

DRAFT — DIANO Operator Agreement (POPIA section 21)

DRAFT for review by DIALE Consulting's lawyer. Not signed and not in force.

DIA_TRUST_CENTRE_V1 (build U, 19 Oct 2026). Plain-words draft written from POPIA ss 19–22 and 72, the Trust Centre and DIANO's live configuration (docs/trust/claims-evidence.md). Points for the lawyer are marked **[Lawyer: ...]**.

Between DIALE CONSULTING (PTY) LTD, Reg No 2020/124968/07, 16 Puffback Street, Centurion, Gauteng, 0157 ("**DIANO**", the operator), and **the subscribing company** named in its DIANO account ("**the Client**", the responsible party).

1. What this agreement is for

1.1 The Client uses DIANO to keep its business records. Those records include personal information about the Client's customers, suppliers, employees and users ("**Client Personal Information**"). 1.2 For Client Personal Information, the Client is the responsible party and DIANO is the operator, as POPIA defines them. This agreement is the written contract POPIA section 21(1) requires. 1.3 It forms part of DIANO's Terms and Conditions. If they conflict on Client Personal Information, this agreement wins. **[Lawyer: incorporation by acceptance at sign-up vs. signature; existing subscribers.]**

2. What DIANO processes (Annex C)

The kinds of personal information and of people are listed in Annex C. DIANO processes them only to provide DIANO to the Client, for as long as the Client subscribes and for the export period in clause 10.

3. Only on the Client's instructions (POPIA s20(a))

3.1 DIANO processes Client Personal Information only to provide the service, on the Client's instructions given through DIANO (what its users capture, import, export and delete) or in writing. 3.2 DIANO will tell the Client if it believes an instruction breaks POPIA, or if the law requires DIANO to process information in another way, unless the law forbids telling.

4. Confidentiality (POPIA s20(b))

4.1 DIANO keeps Client Personal Information confidential and does not disclose it unless the law requires it or it is needed to provide the service. 4.2 Only people bound by confidentiality may reach

it. Today that is the platform owner alone (Trust Centre, "Who can see your data"). 4.3 DIANO does not sell Client Personal Information and does not use it for marketing.

5. Security (POPIA s19 and s21(1))

5.1 DIANO keeps the technical and organisational measures in Annex A, and reviews them at least once a year and after every incident. 5.2 DIANO may improve the measures. It will not reduce their overall protection without 30 days' written notice.

6. Requests from data subjects (POPIA ss 23–25)

6.1 If a person asks DIANO about their personal information held for the Client (access, correction, deletion or objection), DIANO passes the request on to the Client within **2 business days** and does not answer it itself, unless the Client asks it to. 6.2 DIANO helps the Client answer, using DIANO's export, edit and delete functions, or by hand where they don't reach.

7. Sub-operators (Annex B)

7.1 The Client agrees to the sub-operators in Annex B. 7.2 DIANO gives at least **30 days'** notice of a new sub-operator by e-mail to the Client's Company Admins and on the Trust Centre. The Client may object within 14 days on reasonable data-protection grounds; if DIANO cannot meet the objection, the Client may cancel without penalty and receive a pro-rata refund of fees paid in advance. 7.3 DIANO binds each sub-operator to data-protection terms at least as protective as this agreement (for Google Cloud, its Cloud Data Processing Addendum). **[Lawyer: whether Google's standard terms satisfy "at least as protective".]**

8. Security compromises (POPIA s21(2) and s22)

8.1 DIANO tells the Client **as soon as it has reasonable grounds to believe** that Client Personal Information has been accessed or acquired by an unauthorised person, and in any case **within 24 hours** of reaching that view. 8.2 The notice says, as far as is known: what happened and when, which records and people may be affected, the possible consequences, what DIANO has done and will do, what the Client and the affected people should do, and, if known, who the unauthorised person is (the content POPIA s22(5) needs). DIANO updates it as it learns more. 8.3 The Client decides on notice to the Information Regulator and to data subjects (POPIA s22). DIANO helps with the facts the Regulator's eServices form asks for. DIANO does not notify the Client's data subjects itself unless the Client asks it to or the law requires it. **[Lawyer: "immediately" in s21(2) vs. the 24-hour outer limit.]**

9. Information sent outside South Africa (POPIA s72)

9.1 Some processing happens outside South Africa, as Annex B lists (sign-in in the United States; uploaded files in the United States until their planned move; one backup copy in Belgium; e-mail sending). 9.2 DIANO relies on POPIA s72(1)(a): each recipient is bound by a binding agreement giving

protection substantially similar to POPIA (Google's Cloud Data Processing Addendum). **[Lawyer: confirm the s72 basis; and SARS GN 787 rule 4 for the Client's electronic tax records kept outside South Africa (the backup copy in Belgium, uploaded files in the US) — does the Client need a rule 4.2 authorisation?]**

10. When the subscription ends (POPIA s14)

10.1 After the paid period ends, the Client may read and export its records for **90 days** (the Cancellation Policy). 10.2 DIANO then deletes Client Personal Information from the live system, unless the Client asks for earlier deletion or the law requires DIANO to keep it. Copies in backups expire on the dates in Annex A; the audit trail archive is locked for 7 years and cannot be deleted earlier. 10.3 On request DIANO confirms the deletion in writing.

11. Information and audits

11.1 DIANO keeps the Trust Centre, the Security Pack and the security questionnaire current, and answers the Client's reasonable written questions about the measures within 10 business days. 11.2 DIANO's infrastructure is Google Cloud; physical audits of Google's data centres are not possible. Google's certificates and reports are the evidence for that part. **[Lawyer: whether to offer a remote audit by an independent auditor at the Client's cost.]**

12. Liability

As in DIANO's Terms and Conditions. **[Lawyer: cap and exclusions for data-protection breaches.]**

13. Duration

This agreement lasts as long as DIANO processes Client Personal Information.

14. Law

South African law; the courts of South Africa.

Annex A — security measures (summary; the Trust Centre has the current detail)

- Records stored in Google Cloud africa-south1 (Johannesburg); exceptions in Annex B.
- Encryption in transit (TLS 1.2 or 1.3 only) and at rest (Google, AES-256, Google-managed keys).
- Each company's records separated by database rules; roles inside each company; every request checked on the server.
- Platform owner accounts require two-step sign-in; Company Admin two-step sign-in planned.

- Audit trail of every change (who, role, what, before/after, when); entries cannot be edited; archive locked 7 years.
- Backups: point-in-time recovery 7 days; daily backups kept 14 days; weekly 8 weeks; nightly export kept 90 days; a copy in Belgium kept 30 days; per-company backups kept 90 days. Restores tested on 8 and 10 October 2026.
- Releases through a deploy guard, staging first; Google-patched runtime; incident steps written down.

Annex B — sub-operators and locations

Sub-operator	Purpose	Location
Google Cloud (Google LLC and group companies)	Database, server functions, file storage, backups	South Africa (africa-south1); uploaded files United States (us-east1) until moved; one backup copy Belgium (europe-west1)
Google (Firebase Authentication)	Sign-in	United States
Google (Firebase Hosting)	Web pages (no records)	Worldwide network
Google Workspace (Gmail)	Sending DIANO's e-mails	Google's network; sending function in the United States (us-central1)
PayFast (Pty) Ltd	Subscription card payments — not in use yet	South Africa [check with PayFast before use]
Anthropic	Optional DIANO Assistant — not in use yet ; off unless a Company Admin turns it on	United States [check Anthropic's data processing terms before use]

Annex C — personal information and people

- **People:** the Client's users; its customers, suppliers and their contact people; its employees (if HR and payroll are used).
- **Information:** names, e-mail addresses, phone numbers, postal and delivery addresses, registration and VAT numbers, bank details, transaction records; for employees also ID numbers, tax numbers, pay, leave and contact details; sign-in records (time, account, IP address).