



Information Privacy Policy



Contents

1. Purpose.....	4
2. Scope.....	4
3. Appetite Statement.....	4
4. Roles and Responsibilities.....	4
5. Key Principles	6
6. Accountability.....	6
7. Processing Limitation	6
8. Purpose Specification.....	7
9. Further Processing Limitation.....	7
10. Information Quality.....	8
11. Openness	8
12. Security Safeguards.....	8
13. Data Subject Participation	9
14. Special Personal Information and Information of Children	9
15. Direct Marketing.....	10
16. Automated Decision-Making	10
17. Privacy Incident Management	10
18. PAIA Manual.....	11
19. Privacy By Design	11

20. Training and Awareness.....	11
21. Third Party Privacy Risk Management.....	11
22. Transferring Data.....	11
23. Policy Review and Version Control	12
24. Definitions	12

1. Purpose

The purpose of the Policy is to describe Hollard's commitment to strive to act with skill, care and diligence when dealing with data subjects' Personal Information (PI).

The Policy contains:

- a) The scope of the Policy and all the parties and stakeholders which must comply with it.
- b) Key Information Privacy principles and requirements.
- c) The principles of Privacy by Design applied to the creation or change of products, services, systems, and processes.
- d) Hollard's risk appetite statement and reference to Privacy Incident Management ("PIM").
- e) The roles and responsibilities of parties involved in the governance framework to give effect to the Policy.

2. Scope

The Policy applies to:

- a) Hollard Holdings (Pty) Ltd, Hollard Fundco (RF) Pty Ltd, Hollard Life Assurance Company Limited, The Hollard Insurance Company Limited, Hollard Specialist Life Ltd, and Hollard Specialist Insurance Ltd, (collectively referred to as "Hollard");
- b) all Hollard Employees and Contractors;
- c) all PI being processed by agents, partners, affiliates where they act as either an operator or co-responsible party with Hollard;
- d) all PI under the control and/or ownership of Hollard; and
- e) any device or IT Infrastructure used to process PI.

3. Appetite Statement

In line with Hollard's Risk Strategy, the Group is committed to avoiding non-compliance with legal and regulatory obligations, including those related to the protection of personal information under POPIA.

This means Hollard will apply the most effective and lowest-risk treatment options available to manage privacy risks, taking into account the size and nature of the business operation.

Hollard will not knowingly implement any process, system, or initiative that results in non-compliance with information privacy laws. If privacy incidents do occur in the course of business, they must be addressed promptly and in line with Hollard's risk mitigation approach.

While our Business Units operate with autonomy, senior management is expected to engage with the Information Officer when dealing with significant privacy risks. This ensures that controls are in place to reduce Hollard's exposure to privacy-related compliance failures.

4. Roles and Responsibilities

The Board delegates specific operational responsibilities as set out below but remains ultimately accountable and will oversee the performance of the delegated responsibilities.

4.1 Hollard EXCO

- a) Establishing an effective compliance function capable of assisting the Board of Directors in overseeing and monitoring that Hollard meets its legal and regulatory obligations, while promoting and sustaining a sound compliance culture.
- b) Monitoring whether senior management promotes a culture of sound risk management, compliance, and protection of policyholders and investors, and overseeing senior management and heads of control functions.
- c) Exercising oversight of this Policy and being responsible for ensuring compliance with this Policy, as well as any regulations, rules, and guidelines, and regulatory requirements.

4.2 Governance

All privacy-related matters are now being addressed within the Combined Assurance meetings (CAMS). This ensures that information privacy aligns with broader governance structures and is managed in a comprehensive, integrated manner, alongside other key compliance issues.

4.3 The Information Privacy Officer

The Information Privacy Officer is responsible for this Policy, the related Information Privacy Guidelines, as well as related regulations, rules, and guidelines.

This includes:

- a) Preparing, submitting, and maintaining notifications to the Information Regulator.
- b) Monitoring and oversight the risks associated with information privacy and data protection within Hollard.
- c) Being responsible (strategically and operationally) for Information Privacy and compliance with the Protection of Personal Information Act, Act 4 of 2013 (PoPIA) and Promotion of Access to Information Act 2 of 2000 (PAIA) across Hollard.
- d) Being responsible for engaging with the Information Regulator.
- e) Managing privacy across Hollard.
- f) Managing privacy incidents.
- g) Managing the relationship and requirements from the Information Regulator.
- h) Monitoring privacy practices and reporting on them.

The Information Privacy Officer may delegate responsibilities to Deputy Information Officers (DIOs) to support the implementation of the requirements of the Act. These responsibilities include promoting PoPIA compliance within Hollard, responding to PAIA requests and monitoring information security and protection of PI measures.

4.4 Information Systems and Information Security

Central and BU IT and Information Security are responsible for:

- a) Ensuring that equipment and systems are monitored so that PI and SPI are not processed by unauthorised users.
- b) Ensuring that all devices are equipped with up-to-date virus protection software.
- c) Ensuring the existence and compliance with relevant policies, procedures, and security guidelines.
- d) Implementing ongoing information security and privacy awareness and training programs.
- e) Ensuring that regular systems penetration testing, vulnerability and security assessments are conducted.
- f) Ensuring that appropriate security protocols are in place to manage network, endpoint, data, and application security.

4.5 Deputy Information Officers

Senior Management plays a crucial role to ensure that the policy is compliance with this Policy within their respective areas and functions.

Their responsibilities include the following:

- a) Monitoring compliance with this Policy within their areas of control.
- b) Ensuring the accuracy of the PI within their control.
- c) Ensuring adherence to the requirements of PoPIA.
- d) Promoting a culture where PI is respected and treated with the highest level of care.
- e) Clearly communicate to their employees their responsibilities in respect of PoPIA.
- f) Identifying and managing Information Incidents and Breaches as per the Information Incident Management Policy.
- g) Monitoring the adequacy and effectiveness of information controls in their areas.
- h) Ensuring openness principle is covered through appropriate communication channels, integrated into relevant business processes.

5. Key Principles

The Key Information Privacy principles are described as conditions of PoPIA.

6. Accountability

Hollard is accountable for overseeing compliance with PoPIA and must ensure that the technology, structures, processes, procedures, roles, and responsibilities put in place create an environment where PI is processed lawfully.

This applies from the moment of collection to all subsequent forms of processing.

Hollard has appointed an Information Officer to take overall accountability for PoPIA compliance and ensures the implementation of the privacy strategy, governance framework, and privacy controls across Hollard.

7. Processing Limitation

Hollard must ensure that PI is processed, or further processed, in a lawful and reasonable manner that does not knowingly infringe on the rights of the data subject.

These include:

7.1. Minimality

Hollard must only process the minimal required information to provide the service or product to the data subject. No excessive information should be processed. Information should only be processed if there is a legitimate lawful basis for processing that information.

7.2. Lawful basis to process PI

Under PoPIA, Hollard must be able to demonstrate a lawful basis (ground) for the processing of PI.

Hollard must only process PI when the following conditions are met:

- a) Perform or conclude a contract necessary to deliver a product/service to the data subject.
- b) Comply with a legal/ regulatory obligation.
- c) Express consent is obtained from the data subject.
- d) Protect the legitimate interests of the data subject.

Hollard has interpreted the PoPI Act to imply that consent does not have to be gained explicitly where processing PI is necessary during the course of fulfilling a contractual or performance obligation.

A data subject has the right under PoPIA to object at any time to processing of their PI or withdraw their consent to process their PI. The objection or withdrawal must follow the prescribed procedure, on reasonable grounds relating to his/her situation. This is outlined under data subject participation rights.

PI must be collected directly from the data subject, unless:

- a) Collection from other sources does not prejudice the data subject;
- b) The data is available as a public record or has been made public by the data subject;
- c) The data subject provided consent to the collection of the information from another source;
- d) The collection from another source does not prejudice the legitimate interest of the data subject;
- e) Compliance is not reasonably achievable (the Information Privacy Officer (IPO) must be consulted for these exceptions); or
- f) Collected in compliance with legislation.

8. Purpose Specification

8.1. Retention of Records

Hollard must retain records if it is:

- a) Required by law.
- b) In line with Hollard's legitimate business interests.
- c) In line with the purpose for which it was collected.
- d) For historical, statistical or research purposes.

When the records are no longer required, Hollard must destroy and/or de-identify the PI within a reasonable period. The details regarding record retention are explained in the Hollard Data Retention, Classification and Handling Policy.

9. Further Processing Limitation

Where Hollard is required to further process the information, this must be done in line with the original purpose for which it was collected. This extends to cases where further processing will result in a clear benefit to the data subject or a third party. Should the required further processing not align to the original purpose, then the data subject needs to be notified, and explicit consent needs to be obtained from the data subject.

To assess whether further processing is allowed, consideration should be given to:

- a) The contractual relationship between Hollard and the data subject;
- b) The consequences of further processing for the data subject; and
- c) The nature of the information collected.

Further processing will be considered lawful for Hollard, if the information is derived in terms of the statements hereunder:

- a) It is derived from a source within the public domain.
- b) It is required to avoid prejudice, required for court proceedings or to adhere to regulatory requirements/ requests from regulators.
- c) It is required as a matter of national security or to prevent a real or imminent threat to public health and safety or the data subject.
- d) For historical, statistical and research purposes and in a non-identifiable form.

10. Information Quality

Hollard must take reasonable practical steps to ensure that PI is complete, accurate, not misleading, and updated, where necessary.

11. Openness

When PI is collected, Hollard must take reasonable practical steps to notify the data subject:

- a) That their PI is being collected and the source from which it is collected (if it is not collected from the data subject).
- b) Of the purpose for which the PI is collected.
- c) Whether the information supplied is voluntary or mandatory.
- d) Of the consequences of failure to provide the information.
- e) Whether third parties are involved in processing the information.
- f) Of the data subject's rights as it pertains to:
 - access to their PI.
 - their rights to object to processing.
 - their rights to correct/delete their PI.
 - their right to lodge a complaint with the Information Regulator.

The Openness principle is embodied in the following ways:

- a) Full and detailed Privacy Notice: Hollard public website.
- b) Summarised Privacy Notice: Terms and conditions for policy wording.
- c) Short Form Notices: In-bound and out-bound call centre scripts, letters, and form footers, etc.

12. Security Safeguards

Hollard must use its operations, safeguard, and secure the PI in its possession or under its control. It must implement appropriate, reasonable technical and organisational measures to prevent:

- a) Loss, damage, or unauthorised destruction of PI; and
- b) Unlawful access to or processing of PI.

Hollard must secure the integrity and confidentiality of PI by taking reasonable practical steps to:

- a) Identify foreseeable internal and external risks to PI.
- b) Establish and maintain appropriate safeguards against risk.
- c) Ensure ongoing, continual updates of risk responses.

When PI is processed on behalf of Hollard, the third party must process PI:

- a) only with the knowledge and authorisation of Hollard as the responsible party. Hollard must ensure that there is a written contract between itself and its operators (third parties) or co-responsible parties, to establish and maintain security safeguards.
- b) by treating the PI as confidential.

13. Data Subject Participation

Hollard is committed to protecting the rights of individuals whose personal information it processes. In line with the Protection of Personal Information Act (POPIA), data subjects have the right to participate in how their personal information is used. This includes the ability to request updates or corrections, object to processing, and lodge complaints. Hollard has established clear procedures to manage these requests and ensure compliance with the regulation. The following subsections outline these rights and responsibilities in more detail.

11.1 Requests and Objections

Data subjects have the right to ask Hollard to update, correct, or delete their personal information if it is inaccurate, irrelevant, outdated, incomplete, or collected unlawfully. These requests can be submitted through various channels, including hand delivery, postal mail, email, or telephone. If a request or objection is made telephonically, Hollard will record the call and provide a copy of the call to the data subject upon request.

Once an objection is raised, Hollard is required to restrict the processing of the affected personal information. If the objection or withdrawal of consent prevents Hollard from fulfilling its contractual or performance obligations, Hollard will follow its standard business procedures to end the contractual relationship. In such cases, Hollard will inform the data subject of the decision and explain the consequences.

If a request cannot be fulfilled, due to reasons such as the inability to verify the data subject's identity or the potential impact on decision-making or contractual obligations, Hollard will communicate this to the data subject and clarify the implications.

11.2 Procedures under POPIA Regulations

To manage these interactions effectively, Hollard has implemented a Privacy Incident Management process. It also covers the handling of complaints, which may be submitted by the data subject, a representative, or any party with sufficient interest.

Hollard will acknowledge receipt of complaints within 14 calendar days. If necessary, complaints may be escalated to the Information Regulator, who may assist with lodging and resolving the matter. Any disputes or reasons for the non-supply of information will also be addressed through this process.

Once a request is validated and authorised, Hollard must ensure it is actioned within 30 calendar days.

14. Special Personal Information and Information of Children

Hollard must not process Special Personal Information and Information of Children unless:

- a) The processing is carried out with the data subject's explicit consent, or in the case of children, with the prior explicit consent of a competent & legally authorised person.
- b) The processing is necessary to establish, exercise, or defend a right, or to comply with a regulatory requirement.
- c) The processing is necessary to comply with international public law.

- d) The process is for historical, statistical, or research purposes to the extent that:
- It serves a public interest and is necessary for the purpose concerned; or
 - It appears to be impossible or would involve a disproportionate effort to ask for consent and enough guarantees are provided for, to ensure that the processing does not adversely affect the individual privacy of the data subject to a disproportionate extent.

Extra care must be taken when deciding to process this information, including applying for processing authorisation from the Information Regulator (where required).

15. Direct Marketing

Hollard must ensure that they gain explicit consent from the data subject in order to market directly to the data subject. Consent may be obtained using a method that is substantially similar to Form 4 or through any accessible, free, and reasonable means including email, SMS, or telephone. Where consent is obtained telephonically, an electronic record of such consent will be kept and made available to the data subject upon request free of charge.

If a data subject withdraws their consent for direct marketing Hollard must cease to market directly. Hollard may approach a data subject once to obtain their consent to market directly, unless the data subject requests that they be approached at a later stage. Opting out of direct marketing communications does not constitute valid consent under POPIA.

Hollard must maintain an up-to-date record of the customer's marketing preferences and use the incident response process to address withdrawal of consent both internally and with any third parties that market on behalf of Hollard.

16. Automated Decision-Making

Hollard must not make decisions that will subject a data subject to legal consequences, or affect them substantially based solely on the automated processing of information unless:

- a) It is taken in connection with the conclusion or execution of a contract.
- b) The request of a data subject, or measures have been taken to protect the data subject's legitimate interest.
- c) It is governed by a law or code of conduct.

If Hollard uses automated decision making, Hollard will ensure that measures are in place that ensures that:

- a) The data subject's rights and legitimate interests are not infringed; and
- b) The data subject can request human intervention to discuss the decision or contest it.

17. Privacy Incident Management

In the case where there are reasonable grounds to believe that PI has been accessed or acquired by any unauthorised person, Hollard must deal with this incident in accordance with the prescripts described in the Risk Event Management Policy.

Hollardites must report any data breach or privacy incident as soon as they become aware of it to the IO or the relevant BU Incident response representative. In line with established escalation protocols, the incident must be logged with Group Risk Management for appropriate tracking, response, and oversight.

18. PAIA Manual

The objective of PAIA is to uphold the constitutional right of all individuals in South Africa to access their information held by either the state, or a private body. This information can be obtained for the purpose of exercising or protecting any right contained in the Bill of Rights. Hollard needs to have a PAIA manual that fosters a culture of transparency and accountability. Hollard must recognise the rights of a data subject who has adequately validated their identity to gain access to their PI.

Hollard must at all times have a PAIA manual saved on the Hollard website with clear instructions to assist data subjects to access their information.

Hollard must confirm, free of charge, whether Hollard holds PI about the data subject. This process should be managed as part of the existing incident response processes.

In the case where the data subject requests a record or description of PI held by Hollard, Hollard will provide it:

- a) Within a reasonable time (maximum of 30 calendar days)
- b) At a prescribed fee (if applicable)
- c) In a reasonable manner and format; and
- d) In a form that is understandable.

19. Privacy By Design

As best practice, Privacy by Design (PbD) principles must be embedded to ensure that all new projects and products that Hollard develops or embark on are assessed vigorously. Hollard must adhere to privacy by design processes that had been put in place to ensure that the privacy and security impact is assessed, and the appropriate privacy controls are considered from the design phase.

20. Training and Awareness

Hollard is committed to raising awareness and ensuring that all employees understand the importance of privacy awareness, specific privacy policies, procedures and processes.

21. Third Party Privacy Risk Management

As a Responsible party, Hollard is accountable for any PI we share with our third parties, vendors, and suppliers, therefore Hollard must ensure that:

- a) All new and existing third-party contracts/agreements are updated with data protection clauses.
- b) All new and existing third parties are assessed through the third-party risk assessment questionnaire and ensure all privacy gaps identified are remediated accordingly.

22. Transferring Data

Hollard must ensure that reasonable controls, in line with Hollard's Security policies, are put in place when transferring data both internally, with third parties and/or outside the borders of South Africa.

The following must be followed or assessed:

- a) Internal data transfers - Hollardites must use a secure medium or password protect the data if there is sensitive information including PI that others would not be authorised to see.

b) Third party data transfers -

- Use a secure file transfer method or password protecting the data and sharing the password using a different medium.
- If the transfer is outside the borders of South Africa (cross border flows), ensure the contract/agreement has data protection clauses, if not the Data transfer agreement must be signed by both parties. Hollardites must check whether the country the information is being transferred to has data protection laws, if not, the agreement and third-party risk assessments must be in place and approved by the PIO or DIO.

Hollardites are not allowed to download unauthorised software to transfer data (e.g., drop box). Hollardites must reach out to IT to check whether the transfer tools they are using are allowed. Failure to use authorised systems may lead to PI being hacked and subsequently a data breach.

23. Policy Review and Version Control

The policy is reviewed by the Information Privacy Officer to ensure it accurately reflects the desired practice within Hollard when necessary or due to regulatory or legislative changes.

Owner	Mohammed Aslam Patel (Head of Group Compliance & Privacy Information Officer)
Policy effective date	Approval date
Policy Level	Level 2
Approved by	Board of Directors (Group Audit & Compliance Committee)
Approval date	6 March 2026
Version control	Version 10
Version updates	The policy needed to be updated to comply with the current regulatory updates.

24. Definitions

Term	Description
Automated decision-making	An automated transaction where there is no human intervention involved in the decision-making process. This can include decisions in respect of work performance, credit worthiness, reliability, location, health, personal preferences, or conduct.
Data subject	The Person to whom the information relates.
Information Privacy Officer (IPO)	• Manage privacy across Hollard. • Manage privacy incidents. • Manage Regulator relationship and requirements from the Information Regulator. • Monitor privacy and reporting and reporting on them.
Person	Any natural person or juristic person.
Personal Information(PI)	Any recorded information pertaining to a Person, including but not limited to the following, which can be in either hard copy or electronic format: • Race, gender, sex, pregnancy, marital status, nationality, ethnicity or social origin, colour, sexual orientation, age,

	physical or mental health and well-being. • Belief, religion, conscience, culture, language and birth. • Information relating to education, medical, financial, criminal or employment history. • An identifying number or symbol. • Disability, blood type, biometric information. • Personal opinions, views, or preferences. • Correspondence of private or confidential nature, views, or opinions of another individual. • Name of a Person if it appears with other personal information. • Consumer or purchasing pattern. • E-mail address, physical address, location information or online identifier and telephone number. • Any item of information that, either on its own or in conjunction with any other item, can uniquely identify and/or Special Personal Information.
Processing / Processes / Processed	Any operation or set of operations or activity, whether by automatic means, concerning Personal Information, includes: • Collection, receipt, recording, organisation, collation, and storage. • Updating, modification, retrieval, and alteration. • Consultation or use. • Dissemination by means of transmission. • Distribution or making available in any other form, or • Merging, linking as well as restriction, degradation, erasure, or destruction of information.
Promotion of Access to Information Act 2 of 2000 (PAIA)	The Promotion of Access to Information Act 2 of 2000 (PAIA) gives effect to the constitutional right of access to any information held by the State and any information that is held by another person and that is required for the exercise or protection of any rights. PAIA gives the requester the right to lodge a request from the information officer of a public or private body. PAIA requires all private and public bodies to prepare a PAIA manual.
Protection of Personal Information Act 4 of 2013 (PoPIA)	The Act emphasises the importance of protecting personal information and the rights of individuals regarding their personal data. It highlights the constitutional right to privacy and the need to regulate the processing of personal information in a manner that respects and fulfills this right. The Act establishes minimum conditions for the lawful processing of personal information.
Special Personal Information (SPI)	A specific category of Personal Information. Examples of Special Personal Information are, religious or philosophical beliefs, race or ethnic origin, trade union membership, political opinions, health, sex life, criminal behaviour, and biometric information. Where Personal Information is referenced, it will automatically include Special Personal Information unless otherwise indicated.