

Data Processing Agreement

VERSION

1.0

EFFECTIVE

18 October 2026

SHA-256 6672da407086649e9e529be27ff0b51c90717109312aefd7c3efa1d7f26c4a9c

This Data Processing Agreement ("DPA") is between Practor (Pty) Ltd, a private company registered in South Africa ("Practor"), and the healthcare practice that uses the Practor platform (the "Practice"). It forms part of the Practor [Terms of Service](#) (the "Terms").

Part A applies to every Practice. Part B applies in addition where the GDPR or the UK GDPR applies to the Practice's processing. The Annexes form part of this DPA.

Part A: Operator terms

1. Acceptance of the DPA

1.1 This DPA is accepted electronically. A person with authority to bind the Practice accepts it on the Practice's behalf when the Practice is created on Practor, or later from the Practice's settings. Practor records the version accepted, the person who accepted it, the role they held in the Practice and the time of acceptance.

1.2 Acceptance by electronic means is a written agreement signed by the parties for the purposes of POPIA Section 21, in accordance with Sections 12 and 13 of the Electronic Communications and Transactions Act, 2002. No separate signature is needed. A copy signed by Practor is available on request from legal@practor.app.

1.3 The person who accepts this DPA confirms that they are authorised to bind the Practice. Practor relies on that confirmation.

1.4 This DPA applies from the earlier of the date the Practice accepts it and the date Practor first processes Practice Personal Information under the Terms, and continues for as long as Practor processes Practice Personal Information.

2. Definitions

2.1 In this DPA:

- **"Practice Personal Information"** means personal information that Practor processes on the Practice's behalf in providing the Service, including the personal information of the Practice's patients, their related persons (such as parents, guardians and medical insurance members), and the Practice's staff in their use of the Service. It includes special personal information, such as health information.
- **"POPIA"** means the Protection of Personal Information Act, 2013, and its regulations.
- **"GDPR"** means Regulation (EU) 2016/679 (the General Data Protection Regulation), and **"UK GDPR"** means the GDPR as it forms part of the law of the United Kingdom.
- **"Data Protection Law"** means POPIA and, where they apply to the processing, the GDPR, the UK GDPR and the laws implementing or supplementing them.
- **"Security Compromise"** means any situation in which there are reasonable grounds to believe that Practice Personal Information has been accessed or acquired by an unauthorised person, and includes a personal data breach under the GDPR.
- **"Sub-operator"** means a third party Practor engages to process Practice Personal Information on the Practice's behalf.
- **"Sub-processor Register"** means the list of Sub-operators published at practor.app/legal/sub-processors.
- **"Service"**, **"Customer Data"** and **"Authorized Users"** have the meanings given in the Terms.

2.2 POPIA and the GDPR use different words for the same roles. In this DPA, "responsible party" includes "controller", "operator" includes "processor", "Sub-operator" includes "sub-processor", "personal information" includes "personal data", and "special personal information" includes the "special categories of personal data" in Article 9 of the GDPR.

3. Roles of the parties

3.1 For Practice Personal Information, the Practice is the responsible party and Practor is its operator. The Practice decides why and how Practice Personal Information is processed. Practor processes it on the Practice's behalf.

3.2 This DPA does not apply to personal information that Practor processes for its own purposes as a responsible party, such as account and sign-in information, information used to bill the Practice for the Service, and information about visitors to Practor's websites. The [Privacy Policy](#) describes that processing.

3.3 Claims and eligibility requests that the Practice sends to a medical insurer, medical scheme or claims network through the Service are disclosed to that recipient on the Practice's instruction. The recipient processes them as a responsible party in its own right and is not a Sub-operator of Practor.

4. Processing on the Practice's instructions

4.1 Practor processes Practice Personal Information only with the knowledge or authorisation of the Practice, as POPIA Section 20 requires, and only on the Practice's documented instructions. The Practice's instructions are the Terms, this DPA, and the Practice's configuration and use of the Service. Annex 1 describes the processing.

4.2 Practor tells the Practice promptly if, in its opinion, an instruction infringes Data Protection Law. Practor may decline to follow that instruction until the Practice confirms or changes it.

4.3 If a law requires Practor to process or disclose Practice Personal Information other than on the Practice's instructions, Practor tells the Practice before it does so, unless that law prohibits telling the Practice. Practor discloses only what the law requires.

4.4 Practor does not sell Practice Personal Information, does not use it for marketing, and does not use it to train machine-learning models offered to anyone other than the Practice.

5. Confidentiality

5.1 Practor treats Practice Personal Information as confidential and does not disclose it unless the law requires it or the proper performance of its duties under the Terms requires it.

5.2 Practor ensures that every person it authorises to process Practice Personal Information is bound by a duty of confidentiality, whether by contract or by law, and has access only to the extent their work requires.

6. Security safeguards

6.1 Practor secures the integrity and confidentiality of Practice Personal Information by taking appropriate, reasonable technical and organisational measures to prevent its loss, damage, unauthorised destruction, and unlawful access or processing, as POPIA Section 19 and Article 32 of the GDPR require.

6.2 To do so, Practor identifies reasonably foreseeable internal and external risks, puts safeguards in place against them, checks regularly that the safeguards work, and updates them in response to new risks or deficiencies.

6.3 Annex 2 describes the measures in place. Practor may change them, provided that a change does not lower the overall level of protection.

7. Security Compromises

7.1 Practor notifies the Practice immediately, and in any event within 48 hours, after becoming aware of a Security Compromise, as POPIA Section 21(2) requires. Practor sends the notice to the Practice's owners by email and may also show it in the Service.

7.2 The notice describes, as far as Practor then knows, what happened, the categories and approximate number of patients and records concerned, the likely consequences, the measures Practor has taken or proposes to take, and a contact person. Where Practor does not yet know something, it says so and sends the information as it becomes available.

7.3 Practor takes reasonable steps to contain the Security Compromise, limit its consequences and restore the integrity of the affected systems.

7.4 The Practice, as responsible party, decides whether to notify the Information Regulator, any other supervisory authority, and the affected data subjects, as POPIA Section 22 and Articles 33 and 34 of the GDPR require. Practor gives the Practice the information and help it reasonably needs to do so. Practor does not notify the Practice's patients itself unless the Practice asks it to or the law requires it.

7.5 A notice under this clause is not an admission of fault or liability.

8. Sub-operators

8.1 The Practice authorises Practor to engage Sub-operators. The Sub-operators engaged at any time are those listed in the Sub-processor Register in force at that time.

8.2 Before a Sub-operator processes Practice Personal Information, Practor puts in place a written agreement that requires it to establish and maintain security safeguards and to treat the information as confidential, on terms that protect Practice Personal Information to at least the standard of this DPA.

8.3 Practor gives at least 30 days' notice before it adds or replaces a Sub-operator. Practor gives notice by publishing a new version of the Sub-processor Register and emailing the Practice's owners. The notice states the date the change takes effect.

8.4 The Practice may object to a change on reasonable data protection grounds by emailing privacy@practor.app before the change takes effect. Practor will try in good faith to address the objection. If it cannot, the Practice may stop using the part of the Service that depends on the new Sub-operator, or terminate the Terms, without penalty and with a pro-rated refund of any fees paid in advance for the period after termination.

8.5 Practor may replace a Sub-operator at short notice where it must do so to protect Practice Personal Information or to keep the Service running. Practor tells the Practice as soon as it can, and clause 8.4 still applies.

8.6 Practor remains liable to the Practice for the acts and omissions of its Sub-operators as if they were its own.

9. Where Practice Personal Information is processed

9.1 Practor hosts the Service and its databases on Amazon Web Services in Ireland (AWS region eu-west-1). Files uploaded to the Service, such as attachments, documents and recordings of consultations, are stored by Cloudinary in the United States. Other Sub-operators process Practice Personal Information in other countries. The Sub-processor Register lists where each one processes it.

9.2 Because Ireland and the other countries listed are outside South Africa, using the Service involves a transfer of Practice Personal Information across the border. Practor transfers it only where POPIA Section 72 permits, under binding agreements that give protection substantially similar to the conditions in POPIA, as Section 72(1)(b) provides. The protection given by the GDPR in Ireland and the European Union forms part of that protection.

9.3 Health information is special personal information. POPIA Section 57 may require the Practice, as responsible party, to obtain the Information Regulator's prior authorisation before special personal information is transferred to a country that does not provide an adequate level of protection. Whether it applies is for the Practice to decide. Practor gives the Practice the information about hosting and Sub-operators that it reasonably needs to make that decision.

9.4 Practor does not move the primary hosting of Practice Personal Information to another country without the notice that clause 8.3 requires for a new Sub-operator.

10. Help with data subjects and with compliance

10.1 Taking into account the nature of the processing, Practor helps the Practice by appropriate technical and organisational measures, so far as possible, to respond to requests from data subjects to exercise their rights, including requests for access, correction, deletion, objection and data portability. Most requests can be met with the tools in the Service. For anything the tools cannot do, the Practice can contact privacy@practor.app.

10.2 If a data subject sends Practor a request about Practice Personal Information, Practor refers them to the Practice and does not respond to the request itself, unless the Practice asks it to or the law requires it.

10.3 Practor gives the Practice reasonable help, using the information available to it, with data protection impact assessments, prior consultations and prior authorisations the Practice needs for its use of the Service.

11. Information and audits

11.1 Practor makes available to the Practice the information reasonably necessary to show that it meets its obligations under this DPA.

11.2 The Practice may audit Practor's compliance with this DPA once in any 12-month period, and also after a Security Compromise, or where a regulator requires it. The Practice gives at least 30 days' written notice, and the audit takes place during business hours, at the Practice's cost, under a duty of confidentiality, and without access to other customers' information.

11.3 Practor may meet an audit request first by giving written answers, documentation and evidence of its controls. An on-site audit takes place only if those do not reasonably answer the Practice's questions.

12. Return and deletion

12.1 During the Terms, the Practice may export Customer Data at any time using the Service's export tools.

12.2 When the Terms end, Practor makes Practice Personal Information available for export for the Retrieval Period described in Section 15 of the Terms. After that period, Practor deletes or de-identifies Practice Personal Information, unless a law requires Practor to keep it, in which case Practor keeps it confidential and processes it only for the purpose that law requires.

12.3 Deletion includes copies held by Sub-operators. Information in backups is deleted when the backups expire on their normal cycle, and is not restored in the meantime except to recover from a failure.

12.4 Practor confirms deletion in writing on request.

12.5 Health records are subject to the retention periods set by the Health Professions Council of South Africa and other laws that apply to the Practice. The Practice is responsible for keeping the records it must keep, and Section 15 of the Terms describes how Practor applies those periods.

13. The Practice's responsibilities

13.1 The Practice is responsible for:

- having a lawful basis for collecting and processing Practice Personal Information, including the authorisation POPIA Section 32 gives healthcare providers to process health information and any consent it needs;
- telling its patients how their information is processed, including that it uses Practor as its operator;
- the accuracy of the information it enters into the Service;
- deciding who in the Practice has access to the Service and at what level, and removing access when it is no longer needed;
- keeping sign-in credentials secure and using the security settings the Service offers; and
- ensuring that its instructions to Practor comply with Data Protection Law.

14. De-identified data

14.1 Practor may de-identify Practice Personal Information so that it can no longer identify a data subject, cannot be re-identified by reasonably foreseeable means, and cannot be linked to other information that identifies the data subject, as "de-identify" is defined in POPIA Section 1. Where the GDPR applies, the result must also be anonymous information within the meaning of the GDPR.

14.2 Information de-identified in this way is no longer Practice Personal Information. Practor may use it as Section 10.3 of the Terms allows. Practor does not attempt to re-identify it.

15. Liability

15.1 Each party's liability under this DPA is governed by the Terms, including Section 18 of the Terms.

15.2 Nothing in this DPA limits a party's liability to a data subject under POPIA Section 99, or any other liability that the law does not allow to be limited.

16. Precedence, changes and governing law

16.1 If this DPA conflicts with the Terms on the processing of Practice Personal Information, this DPA prevails. If Part B conflicts with Part A on processing to which the GDPR or the UK GDPR applies, Part B prevails. If the Standard Contractual Clauses conflict with this DPA, the Standard Contractual Clauses prevail.

16.2 Practor publishes each version of this DPA with a version number and an effective date at practor.app/legal/data-processing-agreement, and keeps every earlier version available there. A published version is never changed. A correction is published as a new version.

16.3 When Practor publishes a new version, it notifies the Practice's owners by email and shows the new version in the Practice's Legal agreements settings. A new version that adds to the protection of Practice Personal Information, or that only reflects a change in the law, takes effect on its effective date, which is at least 30 days after the notice. Any other new version takes effect for the Practice when the Practice accepts it. Until then, the version the Practice last accepted continues to apply.

16.4 This DPA is governed by the laws of the Republic of South Africa, except that Part B and the Standard Contractual Clauses are governed by the law Part B specifies.

Part B: GDPR terms

17. When Part B applies

17.1 Part B applies to Practice Personal Information whose processing is subject to the GDPR or the UK GDPR, for example because the Practice is established in the European Economic Area or the United Kingdom.

17.2 Practor's Service is available only in the markets listed on [practor.app](#). Before Practor accepts a Practice to which the GDPR or the UK GDPR applies, it will appoint a representative under Article 27 of the GDPR or the UK GDPR where the law requires a representative, and will publish the representative's details in the Privacy Policy.

18. Additional processor terms

18.1 Practor processes personal data only on documented instructions from the Practice, including with regard to transfers to a third country, as Article 28(3)(a) of the GDPR requires, unless Union or Member State law to which Practor is subject requires otherwise. Clause 4.3 applies to that case.

18.2 Clauses 5, 6, 7, 8, 10, 11 and 12 of Part A are Practor's commitments under Article 28(3)(b) to (h) of the GDPR. The notice periods and the right to object in clause 8 are the specific prior authorisation and the information about intended changes that Article 28(2) requires.

18.3 Practor notifies the Practice of a personal data breach without undue delay, in accordance with clause 7, so that the Practice can meet the 72-hour period in Article 33 of the GDPR.

19. International transfers

19.1 Practor is established in South Africa, which is not the subject of an adequacy decision under Article 45 of the GDPR. Where the Practice transfers personal data subject to the GDPR to Practor, the parties enter into, and this DPA incorporates by reference, the standard contractual clauses annexed to Commission Implementing Decision (EU) 2021/914 (the "Standard Contractual Clauses"), as follows:

- Module Two (controller to processor) applies where the Practice is a controller, and Module Three (processor to processor) applies where the Practice is itself a processor;
- the Practice is the data exporter and Practor is the data importer;
- the optional docking clause in Clause 7 applies;
- in Clause 9(a), Option 2 (general written authorisation) applies, with the notice period in clause 8.3 of this DPA;
- the optional wording in Clause 11(a) does not apply;
- in Clause 13, the competent supervisory authority is the one determined by Clause 13(a) for the Practice;
- in Clause 17, Option 1 applies and the governing law is the law of Ireland;
- in Clause 18(b), disputes are resolved before the courts of Ireland; and
- Annex I.A lists the parties as in this DPA, Annex I.B is Annex 1 of this DPA, Annex I.C is given by Clause 13 as above, Annex II is Annex 2 of this DPA, and Annex III is the Sub-processor Register.

19.2 Where the Practice transfers personal data subject to the UK GDPR, the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued by the UK Information Commissioner (version B1.0) applies, completed with the information in clause 19.1 and the Annexes. Either party may end the Addendum as its Section 19 allows.

19.3 Where the Swiss Federal Act on Data Protection applies, the Standard Contractual Clauses apply with the changes it requires, and the Swiss Federal Data Protection and Information Commissioner is a competent supervisory authority.

19.4 Practor transfers personal data to Sub-operators outside the European Economic Area only under an adequacy decision or with appropriate safeguards under Article 46 of the GDPR, such as the Standard Contractual Clauses.

20. Governing law of Part B

20.1 Part B is governed by the law of Ireland where the GDPR applies, and by the law of England and Wales where the UK GDPR applies.

Annex 1: Description of the processing

Subject matter. Providing the Service: a practice management and electronic health record platform, with scheduling, clinical records, billing and claims, patient communications, a patient portal and AI-assisted features.

Duration. For as long as the Terms are in force, and afterwards for the Retrieval Period and any period the law requires, as clause 12 describes.

Nature and purpose. Collecting, recording, organising, storing, retrieving, using, transmitting, displaying and deleting Practice Personal Information so that the Practice can run its practice: booking and reminding patients of appointments, recording consultations and treatment, drafting clinical notes from recorded or transcribed encounters where the Practice uses that feature, answering patients' phone calls and messages where the Practice uses Ava, invoicing and submitting claims, and giving patients access to their own information through the patient portal.

Data subjects.

- The Practice's patients, including children.
- People related to patients, such as parents, guardians, next of kin and the main members of medical insurance.
- The Practice's staff and practitioners, in their use of the Service.
- People who contact the Practice through the Service, such as callers to the Practice's phone line.

Categories of personal information.

- Identity and contact details: names, identity or passport numbers, dates of birth, sex, addresses, phone numbers and email addresses.
- Medical insurance details: insurer, plan, membership and dependant numbers.
- Health information: medical history, diagnoses and their codes, observations, allergies, medications, immunisations, procedures, clinical notes, documents and images, questionnaires, and recordings and transcripts of consultations where the Practice records them.
- Billing information: invoices, claims, payments and remittances.
- Communications: messages, emails, SMS and WhatsApp messages, and recordings and transcripts of phone calls handled by Ava.
- Information about use of the Service by staff and patients: sign-in records and audit logs.

Special personal information. Health information, and personal information about children. The measures in Annex 2 apply to all of it.

Recipients. Practor's authorised personnel, the Sub-operators in the Sub-processor Register, and the recipients the Practice chooses, such as the medical insurers and claims networks it submits claims to and the patients it gives portal access to.

Annex 2: Technical and organisational measures

Encryption. Data in transit between users and the Service is encrypted with TLS. The primary database, the search index, the cache and the storage used for background processing are encrypted at rest.

Hosting and network. The Service runs in a private network in AWS Ireland. The database, cache and search index are not reachable from the internet. Public traffic reaches the Service through Cloudflare and Amazon CloudFront, which protect it against denial-of-service attacks.

Access control. Every person using the Service signs in with their own account. Practices can require a second factor at sign-in. Each Practice's information is kept separate from every other Practice's, and access within a Practice follows the roles and permissions the Practice assigns. A patient using the portal sees only their own information.

Audit logging. The Service records access to patient records and security-relevant events, such as sign-ins, changes to roles and permissions, and exports, in an audit log the Practice can read.

Practor personnel. Access to production systems is limited to the personnel who need it to run the Service. Personnel are bound by confidentiality.

Backups and availability. The primary database is backed up automatically every day, and backups are kept for 7 days. Backups are encrypted and stored in the same AWS region.

Secure development. Changes to the Service are tested before release.

Incident response. Practor monitors the Service for errors and security events and responds to a Security Compromise as clause 7 describes.

Retention and deletion. Practor deletes or de-identifies Practice Personal Information as clause 12 describes. Transcripts of phone calls handled by Ava are deleted after the retention period the Practice sets, which is 90 days unless the Practice changes it.

Sub-operators. Practor assesses the security and privacy practices of a Sub-operator before engaging it and binds it by contract as clause 8.2 describes.

Annex 3: Sub-operators

The Sub-operators Practor engages, what each one processes, and where, are listed in the Sub-processor Register at practor.app/legal/sub-processors. Each version of the Register is kept there with its effective date.

Version history

VERSION	EFFECTIVE	CHANGES
1.0	18 October 2026	First version.