

PAIA Manual

My Global Vault (Pty) Ltd — Manual prepared in terms of section 51 of the Promotion of Access to Information Act 2 of 2000 (PAIA) and the Protection of Personal Information Act 4 of 2013 (POPIA)

Date of compilation: 8 October 2026

1. Introduction and purpose

This Manual is published by My Global Vault (Pty) Ltd, a private body, in accordance with section 51 of PAIA and the Information Regulator's template for private bodies. It explains how to request access to records held by the company and how the company processes personal information under POPIA.

This Manual is available on our website at <https://myglobalvault.com/paia-manual>, as a downloadable PDF, at our registered address for public inspection during business hours, and on request to the Information Officer free of charge.

2. Company details

Name of private body	My Global Vault (Pty) Ltd
Registration number	2026/641330/07
Date of incorporation	12 August 2026
Registered, postal and legal address	29 Patrick Road, Charlo, Port Elizabeth, 6070, South Africa
Website	https://myglobalvault.com
Email (PAIA / POPIA)	info@myglobalvault.com
General support	support@myglobalvault.com
VAT status	Not VAT registered

3. Information Officer

Information Officer	Jacques Allistar Nel
Email	info@myglobalvault.com
Postal / physical address	29 Patrick Road, Charlo, Port Elizabeth, 6070
Registration with Information Regulator	Completed through BizPortal on 8 October 2026
Deputy Information Officer	None appointed

4. Guide on how to use PAIA (section 10)

The Information Regulator has published a Guide in each official language explaining how to exercise any right under PAIA and POPIA. It is available on the Information Regulator's website and from the Regulator at the details below. A copy may also be inspected at our registered address or requested from our Information Officer.

Information Regulator (South Africa): Woodmead North Office Park, 54 Maxwell Drive, Woodmead, Johannesburg, 2191 · Telephone: 010 023 5200 · Toll-free: 0800 017 160 · General enquiries: enquiries@inforegulator.org.za · PAIA complaints: PAIAComplaints@inforegulator.org.za · POPIA complaints: POPIAComplaints@inforegulator.org.za · Website: <https://inforegulator.org.za>

5. Records automatically available (section 52)

The following records are available without a formal PAIA request, free of charge, on our website: Privacy Policy, Terms of Service, Disclaimer, this PAIA Manual, product and pricing information, and the account deletion procedure.

6. Records held in accordance with other legislation

Where applicable, the company holds records in terms of the following legislation (this list is not exhaustive):

- Companies Act 71 of 2008
- Income Tax Act 58 of 1962
- Tax Administration Act 28 of 2011
- Basic Conditions of Employment Act 75 of 1997 and Labour Relations Act 66 of 1995 (if and when employees are appointed)
- Consumer Protection Act 68 of 2008
- Electronic Communications and Transactions Act 25 of 2002
- Protection of Personal Information Act 4 of 2013
- Promotion of Access to Information Act 2 of 2000

7. Subjects and categories of records held

- Company records: incorporation documents, share register, directors' records, statutory returns and resolutions.
- Financial and tax records: accounting records, bank statements, tax records and app-store payout statements.
- Customer account records: name, email address, authentication records, account settings and Free / Premium entitlement status.
- Vault content: documents, notes and attachments uploaded by customers, stored encrypted in private storage. These are held on behalf of the customer and are not accessible to staff in the ordinary course.
- Trusted Recipient records: names and contact details of recipients nominated by customers and the documents each customer has authorised for release.
- Claim records: claims opened by recipients, submitted claim evidence, decisions, and an append-only audit trail of claim events.
- Billing records: app-store purchase references and verification results. No card numbers are received or stored.
- Operational and security records: sign-in events, Pulse check-in state, security logs, account deletion requests and first-party usage counters.
- Correspondence: support and privacy correspondence received by email.
- Supplier and service-provider records: agreements and correspondence with hosting, email and app-store providers.

8. Procedure for requesting access

- Complete the prescribed request form (PAIA Form 2 — Request for Access to Record) available from the Information Regulator's website or from our Information Officer.
- Send the completed form to the Information Officer at info@myglobalvault.com or deliver it to our registered address.

- Provide proof of identity. If you act on behalf of another person, provide proof of your authority to do so.
- Identify the record(s) requested with enough detail, state the form of access required, and state the right you wish to exercise or protect and why the record is required for that purpose.
- We will decide on the request within 30 days of receipt. This period may be extended once by a further 30 days where PAIA permits, and you will be notified of any extension.
- Access may be refused only on the grounds set out in Chapter 4 of Part 3 of PAIA, including protection of the privacy of third parties, commercial information, confidential information and the safety of individuals and property. Customer vault content belonging to another person will not be disclosed except where the law requires it.
- There is no internal appeal against a decision of a private body. If you are dissatisfied, you may lodge a complaint with the Information Regulator using PAIA Form 5, submitted through the Information Regulator's eServices Portal (via <https://info regulator.org.za>) or by email to PAIAComplaints@info regulator.org.za, or apply to a court within 180 days of the decision.

9. Prescribed fees

Fees are payable as prescribed in the Regulations relating to the Promotion of Access to Information, 2021 (as amended), Annexure B (fees for private bodies). A request fee is payable by requesters other than personal requesters seeking their own personal information. An access fee for search, preparation and reproduction may be payable, and a deposit may be required where the search exceeds the time set out in the Regulations. We will notify you of any fee payable (PAIA Form 3) before processing continues. The current amounts are those published by the Information Regulator.

10. Processing of personal information (POPIA)

10.1 Purposes of processing

- To provide, secure and support the My Global Vault service.
- To verify customer identity during registration, sign-in and sensitive actions (email verification codes).
- To release documents to a nominated Trusted Recipient when the customer's chosen conditions are met and a claim is verified.
- To verify app-store purchases and grant Premium entitlements.
- To understand, in aggregate, where people get stuck while registering (first-party counters only).
- To comply with legal, tax and regulatory obligations.

10.2 Categories of data subjects and information

- Customers: name, email address, authentication records, vault content, settings, entitlement status, sign-in and check-in events.
- Trusted Recipients: name and contact details provided by the customer; identity and claim documentation they submit.
- Deceased or incapacitated customers: information contained in death certificates, medical or legal certificates of incapacity, or executor/court authority submitted with a claim.
- Website and app visitors: anonymous visit reference, platform and stage reached; no IP address, fingerprint or advertising identifiers for statistics.
- Suppliers and correspondents: contact details and correspondence.

10.3 Special personal information

Customers may choose to upload documents that contain special personal information (for example health information) or information of children. Such content is stored encrypted, is processed only to provide the service the customer requested, and is not inspected or used for any other purpose. Claim evidence may contain health or death information and is used only to assess that claim.

10.4 Recipients of personal information

- Trusted Recipients nominated by the customer — only the specific documents the customer authorised, after a verified claim.
- Operators (service providers) acting on our instructions: managed cloud hosting, database, file storage and authentication; managed email delivery; global website edge delivery; Google Play and Apple App Store for purchase verification.
- Authorities, where required by law.

10.5 Cross-border transfers

The service's database, private file storage and authentication are hosted on managed cloud infrastructure in the European Union (Ireland, AWS eu-west-1). The website is delivered through a global edge network. Email delivery and app-store providers may process information in other countries. Transfers take place under safeguards required by section 72 of POPIA, including the operator's contractual obligations and the data-protection laws applicable in the European Union.

10.6 Security measures

- Encryption in transit (TLS) and encryption at rest (AES-256).
- Private, access-controlled file storage; files are not publicly reachable.
- Per-user row-level security on the database and role-based administrative access.
- Email verification codes for registration and sensitive actions; re-authentication before account deletion.
- Append-only audit trail of claim events.
- Scheduled removal of abandoned uploads and of claim evidence after its retention period.

10.7 Retention (summary)

- Vault content and account data: kept while the account is active. In-app account deletion removes stored files and then the account immediately. Copies in the hosting provider's routine backups expire on that provider's backup cycle.
- Claim evidence: deleted automatically 90 days after a rejected, cancelled or closed claim and 12 months after a completed claim; a minimal non-content record remains.
- Death determination: after a completed claim, a 30-day deletion countdown runs before vault content is erased.
- Billing and tax records: kept for the period required by tax and company law.
- Other records (audit trail, usage counters, support correspondence, deletion requests): retained for accountability and legal purposes. Specific periods are under legal review and will be published once confirmed.

11. Objection, correction and deletion (POPIA)

You may object to processing using POPIA Form 1 (Objection to the Processing of Personal Information) and request correction or deletion using POPIA Form 2 (Request for Correction or Deletion of Personal Information or Destruction or Deletion of Record). The forms are available from the Information Regulator's website or from our Information Officer. Send them to info@myglobalvault.com. Customers can also delete their account directly in the app or at <https://myglobalvault.com/delete-account>. Complaints may be lodged with the Information Regulator through its eServices Portal (via <https://inforegulator.org.za>) or by email to POPIAComplaints@inforegulator.org.za.

12. Availability and updating

This Manual will be reviewed and updated whenever there is a material change. The latest version is always available at <https://myglobalvault.com/paia-manual>.