in accordance with the retention policy set.

Critical Data

- If any of the records hold Critical/Personal Data, the Critical Data Asset/Element and the Data Owner will be documented under the relevant columns.

- The Data Owner should be aware of their data residing under other function’s records.

- The name of the Critical Data recorded should correspond with the Critical Data Asset/Element recorded in the Data Inventory.

- If the Critical/Personal Data is not in the Data Inventory, the Data Owner shall add the Critical Data Asset/Element to the Data Inventory.

Records under Embargo (or “Legal Hold”)

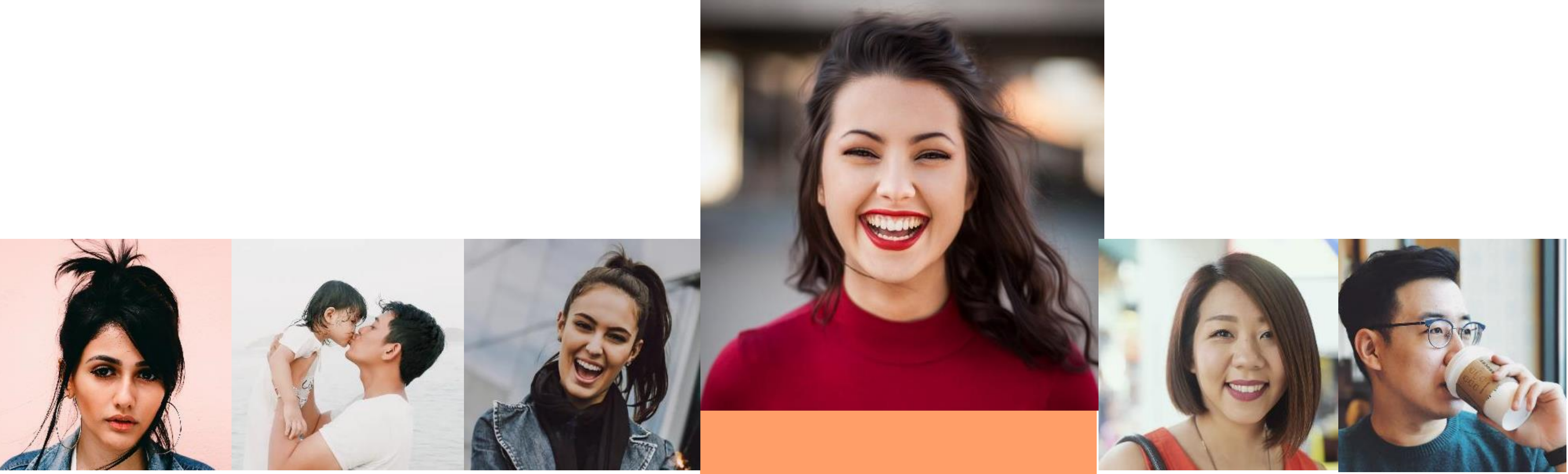
- If an Embargo is issued or required, the Records Owner, together with the relevant department Representatives, Data Owners and/or Data Protection Officers will work with the Legal function to identify all documents which may be relevant to the Embargo and take the necessary steps to ensure that the documents are transferred to the Legal Function and/or retained even if they are past their retention period.

- An Embargo overrides the Records Retention Schedule and Disposal Schedule whilst the Embargo is in place.

- The Legal function will notify the parties concerned when the Embargo is lifted, after which the retention period for such documents will follow the retention period for as documented in the Records Retention Schedule.

Roles and Responsibilities

- For each function, a Records Owner is appointed to document the Records with data for the function.
- The Record Owner is by default, the representative in the Data Risk Forum unless otherwise appointed.
- The Records Owner need not be a Data Owner but should ensure that Data Owners are aware of the records with their Critical Data and Action Owners are aware of and perform the disposal of the records in accordance with the retention policy.
- The Action Owner is the party assigned to perform the disposal of the record. The Action Owner need not be the Data Owner or Records Owner.



05 Disposal Schedule

Disposal Schedule

- The Disposal Schedule is an inventory list of data repositories with Critical Data, together with the corresponding retention policy and disposal solution for the data in the repository.

- Data Repositories may hold multiple Critical Data and the retention policy for the data repository will need to take into consideration the retention requirements of all the Critical Data in the repository.

- The objective of the Disposal Schedule is to help business and the Data Owners ensure that their Critical Data in the identified Data Repositories have disposal solutions put in place to meet the retention policy of their Critical Data.

Ownership and Responsibilities

- The Data Owner is responsible to define and implement the appropriate retention policy and disposal solution for the Critical Data under their care.
- If the Data Owner is not the Repository owner, they will work with the respective Repository owner to put in place and implement the disposal solutions for their Critical Data residing in the repository.

06 Consumer Log

22/8/2022

Consumer Log

- The Consumer Log is a list of external suppliers, distributors, third parties or related entities, to whom our critical data is disclosed or transferred to for various business purposes.

- The Data Owner, together with the Vendor Owner shall have an understanding of the relationship (in particular the business rationale and purpose) for the data transfer and ensure that an appropriate data sharing agreement is in place.

- Where Critical Data (particularly, Personal Data) is transferred out of Singapore, the Data Owner/Data Protection Officer shall check that a legitimate transfer mechanism (e.g. relevant contract clauses) is in place before allowing the data to be transferred to another jurisdiction.

Ownership and Responsibilities

- The Data Owner is responsible to assess and approve the disclosure or transfer of Critical Data to another party.

- The Vendor Owner should have the consent of the Data Owners for any disclosure and/or transfer of the Data Owner’s Critical Data to the Third Parties.

07 Updating Procedure

Updating Procedure

- **Regular Review**
  1. The Data Inventory, Data Maps, Records Retention Schedule, Disposal Schedule and Consumer Log are to be reviewed and refreshed annually.

- **Scheduled updates – Template refresh**
  1. Data Risk will review and refresh the document templates, where applicable.
  2. The templates will be published in the Data Risk sharepoint

Scheduled Updates – Document Refresh

Data Risk will initiate the annual refresh for Data Inventory documents. All documents to be updated and published in the Data Risk sharepoint.

Data Inventory

i. All Data Owners (DO) will be requested to update the Critical Data information under their care in their department Data Inventory;
ii. All Data Risk Forum members and Data Owners will be requested to review the data under their functions to identify if there is any Critical Data not currently listed in the Data Inventory.
iii. If there is any Critical Data not currently listed in the Data Inventory, the Data Risk Forum member or appointed Data Owner will use the Data Inventory template to record the new Critical Data into their department Data Inventory.
iv. Data Risk Function will consolidate the updated and new department Data Inventories and issue an Organisation and/or Group level Data Inventory.

Records Retention Schedule

i. All Data Risk Forum members and Record Owners will be requested to review and update the Records with data under their functions into their department Records Retention Schedule.
ii. Data Risk Function will issue the consolidated Organisation and/or Group level Records Retention Schedule after the Data Risk Forum members and Record Owners have completed their updates.

Data Maps

i. All Data Owners (DO) will be requested to create or update the Data Maps for the Critical Data under their care.
ii. Data Risk Function will publish the updated Data Maps

Disposal Schedules

i. All Data Owners (DO) will be requested to update the Disposal Schedule for the Critical Data under their care into their department Disposal Schedule.
ii. Data Risk Function will consolidate the updated Disposal Schedules and issue an Organisation and/or Group level Disposal Schedule.

Data Consumer log

i. All Data Owners (DO) will be requested to update the Consumer Log for the Critical Data under their care into their department Consumer Log.
ii. Data Risk Function will consolidate the updated Consumer Logs and issue an Organisation and/or Group level Consumer Log.

Ad-Hoc Updates

- The Data Owners, Record Owners and/or Data Risk Forum members may update the Data Inventory documents at any time.

- If the change is critical, Data Risk will update and re-issue the consolidated document, where applicable. Otherwise, the change will be included in the scheduled annual refresh exercise.

Appendix 1

Resources

Resources

Document
Data Inventory documents • Data Inventory Guide • Data Inventory • Data Map • Records Retention Schedule • Disposal Schedule • Consumer Log
Data Risk Forum documents • Terms of Reference • Members (including DO and DPO) • Meeting Minutes
Data Risk Framework & Policies • Data Risk Governance Framework • Data Management Policy
Data Risk Standards • Data Incident and Breach Management Standard
Privacy Policy • Privacy Policy
Integrated Assurance Framework