DATA AND INFORMATION PRIVACY POLICY

This policy describes the policy statements, accountabilities and responsibilities for implementing, monitoring, reviewing, and reporting on data and information privacy management in Envestpro (Pty) Ltd.

Table of Contents

Glossary of abbreviations and definitions

The table below lists the terms and acronyms used within this document.

TERM	DISCRIPTION
Affected Person	A data subject or representative of a data subject.
Biometrics	A technique of personal identification that is based on physical, physiological or behavioural characterisation including blood typing, fingerprinting, DNA analysis, retinal scanning and voice recognition.
Child	Means a natural person under the age of 18 years who is not legally competent, without the assistance of a competent person, to take any action or decision in respect of any matter concerning the child.
Competent person	Any person who is legally competent to consent to any action or decision being taken in respect of any matter concerning a child.
Consent	Any voluntary, specific and informed expression of will in terms of which permission is given for the processing of personal information.
Data subject	The person to whom personal information relates to.
De-identify	In relation to personal information of a data subject, means to delete any information that: • identifies the data subject; • can be used or manipulated by a reasonably foreseeable method to identify the data subject; or • can be linked by a reasonably foreseeable method to other data and information that identifies the data subject.
Direct Marketing	To approach a data subject, either in person or by mail or electronic communication, for the direct or indirect purpose of: • promoting or offering to supply, in the ordinary course of business, any goods or services to the data subject; or • requesting the data subject to make a donation of any kind for any reason.
Electronic communications	Any text, voice, sound or image message sent over an electronic communications network which is stored in the network or in the recipient's terminal equipment until it is collected by the recipient.
FSCA	Financial Services Conduct Authority.
Juristic Person	A legal entity such as a company, close corporation or trust.
Operator	A person who processes personal data and/ or information for a responsible party in terms of a contract or mandate, without coming under the direct authority of that party.
Person	A natural person or a juristic person to whom personal information relates (data subject).
Personal Information	• Data and/ or information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person; • Data and information relating to the education or the medical, financial, criminal or employment history of the person; • any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person; Envestpro (Pty) Ltd: Data and information privacy Policy • the biometric data and/ or information of the person; • the personal opinions, views or preferences of the person; • correspondence sent by the person that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence; • the views or opinions of another individual about the person; and • the name of the person if it appears with other personal data and information relating to the person or if the disclosure of the name itself would reveal data and information about the person.
PoPIA	Protection of Personal Information Act No. 04 of 2013.
Processing	Any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including: • the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, 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.
Record	Any recorded information— (a) regardless of form or medium, including any of the following: (i) Writing on any material; (ii) Data and Information produced, recorded or stored by means of any tape-recorder, computer equipment, whether hardware or software or both, or other device, and any material subsequently derived from data and/ or information so produced, recorded or stored; (iii) label, marking or other writing that identifies or describes anything of which it forms part, or to which it is attached by any means; (iv) book, map, plan, graph or drawing; photograph, film, negative, tape or other device in which one or more visual images are embodied so as to be capable, with or without the aid of some other equipment, of being reproduced; (b) in the possession or under the control of a responsible party; (c) whether or not it was created by a responsible party; and (d) regardless of when it came into existence.
Responsible Party	Means a public or private body or any other person which, alone or in conjunction with others, determines the purpose of and means for processing personal information.
Special Personal Information	Personal information as referred to in section 26 (of the POPIA act) including any elements or fields related to the following categories: • Religious or philosophical beliefs • Race or ethnic origin • Trade union membership • Political persuasion or affiliations • Health or sex life • Criminal behaviour • Biometrics • Personal information of children
Liberty Group Limited	Liberty Group Ltd is an Authorised Financial Services Provider in terms of the FAIS Act (Licence No. 2409)
Envestpro (Pty) Ltd	Envestpro (Pty) Ltd is affiliated to the Liberty Group Limited and a national distribution partner.

1 Purpose

The purpose of this policy is to establish the policy statements, accountabilities and responsibilities for implementing, monitoring, reviewing and reporting on data and information / data privacy management (hereafter referred to as information) in Envestpro (Pty) Ltd (ENV). The policy has been developed to protect ENV, its employees, assets,

operations and reputation in the environment in which it operates and to ensure the protection of personal information (with a focus on customers and employees).

ENV is committed to safeguarding its data and information assets, operations and reputation; at all times acting in a manner consistent with the relevant regulations, frameworks and compliance obligations.

2 Scope and applicability of this policy

2.1 This policy applies to all persons within ENV and all of its subsidiaries. Any deviation from the requirements of this policy requires approval from the appropriate governance structures. The sophistication of this policy is appropriate to the nature, scale and complexity of the specific business area and risk concerned and will be adapted as the business and environment changes.

2.2 This policy reflects ENV's minimum requirements and may be supplemented in a local jurisdiction or business policy or procedure. The local Compliance function or Business Compliance Officer (BCO) must be consulted in respect of the existence of any local or business policies.

2.3 In the event of any conflict between this policy and any other policy dealing with the Processing of Personal Information, this policy takes precedence. Where a local jurisdiction or business line requires stricter requirements, those requirements will apply. This policy is applicable to all personal information elements stored physically or electronically, independently or in conjunction with other personal information elements, across the entire information management lifecycle as described in the ENV Group Data and Information Lifecycle Management Policy.

3 Policy Statement

This policy sets out ENV's approach and practices to manage data and information privacy across the entirety of ENV's operations as a Responsible Party. The policy upholds the spirit intended by the South African constitution as it preserves the integrity and quality of personal information entrusted to LHL.

This policy further supports the privacy rights of individuals and complies with the conditions for lawful processing of personal data and information as described in the Protection of Personal Information Act (PoPIA), including subsequent regulations and guidelines or industry codes which may be issued by relevant regulatory authorities i.e., the Information Regulator and/ or Financial Services Conduct Authority (FSCA), ensuring that:

- ENV manages Data Privacy Risk;
- ENV maintains and continuously improves its Data Privacy culture;
- all Employees and advisors and advisor private assistants are made aware of their obligations in terms of applicable legislation and internal rules relating to the Protection of Personal Information;

The following policy statements depict ENV's stance and its allegiance to its obligations:

3.1 Policy Statement 1: Accountability

ENV must identify and make organisational provisions (governance, people, process and technology) to manage data and information privacy throughout the information life cycle. These provisions must support and align with applicable data and information privacy regulations, legislation and internal directives.

3.2 Policy Statement 2: Processing limitation

All personal information collected and used by ENV must be done lawfully and in a reasonable manner which does not infringe on any person's privacy. This includes holding only the minimal amount of personal data and information required, obtaining consent to use personal information (where required), and allowing individuals to object to the use of their information, and as far as possible, collecting data and information directly from persons and juristic entities.

NEVER:

- share personal information of a client with anyone unless you have written consent from the client;
- share any policy or insurance related detail with any third party including the spouse of the client.

These are areas of specific concern where the POPI requirements are breached.

ASTUTE

Scenario 1:

An authority to release policy information is signed by the client. The consultant proceeds to obtain and download the client's policy / investment information from Astute. Policies and or Investments where the client is **not the owner** but only the Life Assured (e.g., Buy & Sell Policies / Keyman Policies) also download due to the clients ID number being associated with the policy. Consultant proceed to discuss and or give advice on the policies and or investments with the client where the client is only the life assured on the policy and not the owner.

This is a breach of the POPI act. Insurer and the consultant are fined due to this breach of the act as they do not have the Owners authority to discuss/ obtain or share personal information.

Remedy:

- Obtain written authorisation from the Owner to share and or advise on the policies where your client is not the owner but only the life assured.

PERSONAL INFORMATION GENERAL

Scenario 2:

Client's Wife phones stating that she needs her husband's policy information on their joint policy where she is the spouse on the policy or need the husband's policy information as she is handling all debit orders or need to check that their insurance is correct on their short-term policy or they are going through a divorce.

Consultant proceed to supply the information.

Consultant is in breach of the POPI act as the consultant processed personal information to a 3rd party without consent.

Remedy:

- Obtain written authorisation from the Owner to share the information.

  Or

- Agree to send the information but send the information to the client (owner) and ask the owner to share the information with the wife or 3rd party.

3.3 Policy Statement 3: Purpose specification

Personal information must at all times only be collected and used for specific purposes, and the affected person must be aware of the information collected and what it will be used for. Records must only be kept for such time as the person or juristic entity has a relationship with ENV / Liberty Holdings Limited (LHL) or as required by law or to support a business need, following which they will be restricted and securely archived or securely disposed of in such a way that they cannot be reconstructed in any intelligible form.

3.4 Policy Statement 4: Further processing limitation

Personal information may only be used for secondary purposes (processing beyond initial collection purposes), provided this further processing is disclosed to the affected person. Should personal information be de-identified in such a way that it cannot be linked back to an individual, then such information may be used for other purposes without notifying the individual. Consent must be gained and maintained for marketing purposes.

3.5 Policy Statement 5: Information quality

ENV must take reasonable measures to ensure that all personal information under its control is complete, accurate and not misleading, and will offer affected persons various platforms and opportunities to update or correct their personal information. An individual's identity must be appropriately verified before allowing them to access, correct or update any personal information related to them.

3.6 Policy Statement 6: Openness

ENV must maintain a manual for both Promotion of Access to Data and Information (PAIA) and PoPIA requests. This notifies persons and the general public of its data and information practices. At points where personal information is collected, affected persons must be made aware of:

- what the data and information will be used for;
- the consequences of failing to supply such information;
- any laws which authorise such collection;
- where information may be transferred to a third party or across international borders;
- and the rights that they have in terms of their personal information.

3.7 Policy Statement 7: Security safeguards

ENV must ensure that organisational controls (subscribing to international good practices) are in place to protect all personal information for which it is responsible. This includes adhering to the governance set forth by the Chief Information Officer (CIO), access controls, Information security safeguards, processes and technology to prevent loss of, damage to, or unauthorised access or processing of personal information. These controls must be monitored, and periodically be evaluated by the Privacy Officer, to ensure that they are operating effectively and to identify areas for improvement.

PoPIA Awareness & Training

Env will ensure required training and continuous awareness of PoPIA regulations and responsibilities.

This will be applicable to all individuals contracted to Env, all Liberty Group Limited independently contracted Financial Advisors associated with Env and all private administrative personnel employed by Financial Advisors direct.

All new individuals as described above will be required to complete the respective training module as soon as possible within their first 30 days of employment.

Secure physical documents

Volume (Secure filling of all documentation including notes and email correspondence with clients)

Only authorised individuals can access and access is restricted to specific areas within the system.

Shredding

Iron Mountain (secure destruction of ALL physical documents after it was securely filles)

Clean desk policy / Lock drawers

- File paper records and emails on a regular basis in Volume.
- Dispose of all sensitive documents after it was securely filed in Volume using the secure shredding boxes provided.

Secure electronic devices

- All mobile devices / laptops / Desktop Computers / I pads must be secured and have a pass code setup in order to limit unauthorised access to these devices.
- Ensure that complex passwords are used to access all devices and systems.

- **Desktop Computer / Laptop - Lock screens**
  All devices must be secured with a User Password.
  All devices must be locked if not in use.

  Best Practice:
  If you leave your desk and you know that you will be away for some time lock your device manually. Do not wait until the screen saver as per step 2 above is activated.

3RD PARTY CONTRACTORS

Any third parties providing services to ENV and who have access to personal information are required to adhere to similar security safeguards and ENV reserves the right to review their information security practices and procedures at any time. These safeguards must be documented in the form of a written agreement between ENV and the third-party

provider, in accordance with POPIA requirements. In the event that personal information is compromised, appropriate notification and risk mitigation procedures are to be followed, including notification to the Information Regulator, and any potentially affected individuals.

3.8 Policy Statement 8: Data subject participation

ENV must ensure that persons are provided access to their own personal information, so that they may correct or update it as appropriate or exercise any other rights that they may have under applicable data and information privacy laws.

3.9 Policy Statement 9: Special personal information

If any of the categories of special personal information as defined by POPIA are used, suitably stringent security controls must be in place to protect such information. Explicit consent should be collected from any individual before such special personal information is collected, unless otherwise provided for by law. Where the law requires collection of special personal information (e.g., employment equity, disability, health and safety, or other regulations) consent is not required, but individuals should still be informed of the purposes for which this information is collected.

Consent must be obtained from parents or legal guardians in cases where the information of children (i.e., minors under the age of 18) is collected or processed.

3.10 Policy Statement 10: Direct marketing

If it is a business requirement, direct marketing and external communication activities must adhere to POPIA requirements and the Customer Communication Privacy and Information Security Guidelines.

3.11 Policy Statement 11: Automated decision-making

A data subject shall have the right not to be subject to a decision which is based exclusively on an automated decision-making system, and which results in legal consequences or affects him or her to a substantial degree. Liberty must provide persons with a process whereby they may make representation about any decision made solely by an automated system or associated processing.

3.12 Policy Statement 12: Transborder flows of information

The transfer of personal information outside the Republic of South Africa is prohibited unless such transfer adheres to the requirements of POPIA, including:

- seeking prior authorisation from the Information Regulator (as applicable; this is however a mandatory legal requirement for ALL transfers of special personal information),
- ensuring that the jurisdiction to which the personal information is transferred has data protection laws similar to POPIA, and
- for jurisdictions without appropriate laws, ensuring that appropriate security safeguards and other control mechanisms are in place, and that these are documented in a written and enforceable agreement.

4 Responsibilities

The appropriate governance bodies within ENV and at business level will oversee the execution of the policy. The specific responsibilities are described in this section.

4.1 Business Area

- Executive Management must ensure that the appropriate resources (budgetary, skills and capacity) are made available to support the policy statements of this policy and support ENVs privacy compliance requirements.
- Executive management are responsible to ensure their staff, contractors and third parties are aware of and that their relevant BU's comply with this policy and standards, and any other related policies.
- Executive Management must ensure that all changes to business processes are assessed for privacy impact, documented and communicated to the process management team.
- Reviews reports and addresses compliance and non-compliance to this policy within the respective business areas.
- Report material non-compliance to the relevant governance bodies.

4.2 ENV Data and Information, Information Security and Privacy Committee (DIISP)

- Approves this data and information privacy policy.
- Reviews reports of non-compliance and ensures that corrective actions are undertaken to address non-compliance and obtains feedback on the progress of action plans.
- Raises any risks or concerns to the relevant board.

4.3 Group Information Officer / Deputy Officers

- Creates the awareness of this policy and other related data and information privacy directives and ensures a strong risk awareness culture amongst all categories of staff and where applicable, third parties.
- Executes the following duties, as described in privacy related regulation and legalisation e.g. POPIA and PAIA:
    - Encourage compliance with the conditions for the lawful processing of personal information as described in POPIA and any other applicable data protection legislation or regulations;
    - Deal with information requests;
    - Work with the Information Regulator or relevant regulatory bodies in relation to investigations and requests;
    - Ensure and oversee ENV's privacy compliance regulatory universe;
    - Delegate / appoint deputy information privacy officer(s) or privacy managers as necessary.
- Provides general guidance on the direction of privacy and how it is linked to other strategic business initiatives.
- Ensures appropriate privacy governance and oversight across ENV operations.
- Cooperates with internal stakeholders;
- Reports any material Data Privacy Risks and breaches through the reporting governance structures.
- In conjunction with Deputy Privacy Officers and privacy managers ensures that Data Privacy breaches are reported to regulators, if required, in a timely manner and in accordance with the jurisdictional Data Privacy requirements.
- Obtains legal opinions on Data Privacy matters affecting the ENV from LHL Group Legal or from external legal counsel, if necessary;

4.4 Liberty Holdings Group Legal

- Advise on legal aspects regarding data and information privacy related legislation.
- Track and inform business of changes to legislation impacting privacy.
- Draft and review contracts or service agreements as it pertains to privacy requirements.
- Provide privacy focused input on the legalities of certain business activities to ensure that they are aligned with legislation.

4.5 Human Resources (GHR)

- HR assists management in enforcing the disciplinary process for non-compliance.
- HR also assists in socialising the Group privacy policy and standards with new employees through the induction program.

4.6 Employees, Contractors and Third Parties

All employees, contractors or other third parties who may have access to personal information as a result of their relationship with Envestpro must take responsibility for protecting this information.

All employees, contractors and other third parties shall be bound by a duty of confidentiality for all such personal information and may not disclose, distribute, use or store such personal information beyond the execution of their duties or responsibilities within the Envestpro context.

Any incidents or suspected incidents related to personal information, data breaches or non-compliance with this policy or the provisions of POPIA or other applicable data protection legislation or regulations must be reported to the Group Privacy Office immediately.

5 Compliance and Reporting

Executive management within the respective business areas shall report on compliance and non-compliance with this policy and report any issues to the appropriate governance forums.

Any non-adherence to this Policy must be promptly reported to line management, the relevant Business Compliance/ privacy representative and the Group Privacy Office. Any non-adherence with this policy may lead to disciplinary and/or legal action being taken.

6 Related Information

- ENV PAIA Manual
- LHL Group Data & Information Lifecycle Management Policy
- LHL Information Security and Cyber Resilience Policy
- LHL Acceptable Usage Policy
- LHL Compliance Policy
- LHL PAIA Manual
- LHL Data in Transit Standard
- LHL Customer Communication Privacy and Information Security Guidelines