

PAIA Manual – Oaths.co.za™

Operated by Beantech (Pty) Ltd

Beantech (Pty) Ltd is registered and in good standing with the **Information Regulator (South Africa)** under the **Protection of Personal Information Act (POPIA)**, registration number **2025-006973**, and complies with the **Promotion of Access to Information Act (PAIA)** (Act 2 of 2000).

1. Company Details

Information Officer: Mr J.M. van der Westhuizen
Professional Accountant (SA) | Commissioner of Oaths (Ex Officio)

Email: compliance@oaths.co.za

Address: Regus Cradlestone Mall, Entrance 5, L2, 17 Hendrik Potgieter Road, Krugersdorp, Gauteng 1739, South Africa

2. PAIA Guide

The PAIA Guide explaining access rights and procedures is available from the **South African Human Rights Commission (SAHRC)**:

 <https://www.sahrc.org.za>

3. Records Automatically Available

The following records are publicly accessible on the Oaths.co.za™ website without a formal request:

- Company profile and service overview
 - Pricing and FAQs
 - “How it Works” overview
 - Terms and Conditions
 - Privacy Policy
 - Prohibited Use Policy
 - PAIA Manual
-

4. Records Available on Request

The following records may be accessed upon written request, subject to PAIA procedures and applicable laws:

- Certification session and verification logs
- Forensic blockchain audit trails
- User account and verification results
- Commissioner of Oaths enrolment records
- Compliance and internal policy documents
- Guardian consent confirmations (for minor users)
- AML / FICA risk and screening records

Requests must be submitted in writing (using Form C) to  compliance@oaths.co.za

together with proof of identity and any required fee. Requests will be processed per PAIA guidelines.

5. Purpose of Processing

Beantech (Pty) Ltd processes personal information to:

- Deliver certified digital documents to users
 - Verify identity through biometric and liveness checks
 - Conduct FICA, AML, and sanctions screening
 - Maintain secure, auditable blockchain certification records
 - Record and validate guardian consent for minors
 - Support compliance with POPIA, PAIA, and other laws
-

6. Categories of Data Subjects and Information

Data Subjects

- Adult users and subscribers
- **Minors (ages 16 – 17)** with Smart ID Cards
- **Guardians providing consent**
- Commissioners of Oaths
- Employees and service providers

Information Categories

- Identity and biometric data
 - Contact details (email, phone, address)
 - Uploaded documents (ID, licence, passport, proof of address)
 - Guardian consent information
 - Technical and usage metadata
 - Certification records and blockchain hashes
-

7. Recipients of Personal Information

Information is shared only where necessary and lawful with:

- Commissioners of Oaths (for certification purposes)
- Trusted third-party providers (for secure hosting, verification, and compliance checks)
- Regulators or law enforcement (FIC, DHA, NPA) when legally required

All third parties are **POPIA-compliant** and bound by written confidentiality agreements.

8. Security Measures and Infrastructure Location

General Safeguards

- Encryption at rest and in transit (AES-256)
- Role-based access control and multi-factor authentication
- Biometric identity checks and liveness detection
- Blockchain-secured audit trail and routine backups
- Continuous monitoring and security testing

Infrastructure Location and Data Sovereignty

All data, processing operations, and the Oaths.co.za™ application code are hosted on **Microsoft Azure South Africa (North and South regions)**.

No personal information is transferred outside South Africa.

The environment is managed under **ISO 27001** and **SOC 2** standards, ensuring compliance with **POPIA Section 72** (cross-border data transfer restrictions) and South African data sovereignty requirements.

Minor Data Ring-Fencing

- All data relating to minors (16 – 17) is **ring-fenced** in a dedicated encrypted ledger separate from adult data.
 - Managed via **Microsoft Azure Confidential Ledger** with AES-256 encryption and key rotation.
 - Access restricted to authorised compliance officers under dual-control procedures.
 - Every access event is recorded in an immutable blockchain audit trail.
 - Records are **cryptographically deleted** when consent is withdrawn or retention expires.
-

9. Access Procedure

To request access to records under PAIA:

1. Complete **Form C** (available from the SAHRC or Oaths.co.za™ website).
2. Email the form and proof of identity to  **compliance@oaths.co.za**.
3. The Information Officer will acknowledge receipt and respond within **30 days**.

Requests involving a minor's data must include verified guardian consent.

10. Fees and Processing Time

- A prescribed PAIA fee may apply before records are released.
 - Processing may take up to 30 working days, extendable under Section 26 of PAIA for large or complex requests.
-

11. Remedies and Complaints

If access is refused or delayed, you may:

- Lodge a written complaint with the **Information Regulator** ( inforeg@justice.gov.za,  www.inforegulator.org.za); or
 - Approach a competent South African court for review.
-

12. Revision History

Version	Date	Summary of Change
1.0	01 March 2025	Initial PAIA Manual issued
1.1	19 October 2025	Updated for POPIA minor provisions, encrypted ledger ring-fencing, and Microsoft Azure South Africa hosting

Approved by:

Mr J.M. van der Westhuizen

Information Officer – Beantech (Pty) Ltd / Oaths.co.za™

 Summary:

This PAIA Manual now:

- Includes **minors (16–17)** as data subjects under guardian consent
- Confirms full **data residency in Microsoft Azure South Africa**
- Documents encrypted ledger ring-fencing for children's information
- Satisfies the Information Regulator's requirements for POPIA and PAIA compliance