Terms of Reference / Policy	Date Approved	April 2018
Data Management Policy	**Frequency of Review**	Annually
	Related Governance Documents	• Policyholder Protection Rules (PPR), 2017, as amended • Conduct of Business Returns requirements • STIA, Amendments of Regulations under S70 • POPIA • King IV
	Effective Date	27 July 2021

Table of Contents

Document details

Purpose

⇨ This document defines the policies, processes and practices implemented by the data management team, to provide a common basis of understanding of policies and practices in place to manage the collection, use, storage and dissemination of business-critical data.

⇨ This document will also outline the policies owned by the data management team to be implemented by other divisions.

Document Approval

⇨ This policy be approved by the Board of Directors and revised annually.

Role	Position	Name of Approver	Approval Signature	Date Approved
Author	Chief Technology Officer	Barry Dickson		2021/07/19
Final Approver	Chairman of the Board	Miles Japhet		2020/03/18

Revision History

Effective Date	Rev Letter	Document Author	Description of Change
2018/03/28	1.0	Ian Gatley	Original approval by the Board
2020/03/18	2.0	Barry Dickson	Revision approved by the Board
2021/07/19	3.0	Barry Dickson	Revision approved by the Board

**** The date listed in the first line of the Revision History table, is the date the document received its final approval. Hereafter, the date becomes the revision date, displayed as the Effective Date on the first page header information.***

Data Management Overview

Introduction

⇨ The role of data management is to provide an enterprise-wide vision and strategy for all data-related initiatives. This holistic strategy focuses on understanding what data is required by the business, how data enters and flows through the organisation, the processes involving the storage and retrieval, securing and enriching this data and, finally, how this information is disseminated back to stakeholders and used to facilitate fact-based decision making.

⇨ All policies outlined in this document are implemented in accordance with the "***comply and explain***" principle as contained in King IV and with the legislative requirements of the Insurance Act, 2017, and the Protection of Personal Information Act, 2013 (POPIA).

⇨ Should a business reason exist to deviate from the policy it should be done with agreement from the data management team and the reasons documented accordingly. These deviations from the policy will then need to be reported to the Board's Risk and Compliance committee as part of the overall risk and compliance management programmes.

Overview

⇨ Sound data-management policies, procedures and practices support effective, data-driven business decision-making and can contribute significantly to enhancing Lombard's strategic direction and enabling more efficient regulatory reporting and business intelligence.

⇨ Timeous access to accurate and complete data is required by business to meet its underwriting, financial and fiduciary responsibilities.

⇨ Lombard's data-management policies, procedures and practices are designed to safeguard the vital aspects of data: Access, Acquisition, Retention, Integrity, Security and Destruction.

⇨ Data integrity includes qualities of accuracy, consistency, and timeliness. Data is a business resource that may be used and relied upon by many users. Data integrity begins with the person or office creating the data and is the continuing responsibility of all who subsequently access and use it.

⇨ Security of data encompasses more than electronic security, although that is an element of it. While some aspects of security may be assured by technology, security also involves a measure of trust. As a valuable and business-critical resource, data must be safeguarded at all levels against damage, loss, and breaches of security, and all who use it share this responsibility.

⇨ Access to data is granted internally when a legitimate business need for the data is demonstrated, and externally when release of such data would not violate the Lombard's stewardship obligations, privacy legislation, or legal contracts.

⇨ In the context of this policy, the term "***personal information***" has the meaning as assigned to it in terms of the definition in the POPIA and refers to the information of both a natural person and a juristic person.

Data Management: Overarching Policy Statement

⇨ The following policy statements will apply to all data-management initiatives undertaken at Lombard:

- ✓ wherever possible, data should be collected once only, at the source, and made available to all who have a legitimate business need for the data;

- ✓ processes for data capture, validation and processing should be automated wherever possible;
- ✓ data should be collected only when known and documented uses and value of this data exist;
- ✓ collection of accurate and complete data is expected, even when elements of this data are required by a business unit different to the unit capturing the data;
- ✓ for accountability and stewardship, all data must have a defined Data Owner and Data Steward responsible for the accuracy, integrity and security of data;
- ✓ data must be used only by those persons duly authorised to access and use the data by virtue of their functional role and position at Lombard, and only for the purpose for which use has been authorised; authorisation for access to data is not transferable;
- ✓ every data user must recognise that data and the information derived from it are potentially complex; it is the responsibility of every data user to understand the data that they use, and to guard against making misinformed or incorrect interpretations of data or misrepresentations of information;
- ✓ data users must carry out all tasks related to the creation, storage and retrieval, maintenance, cataloguing, use, dissemination and disposal of institutional data responsibly, in a timely manner and with the utmost care;
- ✓ data users must not knowingly falsify data, delete data that should not be deleted or reproduce data that should not be reproduced;
- ✓ data users must respect the privacy of individuals whose records they may access; no subsequent disclosure of personal information contained in files or databases may be made, where disclosure is understood to include (but is not limited to) verbal references or inferences, correspondence, memoranda and sharing of electronic files;
- ✓ wherever possible Lombard should avoid maintaining redundant and duplicate data in multiple systems;
- ✓ data may only be deleted or destroyed in such a manner and timeframe as stated in applicable legislation in relation to prescribed retention periods;
- ✓ data should be readily accessible in electronic form to authorised users to view, query or update;
- ✓ data must be stored in such a way as to ensure that the data is secure, and that access is limited to authorised users; secure storage of Lombard's data assets is the joint responsibility of system and network administrators, database designers, application designers, and the data users who must all ensure that passwords and other security mechanisms are used; and
- ✓ all external vendors requiring access to Lombard data must sign a Non-Disclosure Agreement (NDA) before access to any data is granted; in conjunction with the NDA, for purposes of external processing of data, the parties would need to enter into a formal Service Level Agreement (SLA) or Outsourcing arrangement.

Applicable to which LomHold Entities:

- The following entities within the broader LomHold (Pty) Ltd structure are governed by this Data Management Policy:

  Divisions of Lombard Insurance Company Limited

  ⇨ Guarantee division - Construction guarantees

  ⇨ Guarantee division - General and Commercial

  ⇨ Guarantee division – Mining

  ⇨ Guarantee division – Trade Credit

  ⇨ Partnerships division (including Lombard Broker Partners and Lombard Mobility)

  Juristic representatives

  ⇨ Commercial Crime Concepts Proprietary Limited

  Separate Insurance/FAIS licence

  ⇨ Lombard Insurance Company Limited (FSP 1596)

  Underwriting Managers (UMs)

  ⇨ Although UMs and any other binder holder might have their own operating systems, they must give Lombard access to accurate and detailed policyholder information in line with legislative requirements.

Roles and responsibilities

- To promote and safeguard the integrity and security of, and appropriate access to, business data, the following roles and responsibilities are defined. It is quite possible that any one person could participate in more than one of these roles.

  Data Owner

  ⇨ Lombard is the owner of all business-related data. The various business units have stewardship responsibilities for particular elements and/or aspects of the data.

  Data Stewards

  ⇨ Lombard employees who have planning and policy-level responsibilities for data in their functional areas are considered data stewards.

  ⇨ Data stewards are responsible for identifying the access category (public, internal or limited) of data elements under their authority, and for determining what limitations or conditions apply to access. Because data and the responsibility for data has traditionally been organised along functional lines, data stewards will generally follow the same traditional organisation hierarchical structures. Some data stewardship responsibilities and authority, however, may not be clearly delineated and may be shared or delegated to a specific group of data stewards.

Data Experts

⇨ Data experts are Lombard employees who have operational-level responsibility for data-management activities related to the creation, storage and retrieval, maintenance, cataloguing, use, dissemination and disposal of data. Among the responsibilities of the data experts are any data-administration activities that may be delegated to them by the data stewards. Data experts must ensure that procedures are in place to carry out policies such as this one and comply with the standards approved by Lombard.

Data Users

⇨ Individuals who need and use data as part of their assigned duties or in fulfilment of their role at Lombard are data users. Data users are responsible for complying with the data policies outlined in this document, and for following procedures established by data managers. Since data may cross functional lines, data used by any one data user may have different data managers and data stewards.

The Information Officer

⇨ The Information Officer and deputy information officers provides vision and leadership in the development and use of information and information technologies, including strategic planning, governance, policy, infrastructure and resources.

Data Stewardship

- Data Stewards should ensure that data elements and common shared data standards and structures are identified, documented and made available to all users.
- They should further assist the Data Management (DM) function in cataloguing the types of data and identifying the levels of access and security required for access to each category or type of data
- In conjunction with the identification of Lombard's Master Data Records and the rollout of Master Data Management (MDM) technology, Lombard has identified and empowered data stewards and experts within business.

Data Steward Responsibilities

Participate in the data standards process

✓ Data Stewards participate in defining data standards, documenting these standards and improving business processes. Data Stewards represent the needs of data users within their functional area in the data-governance process.

Ensure that data are created and maintained according to Lombard standards

✓ It is the Data Stewards' responsibility to ensure that data users in their functional area follow the standards developed.

Work with technical teams to ensure data integrity and accuracy.

✓ It is understood that there is always the risk of some level of error associated with data entry. It is the responsibility of the Data Stewards, along with the technical staff responsible for capturing data to create a process for identifying data-entry errors and correcting the data. This may include a series of automated error/audit reports, a formal process for verifying data.

Allocation of Responsibilities

- It is the responsibility of the Information Officer to encourage the organisation's responsible parties to process personal information lawfully and in a reasonable manner that does not infringe the constitutional rights of individuals to privacy. In terms of POPIA, the default Information Officer for any private company is deemed to be the head of the company, but he/she may appoint a designated person to fulfil this role.

- The specific duties and responsibilities imposed on the Information Officer in terms of POPIA (s55) include the following:

  ⇨ encouragement of compliance relating to lawful processing of personal information,

  ⇨ dealing with requests made to the company in terms of the Act,

  ⇨ working with the Information Regulator in relation to investigations, and

  ⇨ ensuring compliance with the provisions of the Act.

- The Information Officer is responsible for monitoring and reporting levels of compliance to the LomHold Group Compliance Control Function.

- The Information Officer is also the custodian of the data security procedures. Depending on the nature, scale and complexity of the business, the company may appoint deputy information officers.

Data Management Policies

- Expanding on the overarching policy earlier in this document, the following policies are applicable to all data-management activities.

Data Classification Policy

Purpose

⇨ In order to protect corporate data, all data must be categorised in order to determine the level of protection required.

Overview

⇨ The following categories of data exist:

Public-access data

✓ *Public-access* data is data that is (or can be) generally available to all employees, the general public, and the media.

Internal data

✓ *Internal data* is data that is available to those employees with a clear business need for access as part of their required functional roles and responsibilities. In general, all data is considered internal data unless otherwise specified. Not all employees have access to all internal data; access is determined by the employee's functional role, responsibilities and legitimate use.

Limited-access data

✓ *Limited-access* data is data of a sensitive or confidential nature that is protected from general distribution, and for which special authorisation must be obtained before access is made available, or to which limited access may be granted.

Data Privacy Policy

Purpose

⇨ The purpose of this policy is to outline the way Lombard treats personal information collected from brokers, policyholders, employees and all other business partners.

Overview

⇨ Lombard respects the privacy of all natural and juristic persons as outlined in POPIA. For this reason, Lombard will take all reasonable measures, in accordance with this Policy, to protect personal information and to keep it confidential.

Policy statement

⇨ Lombard only collects, discloses, collates, processes and stores ('uses') personal information with the express written permission (consent) of the individual concerned, unless legally required to do so, and only uses such information for the lawful purpose for which it is required.

⇨ Lombard discloses in writing the specific purpose for which it uses, requests and stores personal information. It also keeps a record of that personal information and the specific purpose for which it is collected.

⇨ Lombard does not and will not use personal information for any other purpose, other than that which was disclosed, unless express written permission is obtained, or unless permitted to do so by law.

PPR Data Management framework

- The Policyholder Protection Rules (PPR) Data Management Framework is a subset of the overarching data management policy. The data required to meet the PPR requirements forms part of the wider set of data required to meet the regulatory reporting requirements and all other internal reporting requirements.

- Under the requirements of the PPR, Lombard has established an adequate and effective Data Management Framework which includes appropriate strategies, policies, systems, processes and controls relating to the processing of any data which enables the insurer to operate at all times.

- **"Processing"** in this context includes processing of all policy-level and policyholder-level records, including personal information. "Records" refers to any recorded information regardless of the form or medium in which it is obtained.

- The primary objective of the LomHold Data Management Framework pertinent to the PPR is to ensure that LomHold and its subsidiaries have access to all of the policyholder information needed for it to meet its market-conduct and servicing responsibilities to its policyholders regardless of the distribution channels or business models through which it reaches these policyholders.

Core Elements of the Data Management Framework

⇨ LomHold is committed to effective and fair treatment of policyholders and ensures that the conditions for the lawful processing of personal information for business activities are implemented throughout the business operations.

⇨ Any person(s) responsible for collecting or processing any data will do so in order to enable LomHold and its subsidiaries to:

✓ have access, as and when required, to data that is up-to-date, accurate, reliable, secure and complete;

✓ properly identify, assess, measure and manage the conduct of business risks associated with its insurance business to ensure the ongoing monitoring and consistent delivery of fair outcomes to policyholders;

✓ comply with all relevant legislation relating to confidentiality, privacy, security and retention of data;

✓ comply with any regulatory reporting requirements;

✓ assess its liability under each of its policies, including data pertaining to each risk that is covered by a policy and each outstanding claim in respect of a policy;

✓ adequately categorise, record and report on complaints in line with the reporting requirements contained in Lomhold's Complaints Management Policy and in compliance with the regulatory reporting requirements contained in the Conduct of Business Returns; and

✓ access any other relevant data as prescribed by the FSCA, including meeting the data requirements specified for binderholders.

⇨ This policy forms an essential part of the framework of strategies, policies, systems, processes and controls required by LomHold to achieve these objectives.

Allocation of Responsibilities

⇨ LomHold complies with its ongoing duty to confirm that it has (1) sufficient organisational resources and (2) the operational ability to ensure that its data-management framework is effective, adequately implemented and complies with the legislative requirements. It regularly reviews its data-management framework and documents changes thereto as part of its annual policy review and Board sign-off process.

⇨ Each business unit has designated resources and distinctive data management requirements. All conditions specified under POPIA for processing personal information are met, among them, accountability, processing limitations, specification of purpose and any limitations related to this purpose, quality of information, openness, security safeguards and the participation of the subject of the data.

Data specifications

⇨ The data collected, processed and stored depends on the business models of each unit and the products and services offered, subject to minimum regulatory and internal requirements regarding this data. Lombard minimum data requirements include all underwriting information, all financial transactions relating to either premium or claims transactions and all reinsurance data, where applicable. Lombard ensures that it has, at a minimum, the names, identity numbers and contact details of all its policyholders but also, where possible, mobile phone numbers and e-mail addresses.

⇨ To meet the requirements of POPIA, Lombard:

- ✓ distinguishes between personal information, special personal information, and other information, as defined under POPIA, and
- ✓ ensures the preparation of specified documentation prior to processing personal information.

⇨ For the purposes of all regulatory reporting under insurance legislation, personal data is processed and summarised to meet the requirements of the provisions in regulation.

Outsourced processing of data

⇨ Lombard ensures that, where data processing is outsourced, the binder holder:

- ✓ has the operational ability to ensure seamless integration between its IT systems and Lombard's, giving to Lombard access to up-to-date, accurate and complete data regarding its policyholders as and when requested, and
- ✓ provides to Lombard access to up-to-date, accurate and complete data on a daily basis to ensure that Lombard is able to comply with regulatory requirements relating to data management, including those provided for in the PPR.

⇨ The management of these outsourced arrangements is detailed in the data management requirement of the Partnerships division.

⇨ Lombard has contingency plans in place to address the circumstances under which a binder holder is unable to provide the insurer with the relevant data in the appropriate format.

Supporting provisions

Record keeping and retrieval of data

✓ The processes involved in the collection, storing, augmentation and dissemination of data are detailed in the Data Management Guidelines document.

Access to Information and Security

✓ As set out earlier in this document, data may be used only by those authorised, by virtue of their functional role, to use it and only for the purpose for which use has been authorised. Data access matrices have been created detailing the level of access required by each role in the business.

Communication

✓ To ensure that policyholders have knowledge of the Data Management Policy, the details of the Information Officer are included in all disclosure documentation.