



Name	Protection of Personal Information Act (POPIA) Policy Statement	
Version	Version 1	
Publishing Date	31 May 2025	
Last Review Date		
Frequency of Review	Annual	
Next Review Date	31 May 2026	
Policy Owner	Windall Bekker	
Responsible	Business	Management

## POLICY STATEMENT

- Any reference to the “organisation” shall be interpreted as **Digiwealth Pty Ltd (DW)**.
- The organisation’s Governing Body, its employees, volunteers, contractors, suppliers and any other persons acting on behalf of the organisation are required to familiarise themselves with the policy’s requirements and undertake to comply with the stated processes and procedures.

## POLICY ADOPTION

By signing this document, I authorise Digiwealth Pty Ltd (“DW”) approval and adoption of the processes and procedures outlined herein.


Name & Surname	Windall Bekker
Capacity	Key Individual
Signature	
Date	31 May 2025

---

Authorised FSP 55173

e: [info@digiwealth.co.za](mailto:info@digiwealth.co.za) | [www.digiwealth.co.za](http://www.digiwealth.co.za)

a: 13 Belvedere Street, Durbanville, Cape Town, South Africa, 7551

 + (27) 82 759 2318 | t: + (27) 21 975 2535

## TABLE OF CONTENTS

1	DEFINITIONS .....	4
2	Introduction.....	4
3	Purpose .....	5
4	Scope and Application.....	5
5	Definitions .....	6
6	Principles of POPIA Compliance.....	7
7	Conditions for Lawful Processing.....	7
8	Collection and Use of Personal Information.....	8
9	Data Subject Rights .....	8
10	Security Safeguards and Breach Management.....	9
11	Retention and Destruction .....	9
12	Information Officer and Responsibilities.....	10
13	Complaints and Dispute Resolution .....	10
14	Training and Awareness .....	10
15	Review and Amendments.....	10
16	Contact Details.....	11

Authorised FSP 55173

e: [info@digiwealth.co.za](mailto:info@digiwealth.co.za) | [www.digiwealth.co.za](http://www.digiwealth.co.za)

a: 13 Belvedere Street, Durbanville, Cape Town, South Africa, 7551



+ (27) 82 759 2318 | t: + (27) 21 975 2535

## 1 DEFINITIONS

### 1.1 Conflict of Interest

Conflict of Interest means any situation in which a provider or a representative has an actual or potential interest that may, in rendering a financial service to a client:

- influence the objective performance of his, her or its obligations to that client; or
- prevent a provider or representative from rendering an unbiased and fair financial service to that client, or from acting in the interest of that client,
- including but not limited to:
  - a financial interest.
  - an ownership interest.
  - any relationship with a third party.

#

## 2 Introduction

Digiwealth Pty Ltd (the "DW") is committed to protecting the privacy and personal information of its clients, employees, suppliers, and other data subjects in accordance with the Protection of Personal Information Act, No. 4 of 2013 ("POPIA" or "the Act"). As a Financial Services Provider authorised under the Financial Advisory and Intermediary Services Act, 2002 (FAIS), the FSP processes personal information to provide financial advisory, intermediary, and related services.

This Policy Statement outlines the FSP's approach to complying with POPIA, ensuring that personal information is processed lawfully, transparently, and securely. It balances the constitutional right to privacy with the legitimate needs of the FSP to collect and use

---

Authorised FSP 55173

e: [info@digiwealth.co.za](mailto:info@digiwealth.co.za) | [www.digiwealth.co.za](http://www.digiwealth.co.za)

a: 13 Belvedere Street, Durbanville, Cape Town, South Africa, 7551



+ (27) 82 759 2318 | t: + (27) 21 975 2535

personal information for business purposes. The FSP acts as a "Responsible Party" under POPIA, determining the purpose and means of processing personal information.

POPIA applies to all processing activities involving personal information of natural and juristic persons, including clients, prospective clients, employees, and third parties. Non-compliance may result in regulatory penalties, reputational damage, and civil claims.

### 3 Purpose

The purpose of this Policy is to:

- Establish a framework for the governance, management, and protection of personal information.
- Ensure adherence to the eight conditions for lawful processing set out in Chapter 3 of POPIA.
- Promote accountability, transparency, and ethical data handling practices.
- Provide guidance to FSP personnel, operators (third-party processors), and data subjects on rights and obligations.
- Facilitate ongoing compliance monitoring, training, and response to data breaches or complaints.

This Policy aligns with the FSP's broader risk management and compliance obligations under FAIS and other applicable legislation.

### 4 Scope and Application

This Policy applies to:

- All FSP employees, representatives, contractors, and key individuals who process personal information on behalf of the FSP.

- All personal information processed by the FSP, whether in physical, electronic, or other form, including collection, storage, use, disclosure, and destruction.
- Business processes such as client onboarding, needs analysis, product recommendations, claims processing, fraud detection, and direct marketing.

It does not apply to anonymised or de-identified information that cannot be linked to a data subject.

## 5 Definitions

- Data Subject: A natural or juristic person to whom personal information relates (e.g., clients, employees).
- Personal Information: Information relating to an identifiable, living, natural person, and where applicable, an identifiable, existing juristic person, including (but not limited to): name, ID number, contact details, financial information, health records, biometric data, criminal history, or opinions/views about the person.
- Processing: Any operation or activity concerning personal information, including collection, storage, use, disclosure, or destruction.
- Operator: A third party (e.g., cloud service provider) that processes personal information on behalf of the FSP under contract.
- Information Officer: The FSP's designated officer responsible for POPIA compliance (details below).
- Special Personal Information: Sensitive data such as religious beliefs, health status, or biometric information, which requires additional safeguards.



## 6 Principles of POPIA Compliance

The FSP processes personal information in accordance with the following eight conditions under POPIA:

Principle	Description	FSP Application
Accountability	The FSP is responsible for compliance and must demonstrate adherence	Appoint an Information Officer; conduct regular audits and impact assessments
Processing Limitation	Processing must be lawful, for a specific purpose, and minimal	Collect only necessary data for financial services; obtain consent where required
Purpose Specification	Inform data subjects of the purpose before collection	Provide privacy notices during client onboarding
Further Processing Limitation	Further use must be compatible with the original purpose	No repurposing without consent or legal basis
Information Quality	Ensure accuracy, completeness, and timeliness	Implement verification processes; allow corrections
Openness	Notify data subjects of processing activities.	Disclose via policy, website, and consent forms
Security Safeguards	Protect against loss, unauthorised access, or breaches	Use encryption, access controls, and breach response plans
Data Subject Participation	Allow access, correction, or deletion upon request	Handle requests within 30 business days

## 7 Conditions for Lawful Processing


Personal information may only be processed if:

- The data subject consents voluntarily and specifically (e.g., via signed forms for marketing).
- It is necessary to conclude or perform a contract (e.g., financial product provision).

Authorised FSP 55173

e: [info@digiwealth.co.za](mailto:info@digiwealth.co.za) | [www.digiwealth.co.za](http://www.digiwealth.co.za)

a: 13 Belvedere Street, Durbanville, Cape Town, South Africa, 7551

 + (27) 82 759 2318 | t: + (27) 21 975 2535

- It complies with a legal obligation (e.g., FAIS reporting).
- It protects the data subject's legitimate interests (e.g., fraud prevention).
- It is required for the FSP's legitimate interests, balanced against privacy rights.
- It is for journalistic, literary, or artistic purposes (not applicable to FSP).
- It is for historical, statistical, or research purposes (with de-identification).

For special personal information (e.g., health data for insurance), explicit consent or a legal basis is mandatory. Cross-border transfers require adequacy decisions or binding agreements ensuring equivalent protection.

## 8 Collection and Use of Personal Information

The FSP collects personal information directly from data subjects (e.g., via application forms) or indirectly (e.g., from credit bureaus). Purposes include:

- Conducting needs analysis and providing financial advice.
- Underwriting, claims processing, and policy administration.
- Compliance with regulatory requirements (e.g., FIC Act for anti-money laundering).
- Marketing (with opt-in consent).
- Internal record-keeping and research (anonymised).

Direct marketing via electronic means requires prior consent; data subjects may opt out at any time.

## 9 Data Subject Rights

Data subjects have the following rights:

- Access: Request confirmation of whether the FSP holds their information and a copy (free or fee-based).





- Correction/Deletion: Update or delete inaccurate/incomplete information ("right to be forgotten," subject to legal retention).
- Objection: Object to processing on reasonable grounds (e.g., direct marketing).
- Restriction: Limit processing in certain cases.
- Portability: Receive information in a structured format.
- Withdraw Consent: At any time, without affecting prior lawful processing.

Requests must be submitted in writing to the Information Officer. The FSP will respond within 30 business days.

## 10 Security Safeguards and Breach Management

The FSP implements reasonable technical and organisational measures, including:

- Physical security (locked filing cabinets, access-restricted offices).
- Electronic safeguards (firewalls, encryption, multi-factor authentication).
- Employee training on data handling and phishing awareness.
- Contracts with operators ensuring POPIA compliance.

In the event of a security compromise (e.g., breach), the FSP will:

- Assess the impact.
- Notify the Information Regulator and affected data subjects within 72 hours if high risk.
- Take remedial action and document the incident.

## 11 Retention and Destruction

Personal information is retained only as long as necessary for the purpose (e.g., 5 years post-contract for FAIS records) or as required by law (e.g., 7 years for tax). Upon expiry:

- De-identify where possible.

---

Authorised FSP 55173

e: [info@digiwealth.co.za](mailto:info@digiwealth.co.za) | [www.digiwealth.co.za](http://www.digiwealth.co.za)

a: 13 Belvedere Street, Durbanville, Cape Town, South Africa, 7551



+ (27) 82 759 2318 | t: + (27) 21 975 2535

- Securely destroy (shredding, overwriting) or return to the data subject.

## 12 Information Officer and Responsibilities

- Head Information Officer: [CEO], windall@digiwealth.co.za
- Responsible for overall compliance, registration with the Information Regulator, and policy implementation.

All employees must:

- Process information lawfully.
- Report breaches immediately.
- Undergo annual POPIA training.

Non-compliance may lead to disciplinary action.

## 13 Complaints and Dispute Resolution

Data subjects may lodge complaints with:

- The FSP's Information Officer (response within 30 days).
- The Information Regulator ([www.inforegulator.org.za](http://www.inforegulator.org.za)).
- The relevant ombudsman (e.g., FAIS Ombud for financial services).

## 14 Training and Awareness

Annual training is mandatory for all staff. New employees receive induction on this Policy.

Awareness campaigns promote a culture of privacy.

## 15 Review and Amendments

This Policy is reviewed annually or upon material changes to POPIA/FAIS. Amendments require approval by the Information Officer and Board. Data subjects will be notified of significant updates.

---

Authorised FSP 55173

e: [info@digiwealth.co.za](mailto:info@digiwealth.co.za) | [www.digiwealth.co.za](http://www.digiwealth.co.za)

a: 13 Belvedere Street, Durbanville, Cape Town, South Africa, 7551



+ (27) 82 759 2318 | t: + (27) 21 975 2535

## 16 Contact Details

For queries:

- Email: [compliance@adigiwealth.co.za.co.za](mailto:compliance@adigiwealth.co.za.co.za)
- Phone: + (27) 82 759 2318
- Address: 13 Belvedere Street, Durbanville, Cape Town, South Africa, 7551

By adopting this Policy, the FSP reaffirms its commitment to ethical data stewardship, fostering trust with clients and stakeholders.

---

Authorised FSP 55173

e: [info@digiwealth.co.za](mailto:info@digiwealth.co.za) | [www.digiwealth.co.za](http://www.digiwealth.co.za)

a: 13 Belvedere Street, Durbanville, Cape Town, South Africa, 7551



+ (27) 82 759 2318 | t: + (27) 21 975 2535