BEANTECH (PTY) LTD t/a OATHS.CO.ZA™

Privacy Policy

How Beantech collects, uses, shares, protects and retains your personal information

Operator	Beantech (Pty) Ltd, registration number 2010/008997/07
Platform	Oaths.co.za™
Version	3.0 – 14 October 2026
Replaces	Privacy Policy v2.0 (25 May 2026), Privacy Notice, and POPIA Privacy Policy v1.1 (19 October 2025), all of which are withdrawn
Information Officer	Mr J.M. van der Westhuizen

This policy explains what we do with your personal information. It is written to comply with the Protection of Personal Information Act 4 of 2013 ("POPIA"). It should be read with our **Terms and Conditions**, our **Prohibited Use Policy** and our **PAIA Manual**, and with any consent notice shown to you during registration or use.

1. Who we are

Beantech (Pty) Ltd (registration number 2010/008997/07), trading as **Oaths.co.za™**, is the responsible party for the personal information described in this policy. In this policy "we", "us" and "our" mean Beantech.

Oaths.co.za™ is a digital service through which a Commissioner of Oaths, acting **ex officio** under the Justices of the Peace and Commissioners of Oaths Act 16 of 1963, certifies copies of supported South African documents as true copies of the originals presented through the platform.

What certification means, and what it does not. A certification confirms only that the copy corresponds with the original document presented through the platform process. It is not a confirmation that the original document is itself authentic, valid or current, and it is not a sworn statement, affidavit or affirmation.

2. Information we collect

Category	What it includes
Identity information	Full names and surname; South African identity number or passport number; identity document type; date of birth.
Biometric information	A facial image or scan captured during identity verification, and the liveness check performed on it. **This is special personal information – see section 5.**
Contact information	E-mail address, mobile number and physical or postal address.
Document information	The documents you submit for certification, together with the images or scans captured, and information about them such as file type, size and the time of submission.
Verification and screening results	The outcome of identity verification, liveness confirmation and compliance screening. **Screening results are special personal information – see section 5.**
Consent records	Which version of which consent you accepted, when, and how that acceptance was authenticated.

Certification records	The certification act itself, the document certified, the Commissioner of Oaths who certified it, and the verification reference issued.
Technical information	Device and browser details, IP address, operating system, session and access logs.
Payment information	Confirmation that a transaction has been paid for. **Card details are handled by our payment provider and are not stored by Beantech.**
Guardian information	Where the user is aged 16 or 17: the parent or legal guardian's name, identity number, contact details, relationship to the minor, and the record of their consent.
Correspondence	Support requests, complaints and related communications.

3. How we collect it

- **Directly from you** when you register, submit a document, complete identity verification, make a payment or contact us.
- **Automatically** through platform logs, security tooling, cookies and session monitoring.
- **From a parent or legal guardian** where the user is aged 16 or 17.
- **From our identity verification partner**, which returns the result of the identity, liveness and screening checks described in section 5.
- **From our payment provider**, which confirms whether a transaction has been paid for.

4. Why we process it

We process personal information in order to:

- create and administer your account;
- satisfy the Commissioner of Oaths that you are the person you say you are, before any document is certified in your name;
- carry out the certification itself and issue the certified document and its verification reference;
- allow a certified document to be checked afterwards through our verification service;
- keep the records of the certification act that we are required to keep;
- record and manage guardian consent where the user is a minor;
- take payment and confirm it;
- protect the platform against impersonation, fraud and misuse;
- respond to your queries, complaints and requests; and
- comply with our legal obligations, and establish, exercise or defend legal claims.

We do not sell your personal information. We do not use it for behavioural advertising, and we do not make decisions about you by automated means alone.

5. Special personal information – biometrics and screening

Two of the checks we run need your explicit consent, and we will ask for it separately. Biometric information is special personal information under section 26 of POPIA. So is information about alleged criminal behaviour, which compliance screening can reveal. We may process either only on one of the grounds in section 27 – in our case, **your explicit consent under section 27(1)(a)**. A general agreement to identity verification is not enough and we do not treat it as

enough.

Check	What it involves	Why
Identity verification	Your identity document is checked against the records of the Department of Home Affairs through our verification partner.	To confirm you are the person named in the document.
Liveness confirmation	A biometric check confirming that you are a real, living person and that you are the person shown in the identity document.	To prevent impersonation and the use of stolen or fabricated identities.
Compliance screening	Your name is screened against anti-money-laundering, politically exposed person, prominent influential person and sanctions watchlists.	So that we know who we are certifying for.

- The liveness check establishes only that you are a real, living person and that you are the person shown in the identity document. It is used for nothing else.
- A screening result does not by itself mean anything is wrong. If a result affects our ability to act for you, we will tell you.
- **You may refuse.** If you do, we cannot verify your identity to the standard this service requires and we will not be able to certify your documents.

6. Our lawful grounds

Processing	Ground under POPIA
Account administration, certification, payment and support	Performance of our contract with you, and steps taken at your request before entering into it – section 11(1)(b).
Biometric liveness confirmation and compliance screening	**Your explicit consent – section 27(1)(a)**, as these involve special personal information.
Transfer of your information to our verification partner outside South Africa	**Your consent – section 72(1)(b)**. See section 8.
Keeping records of the certification act and of consent	Compliance with a legal obligation, and our legitimate interests in being able to evidence what we certified and on what authority – sections 11(1)(c) and 11(1)(f).
Fraud prevention and platform security	Our legitimate interests and those of our users – section 11(1)(f).
Processing a minor's personal information	The prior consent of a competent person, being the parent or legal guardian – section 35(1)(a).

Where we rely on your consent you may withdraw it at any time, free of charge, by contacting our Information Officer. Withdrawal does not affect the lawfulness of anything done before it, and it does not oblige us to destroy records we are required to keep – see section 10.

7. Who we share it with

Recipient	What they receive, and why
The Commissioner of Oaths	The information needed to perform the certification. During the current phase of the service the Commissioner of Oaths is Beantech's own director, so this is not a disclosure outside Beantech.
Our identity verification partner	Identity document details and the facial image, for the checks in section 5. This partner acts as our operator and may process only on our instruction. **It processes outside South Africa – see section 8.**
Our payment provider	The information needed to take and confirm payment. Beantech does not store card details.
Our cloud provider	Microsoft, as the operator of the infrastructure on which the platform runs. Microsoft processes on our instruction and does not use your information for its own purposes.
Anyone you give a certified document to	A certified document carries a verification reference and QR code so that the recipient can confirm it is genuine. **What they see is limited to the certification details** – that a certification took place, when, by whom, and its current status. The underlying document and your identity information are not exposed through that check.
Professional advisers and auditors	Where necessary for legal advice, audit, assurance, insurance or dispute matters, under confidentiality obligations.
Regulators, courts and law enforcement	Where disclosure is required or permitted by law.

Where a third party processes personal information on our behalf, we require it by written agreement to process only on our instruction, to keep the information confidential, and to maintain appropriate security safeguards.

8. Where your information is processed

The Oaths.co.za™ platform runs on **Microsoft Azure in the South Africa North region**. Your account, the documents you submit, the certification records and the audit trail are stored there.

One part of the service is processed outside South Africa, and we want you to know exactly which. Identity verification, biometric liveness confirmation and compliance screening are performed by **Didit**, our verification partner, which processes in the **European Union** under the General Data Protection Regulation. The information sent to Didit is your identity document details and your facial image. Nothing else is sent, and your certified documents are not sent. Section 72 of POPIA allows this transfer with your consent, and we ask for that consent expressly before the check is run. You may refuse, in which case we cannot verify your identity and cannot certify your documents.

Didit acts as our operator under a written data processing agreement. We configure a finite retention period in Didit rather than leaving an open-ended default in place, and the verification session is deleted once the result has been received.

9. How we protect your information

We apply the technical and organisational measures below. We describe them plainly, and we describe only what is actually in place.

- **Encryption** of personal information in transit and at rest.
- **Access control** through Microsoft Entra ID, with multi-factor authentication for administrative access and secrets held in a managed key vault.
- **A tamper-evident ledger.** Key records are written to database ledger tables that cryptographically chain each change to the one before it, so that any alteration or deletion can be detected. Cryptographic digests of the ledger are stored separately.
- **Write-once storage.** Certified documents and the associated records are written to immutable storage under a retention lock. Once written they cannot be altered or deleted by anyone, including our own administrators, until the retention period expires.
- **Separation of building from operating.** The people who build the platform do not have access to live personal information, and the person who operates the service cannot change the code that enforces these controls without review and approval by a second person.
- **Logging and monitoring** of system access and administrative activity.

The infrastructure beneath our application is operated by Microsoft and is independently certified to ISO/IEC 27001, 27017, 27018 and 27701, and subject to an annual SOC 2 Type 2 examination. Those certifications cover Microsoft's platform. **They are not certifications of Beantech, and we do not present them as such.** Beantech does not hold ISO 27001 or ISO 27701 certification.

No method of transmission or storage is completely secure, and we cannot guarantee absolute security. If a security compromise affects your personal information we will notify you and the Information Regulator as section 22 of POPIA requires.

10. How long we keep it, and the limits on deletion

Record	Retention period
Certification records – the certification act, the document certified and the verification reference	**7 years**
Consent records and the authentication trail	**7 years** from expiry of the consent
Identity, biometric and screening records held by our verification partner	The verification session is **deleted once the result has been received**
Security and access logs	**12 months** available online, then archived for 7 years
Support correspondence	For as long as needed to deal with the matter and any related dispute
Company and accounting records	As required by the Companies Act 71 of 2008 and the Tax Administration Act 28 of 2011

Please read this part carefully. Certified documents and the records of certification are written to storage that cannot be altered or deleted until the retention period above expires. This is deliberate – it is what makes a certified document trustworthy afterwards. It also means that **if you ask us to delete a certification record before that period expires, we cannot do it**, and we will tell you so rather than promise otherwise. Section 14 of POPIA permits retention where a law requires or authorises it, or where retention is required for a lawful purpose related to our functions.

Information that is not subject to that lock – for example your contact details and marketing preferences – can be corrected or deleted on request in the ordinary way.

11. Users aged 16 and 17

The platform may be used by a person aged 16 or 17 who holds a valid Smart ID Card, but only where a parent or legal guardian has given verifiable consent before registration. Section 35 of POPIA requires the prior consent of a competent person before a child's personal information may be processed.

- We record the guardian's identity, their relationship to the minor, and the consent itself.
- A guardian may withdraw consent at any time. If consent is withdrawn we will stop further processing and restrict or close the account, subject to the retention limits in section 10.
- A guardian may exercise the rights in section 12 on the minor's behalf.
- **Additional safeguards apply to minors' information**, including restricted access and separate handling.

12. Your rights

- **Access** – ask what personal information we hold about you, and ask for a copy. Our PAIA Manual explains how.
- **Correction** – ask us to correct or complete information that is inaccurate, irrelevant, excessive, out of date, misleading or unlawfully obtained.
- **Deletion** – ask us to delete or destroy information, subject to section 10.
- **Objection** – object, on reasonable grounds, to processing we base on legitimate interests.
- **Withdrawal of consent** – at any time, free of charge, where we rely on consent.
- **Complaint** – to our Information Officer, or to the Information Regulator.

We may ask you to prove your identity, or your authority to act for someone else, before we act on a request. We will respond as soon as reasonably possible.

13. Cookies

We use cookies and similar technologies for security, session management, platform functionality and performance monitoring. We do not use them to build advertising profiles. You can manage cookies through your browser, though some platform functions may not work properly if you block them.

14. Contact us, and how to complain

Information Officer	Mr J.M. van der Westhuizen
E-mail	compliance@oaths.co.za
Address	Regus Cradlestone Mall, Entrance 5, L2, 17 Hendrik Potgieter Road, Krugersdorp, Gauteng, 1739, South Africa
Information Regulator (South Africa)	Woodmead North Office Park, 54 Maxwell Drive, Woodmead, Johannesburg, 2191
Complaints	Form 05 (Regulation 10) – see inforegulator.org.za

General enquiries	enquiries@inforegulator.org.za
Website	inforegulator.org.za | Tel 010 023 5200 | Toll free 0800 017 160

You may complain to the Information Regulator at any time. You do not have to complain to us first, although we would like the chance to put things right.

15. Changes to this policy

We review this policy at least annually and whenever the service changes materially. The current version is always the one published at oaths.co.za. Where a change materially affects how we process your personal information we will bring it to your attention.

16. Revision history

Version	Date	Summary of change
1.0	20 May 2025	Initial issue.
1.1	19 October 2025	Minor and guardian consent framework added.
2.0	25 May 2026	Privacy wording harmonised. **Withdrawn.**
3.0	14 October 2026	Consolidated into a single privacy policy, replacing the Privacy Policy, the Privacy Notice and the POPIA Privacy Policy, which are withdrawn. Cross-border processing by the verification partner disclosed under section 72. Biometric and screening processing identified as special personal information requiring explicit consent under section 27(1)(a). Security measures restated to describe only measures actually in place. Retention periods aligned to the record-keeping schedule, and the effect of the retention lock on deletion requests disclosed.