Data Processing Agreement

In terms of the Protection of Personal Information Act 4 of 2013 (POPIA) Governing law: Republic of South Africa **Date of agreement:** `[DATE]`

Parties

Responsible Party (Controller) `[CUSTOMER LEGAL NAME]` Registration number: `[COMPANY REGISTRATION NUMBER]` Physical address: `[CUSTOMER PHYSICAL ADDRESS]` Email: `[CUSTOMER INFORMATION OFFICER EMAIL]` Information Officer: `[CUSTOMER INFORMATION OFFICER NAME]`

Operator (Processor) Ruan van der Westhuizen trading as Casepath `[NOTE: Update to "Casepath (Pty) Ltd" once entity is formalised]` Email: ruanvanderwesthuizen96@gmail.com `[NOTE: Casepath should designate a formal Information Officer once the entity is registered. Until then, Ruan acts in that capacity.]`

Background

The Responsible Party uses the Casepath platform under the Master Service Agreement dated `[MSA DATE]` (the "MSA"). In doing so, the Responsible Party processes personal information about data subjects (insureds, claimants, witnesses, investigators, and others) using Casepath's infrastructure. This agreement records the terms on which Casepath, as Operator, processes that personal information on behalf of the Responsible Party.

1. Roles

- The **Responsible Party** determines the purpose and means of processing personal information — it decides which cases to open, which data to record, and how long to keep it.
- **Casepath (Operator)** processes personal information only as a service provider, following the Responsible Party's documented instructions, in accordance with this agreement and POPIA.

2. Categories of Personal Information Processed

Casepath may process the following categories of personal information on behalf of the Responsible Party:

- Identity information: names, ID numbers, contact details of insureds, claimants, witnesses, and investigators
- Case information: claim descriptions, investigation notes, status records, and related documents
- Voice recordings (see clause 6 — these are stored on the Responsible Party's own infrastructure)
- Audit trail data: user actions and timestamps within the platform
- `[NOTE: Add any additional categories specific to the customer's case types, e.g. "medical information" if the customer handles personal injury claims. Certain special categories under POPIA section 26 require explicit consent and heightened controls.]`

---

3. Purpose of Processing

Casepath processes personal information solely for the purpose of providing the case management workflow described in the MSA. Casepath will not:

- Use personal information for any purpose other than delivering the service
- Sell, share, or disclose personal information to any third party except as listed in clause 6
- Process personal information in a way that is incompatible with the Responsible Party's instructions

---

4. Instructions

Casepath processes personal information only on the documented instructions of the Responsible Party (including as set out in this agreement and the MSA). If Casepath considers that an instruction would breach POPIA or any other law, it will notify the Responsible Party in writing before acting.

---

5. Security Measures

Casepath implements the following technical and organisational measures to protect personal information:

- **Encryption in transit:** all data transmitted between users and the platform is encrypted via TLS (HTTPS)
- **Encrypted backups:** daily automated backups, encrypted at rest
- **Access controls:** role-based access (admin, investigator, viewer); users may only access data relevant to their role
- **Audit logging:** all user actions within the platform are logged with timestamps

- **Password security:** user accounts require password authentication; `[NOTE: Ruan to confirm whether MFA is available or on the roadmap — if not, note it as a gap here]`
- **Physical security:** the platform is hosted on a dedicated VPS provided by Hostinger, located in South Africa `[NOTE: Confirm exact data centre location with Hostinger — ideally Johannesburg. This is material to the cross-border transfer position in clause 8. Do not send this DPA until confirmed.]`

---

6. Sub-processors

Casepath currently uses the following sub-processors:

Sub-processor	Purpose	Location
Hostinger	VPS hosting (application + database)	South Africa `[NOTE: Confirm]`
`[CUSTOMER'S OWN DROPBOX ACCOUNT]`	Voice note storage	Controlled by Responsible Party

Note on Dropbox: Voice note audio files are stored in the Responsible Party's own Dropbox account. The Responsible Party is the Dropbox account holder and is responsible for Dropbox's own data processing terms as they relate to those files. Casepath does not have access to the audio files themselves — only to metadata (file name, timestamp, link) recorded in the case notes.

Casepath will notify the Responsible Party at least **30 days in advance** before adding any new sub-processor that will process personal information. The Responsible Party may object in writing within that period; if it does, the parties will seek a resolution in good faith.

---

7. Personal Information Breach Notification

If Casepath becomes aware of a personal information breach (as defined in POPIA section 1) affecting the Responsible Party's data, Casepath will:

- Notify the Responsible Party in writing within **72 hours** of becoming aware of the breach
- Include in the notification: the nature of the breach, the categories and approximate number of data subjects affected, likely consequences, and measures taken or proposed

The Responsible Party is responsible for notifying the Information Regulator and affected data subjects, as required by POPIA section 22, using the information Casepath provides.

---

8. Cross-border Transfers

Personal information processed under this agreement is stored on Casepath's VPS, which is physically located in South Africa `[NOTE: Confirm with Hostinger]`. No personal information is routinely transferred outside of South Africa by Casepath.

If Casepath needs to transfer personal information outside South Africa (for example, if it engages a sub-processor outside SA), it will:

- Obtain the Responsible Party's prior written consent
- Ensure that the transfer complies with POPIA section 72 (adequate protection in the receiving country, or appropriate safeguards)

---

9. Data Subject Rights

Where a data subject exercises rights under POPIA (access, correction, deletion, objection), the Responsible Party will handle those requests as the Responsible Party. Casepath will provide reasonable assistance, including:

- Retrieving specific records on request
- Correcting data if instructed
- Permanently deleting individual records if instructed

---

10. Audit Rights

The Responsible Party may, on **14 days' written notice** and no more than once per calendar year, request that Casepath demonstrate compliance with this agreement. Casepath will respond within a reasonable time by providing relevant documentation (security policy, sub-processor list, breach log). On-site audits are not available at Solo and Growth tier; Premium and Enterprise customers may request a virtual audit session.

`[NOTE: Larger insurers may push for broader audit rights. This is worth discussing at Enterprise tier.]`

---

11. Data Retention and Deletion

Casepath retains personal information for as long as the MSA is active. On termination of the MSA:

- The Responsible Party has a **30-day grace period** to request a CSV data export (at no charge)
- After 30 days, Casepath will securely delete all personal information associated with the Responsible Party's account from its live systems and backups
- Casepath will provide written confirmation of deletion on request

12. Confidentiality of Processing

Casepath's personnel and contractors who access personal information under this agreement are subject to confidentiality obligations. Casepath will ensure that access is limited to those who need it to deliver the service.

13. Liability

Each party is responsible for its own POPIA compliance obligations. Casepath's liability under this agreement is limited to the cap set out in the MSA (clause 9 of the MSA).

14. Term and Termination

This agreement runs for the same period as the MSA and terminates automatically when the MSA terminates. The obligations in clauses 5, 7, 11, and 12 survive termination.

15. Governing Law

This agreement is governed by the laws of the **Republic of South Africa**. Any dispute will be resolved in accordance with the dispute resolution clause in the MSA.

Signatures

By signing, each party confirms they have read, understood, and agreed to this Data Processing Agreement.

Operator — Casepath

Name: Ruan van der Westhuizen Capacity: Owner / Operator Signature: _____ **Date:** _____

Responsible Party — `[CUSTOMER LEGAL NAME]`

Name: `[SIGNATORY NAME]` Capacity: `[Information Officer / Director / Authorised Signatory]` Signature: _____ **Date:** _____ Witness name: `[WITNESS NAME]` Witness signature: _____

This agreement is governed by the Protection of Personal Information Act 4 of 2013 and the laws of the Republic of South Africa.