# Operator Agreement and Data Processing Addendum

**Draft — pending legal review.** This draft has not been reviewed by a lawyer and is not an offer. Do not sign it until it has been reviewed and this notice is removed.

Under section 21 of the Protection of Personal Information Act 4 of 2013 ("POPIA").

Version: draft 0.1, 28 October 2026. Source: docs/legal/operator-agreement.md in the Thisisit repository.

## 1. Parties

1.1 **The Responsible Party:** the client named in the order form or sign-up ("the Client"), which decides why and how its personal information is processed.

1.2 **The Operator:** Thisisit (Pty) Ltd, registration number [registration TBC], of Cape Town, South Africa ("Thisisit"). Information officer: [TBC]. Contact: [contact email TBC].

## 2. Definitions

2.1 Words defined in POPIA have the same meaning here, including "personal information", "processing", "responsible party", "operator", "data subject" and "Regulator".

2.2 **Client Data** means everything the Client or its users bring into Thisisit: uploaded files, documents and email pulled from connected systems, and the records, reports and answers made from them.

2.3 **Service** means the Thisisit application and the hosting, support and backups Thisisit provides with it.

2.4 **Sub-processor** means a third party Thisisit engages to process Client Data on its behalf (clause 7).

## 3. Scope and instructions

3.1 Thisisit processes Client Data only to provide the Service, and only on the Client's documented instructions. The Client's instructions are this agreement, the Client's configuration of the Service (which sources to connect, which folders, labels or mailboxes to read, which AI provider to use) and any further written instructions agreed by both parties.

3.2 The Service reads, sorts and searches Client Data: it extracts typed records with the quote each value came from, answers questions, writes reports and raises alerts. Annex A describes the processing.

3.3 Thisisit does not use Client Data for any other purpose, does not sell it, and does not use it to train AI models.

3.4 If Thisisit believes an instruction breaks POPIA, it will tell the Client and may suspend that processing until the Client confirms or changes the instruction.

## 4. Confidentiality (s20)

4.1 Thisisit treats Client Data as confidential and does not disclose it unless the law requires it. If it is legally required to disclose Client Data, Thisisit will tell the Client first where the law allows.

4.2 Everyone at Thisisit who can reach Client Data is bound by confidentiality and may reach it only to

provide or support the Service.

## 5. Security safeguards (s19 and s21(1))

5.1 Thisisit keeps appropriate, reasonable technical and organisational measures to protect the integrity and confidentiality of Client Data and to prevent its loss, damage, unauthorised destruction and unlawful access. The measures in place at the date of this draft are listed in Annex B and on the public page at /security. Measures under "Coming" there are not yet in place and are not promised by this agreement.

5.2 Thisisit will review its measures regularly and keep them up to date with generally accepted information security practice.

## 6. Notice of security compromises (s21(2) and s22)

6.1 Thisisit will notify the Client **immediately**, and in any case within [48 hours — TBC by lawyer] of becoming aware, where there are reasonable grounds to believe that Client Data has been accessed or acquired by an unauthorised person.

6.2 The notice will include, as far as known at the time: what happened and when; which data and which data subjects are or may be affected; what Thisisit has done and will do; and a contact person. Thisisit will add details as it learns them.

6.3 The Client, as responsible party, decides on and gives the notices to the Information Regulator and to data subjects required by section 22. Thisisit will give the Client the information and help it reasonably needs to do so, and will not notify the Regulator or data subjects on the Client's behalf unless the Client asks it to or the law requires it.

## 7. Sub-processors

7.1 The Client authorises Thisisit to use the sub-processors in the table below. Thisisit binds each one by written contract to protections at least as strong as this agreement, and remains responsible to the Client for their processing.

| Sub-processor | Purpose | Location | Status |
|---|---|---|---|
| OpenAI, L.L.C. | AI extraction, answers and search embeddings, through its API | United States | In use when chosen |
| Anthropic, PBC | AI extraction and answers (Claude), through its API | United States | In use when chosen |
| Amazon Web Services, Inc. (AWS) | Hosting, database, file storage and backups; email through Amazon SES | South Africa (af-south-1, Cape Town) | Planned |
| Cloudflare, Inc. | DNS, TLS and traffic protection in front of the app | Global network | Planned |
| Postmark (ActiveCampaign, LLC) | Transactional email (invites, password resets), only if chosen instead of Amazon SES | United States | Optional |
| Functional Software, Inc. (Sentry) | Server error reports, with request bodies, cookies and headers removed, only if switched on | United States | Optional |

7.2 "In use when chosen": each installation uses one AI provider, set in its configuration. With Anthropic, search embeddings still use OpenAI when an OpenAI key is configured. "Planned": not in use at the date of this draft.

7.3 Systems the Client connects (for example Google Workspace, Microsoft 365 or Xero) are the Client's own service providers, not Thisisit's sub-processors. The Client chooses what Thisisit may read from them, through read-only access the Client grants and can revoke.

7.4 Thisisit will give the Client at least 30 days' written notice before adding or replacing a sub-processor. The Client may object on reasonable data-protection grounds; if the parties cannot resolve the objection, the Client may end the affected part of the Service and receive a pro rata refund of prepaid fees.

## 8. Transfers outside South Africa (s72)

8.1 **AI inference happens outside South Africa.** When the Service sorts a document or answers a question, the relevant text is sent to the chosen AI provider (OpenAI or Anthropic), which processes it in the United States. Only Client Data at rest (the database, files and backups) can be kept in South Africa, once hosting in AWS af-south-1 is live.

8.2 Thisisit relies on section 72(1)(a): each AI provider is bound by a written agreement with Thisisit (the provider's data processing addendum and commercial API terms) that provides an adequate level of protection, substantially similar to the conditions for lawful processing in POPIA, including rules on onward transfer. [Lawyer to confirm that each provider's current terms meet s72(1)(a), and whether the Client should also rely on s72(1)(b) consent or s72(1)(c)/(d) contract necessity for particular data subjects.]

8.3 Under the providers' API terms as Thisisit understands them, API inputs and outputs are not used to train their models by default, and are kept only for a limited period for abuse and safety monitoring. [Lawyer to check the current terms, retention periods, and whether zero-data-retention can be arranged.]

8.4 The Client can reduce what leaves South Africa: scans can be read with local OCR (Tesseract) so page images are not sent to the AI provider, and the Client chooses which sources and folders are connected.

8.5 Thisisit will not transfer Client Data to any other country or recipient outside South Africa without the Client's prior written agreement.

## 9. Data subjects' rights and the Client's obligations

9.1 Thisisit will, taking into account the nature of the processing, help the Client respond to data subjects' requests for access, correction or deletion (sections 23 to 25), and will pass on to the Client any such request it receives directly.

9.2 The Client is responsible for having a lawful basis for the personal information it brings into the Service and for telling data subjects what it is required to tell them (section 18).

9.3 The Client will not bring special personal information (section 26) or personal information of children (section 34) into the Service unless the parties have first agreed in writing how it will be handled. [Lawyer to confirm.]

## 10. Return and deletion on termination

10.1 When the Service ends, the Client may ask, within 30 days, for a copy of its Client Data. Thisisit will provide the approved records as CSV files and the original files as an archive. (A workspace owner can also download all of this at any time, as one ZIP file of records, original files and the audit log, and can delete the workspace in the app.)

10.2 After that copy has been provided, or after the 30 days, Thisisit will delete Client Data from the live Service within [30 days — TBC], and will confirm the deletion in writing. Copies in backups are deleted as the backups expire, within 14 days, and are not restored in the meantime except to recover the Service.

10.3 Disconnecting a source deletes the stored access tokens at once and, for Google and Xero, also revokes access at the provider. Microsoft does not offer token revocation, so for Microsoft 365 the Client should also remove the Thisisit app in its Microsoft Entra admin centre. Documents already pulled stay in the workspace until deleted under this clause.

10.4 Thisisit may keep Client Data longer only where the law requires it, and then only for that purpose, protected under this agreement.

## 11. Audits and information

11.1 Thisisit will make available to the Client the information reasonably needed to show compliance with this agreement, and will answer reasonable written security questionnaires once a year, or after a security

compromise.

11.2 Thisisit holds no security certifications at the date of this draft and does not claim any.

## 12. Liability, term and law

12.1 Liability is as set out in the main terms of service between the parties. [Lawyer to set caps and any carve-outs for breaches of this agreement.]

12.2 This agreement lasts as long as Thisisit processes Client Data for the Client, and clauses 4, 6 and 10 survive its end.

12.3 This agreement is governed by the law of the Republic of South Africa. If it conflicts with the main terms on the processing of personal information, this agreement wins.

## Annex A: Description of processing

- **Subject matter:** providing the Service to the Client.
- **Duration:** the term of the Service, plus the period in clause 10.
- **Nature and purpose:** storing, reading (including OCR), classifying, extracting records with quotes, searching, answering questions, reporting and alerting on Client Data, as configured by the Client.
- **Categories of data subjects:** people named in the Client's documents and email, such as the Client's staff, customers, suppliers, counterparties and contacts; and the Client's users of the Service.
- **Categories of personal information:** whatever the Client's documents and email contain, typically names, contact details, job titles, company and financial details in invoices, contracts and correspondence; for users, name, email address, password hash, sign-in sessions and optional two-step settings.
- **Special personal information:** none, unless agreed under clause 9.3.

## Annex B: Security measures at the date of this draft

Each measure is in the application's code; the public page at /security names the control behind each one.

- **Read-only access to connected systems:** only read-only OAuth scopes are requested, and connectors make only HTTP GET requests, only to each provider's API hosts.
- **Encryption of secrets at rest:** connector tokens and two-step secrets are encrypted with Fernet (AES-128-CBC with an HMAC-SHA256 tag), with a separate key for each purpose derived from the app's secret.
- **Workspace isolation:** every document, record and source belongs to one workspace, every query is scoped to it, and another workspace's ids return "not found".
- **Accounts:** scrypt password hashes; revocable server-side sessions in HttpOnly cookies; sign-in locked for 15 minutes after repeated wrong passwords; single-use, hashed, 30-minute password-reset links; optional two-step sign-in (TOTP) with hashed recovery codes.
- **Roles:** only workspace owners can invite people, change roles, and connect or disconnect sources. Removing a person ends all their sessions.
- **Quote verification:** every extracted value carries the quote it came from, and code checks the quote is really in the document; values that fail go to a person for review.
- **Web protections:** a strict content security policy, clickjacking and MIME-sniffing protection, HTTPS-only cookies and HSTS in production, cross-site request checks, upload size limits, and blocking of internal addresses for website sources.
- **Backups:** a backup script takes a database dump and an archive of the files in one file encrypted with AES-256, keeping 14 days, with a copy in a second location. It runs on the schedule set at deployment, and a restore check restores the newest backup into a scratch database and compares it with the original.
- **AI call log:** every AI call is logged with its purpose, provider, model, token counts and any error.

Document content is not stored in the log.