D

DIANO Security Pack

Version 2026-10-19-u1 · every fact checked on 19 October 2026

How DIANO keeps its clients' business records safe, in plain words, with the proof. Planned items are marked as planned, with a target month. Nothing here is legal advice.

DIALE CONSULTING (PTY) LTD · Reg No 2020/124968/07 · 16 Puffback Street, Centurion, Gauteng, 0157 · info@diale.co.za · 087 265 3889

Contents

1. Where your data lives
2. Who can see your data
3. Encryption
4. Backups and restore
5. Disaster recovery
6. Audit trail and evidence in court
7. Data protection (POPIA)
8. Security practices
9. Physical security
10. Compliance and certificates
11. Your data's lifecycle
12. Status and incidents
13. Roadmap
14. Security questions and answers
15. Sources

1. Where your data lives

> **IN SHORT**
>
> Your business records (customers, quotes, invoices, users and the audit trail) are stored in Google Cloud's Johannesburg region, called africa-south1. A few parts are kept outside South Africa. This page names each one, so you can answer your own clients.

Kept in South Africa

- Your business records (customers, quotes, invoices, users and the audit trail) are stored in Google Cloud's Johannesburg region, called africa-south1.
- DIANO's server code runs in africa-south1 too, with one exception: the function that sends e-mail runs in Google's us-central1 region in the United States.
- The daily and weekly backups, the nightly copies and each company's own backup are kept in africa-south1.

Kept or handled outside South Africa

- Files you upload, such as your company logo, signatures and stored documents, are kept in Google's us-east1 region in the United States.
- One more copy of the nightly backup is kept in Google's europe-west1 region in Belgium, in case the whole South African region fails.
- Sign-in is handled by Firebase Authentication, which Google runs only from data centres in the United States. It holds each user's name, e-mail address and a protected form of the password, not your business records.
- E-mails that DIANO sends, such as invitations and password links, go out through Google Workspace (Gmail). A copy of each e-mail is kept in the database for 7 days, then deleted automatically.
- Google's own system logs for DIANO are kept in Google's global log store for 30 days.
- The web pages themselves are served by Firebase Hosting from Google's worldwide network, so they load quickly everywhere. They contain no business records.

Why this matters for your tax records

SARS's rule says electronic tax records must be kept at a place in South Africa, unless a senior SARS official gives permission to keep them elsewhere. (Government Notice 787 of 1 October 2012, rule 4, made under Tax Administration Act section 30.) Source

Ask your tax adviser whether the copies kept outside South Africa affect you. The plan to bring uploaded files home is in the Roadmap below.

Other companies that process your data (sub-processors)

Company	What it does for DIANO
Google Cloud	Google Cloud (Google LLC and its group companies): hosting, database, sign-in, file storage, backups and e-mail sending.
PayFast	PayFast: will take card payments for DIANO subscriptions. PayFast is not used on DIANO yet.
Anthropic	Anthropic: will power the optional DIANO Assistant. The Assistant is not on DIANO yet.

Google's own list of the companies it uses: Google Cloud's own list of sub-processors.

Roadmap: planned, not true yet

Planned — target October 2026: Uploaded files move from us-east1 to africa-south1, so they are kept in South Africa too.

Planned — target October 2026: The e-mail sending function moves from us-central1 to africa-south1.

Planned — target December 2026: PayFast takes card payments for subscriptions. DIANO will never see or store your full card number.

Planned — target December 2026: The optional DIANO Assistant, powered by Anthropic. It is off until a Company Admin turns it on, and it only answers from DIANO's help pages.

Targets can move. When an item is done, it moves up into the page with its proof. The whole roadmap.

For your IT team / auditor

Each statement on this page, how it was checked and when. Every check was read-only. The full evidence (commands and their output) is available to auditors on request.

STATEMENT

Your business records (customers, quotes, invoices, users and the audit trail) are stored in Google Cloud's Johannesburg region, called africa-south1.

HOW IT WAS CHECKED

Google Cloud database settings (read-only check, 2026-10-20) (locationId: africa-south1); Google: africa-south1 is Johannesburg (published sources (see Sources)).

CHECKED

2026-10-19

STATEMENT

DIANO's server code runs in africa-south1 too, with one exception: the function that sends e-mail runs in Google's us-central1 region in the United States.

HOW IT WAS CHECKED

Google Cloud server functions (read-only check, 2026-10-20) (99 functions africa-south1; outside: us-central1 ext-firestore-send-email-processqueue).

CHECKED

2026-10-19

STATEMENT

The daily and weekly backups, the nightly copies and each company's own backup are kept in africa-south1.

HOW IT WAS CHECKED

Google Cloud backup schedules (read-only check, 2026-10-20) (backups in africa-south1); Google Cloud storage settings (read-only check, 2026-10-20) (firestore-exports, company-backups: AFRICA-SOUTH1). Google: "A backup resides in the same location as the source database."

CHECKED

2026-10-19

STATEMENT

Files you upload, such as your company logo, signatures and stored documents, are kept in Google's us-east1 region in the United States.

HOW IT WAS CHECKED

Google Cloud storage settings (read-only check, 2026-10-20) (dia-accounting.firebasestorage.app: US-EAST1); production Storage files (DIANO's release record of 2026-10-17: "22 files: 5 cloud-vault documents, 14 company logos, 3 signatures").

CHECKED

2026-10-19

STATEMENT

One more copy of the nightly backup is kept in Google's europe-west1 region in Belgium, in case the whole South African region fails.

HOW IT WAS CHECKED

Google Cloud scheduled jobs (read-only check, 2026-10-20) (transfer job dia-firestore-export-dr: firestore-exports → dr-europe-west1, daily); Google Cloud storage settings (read-only check, 2026-10-20) (dr-europe-west1: EUROPE-WEST1). europe-west1 = St. Ghislain, Belgium (Google regions page).

CHECKED

2026-10-19

STATEMENT

Sign-in is handled by Firebase Authentication, which Google runs only from data centres in the United States. It holds each user's name, e-mail address and a protected form of the password, not your business records.

HOW IT WAS CHECKED

Firebase privacy page (published sources (see Sources), B: "The Firebase Authentication service is run only from US data centers."); DIANO's data-location inventory (3 Oct 2026) (Identity Platform: no region option).

CHECKED

2026-10-19

STATEMENT

E-mails that DIANO sends, such as invitations and password links, go out through Google Workspace (Gmail). A copy of each e-mail is kept in the database for 7 days, then deleted automatically.

HOW IT WAS CHECKED

Google Cloud server functions (read-only check, 2026-10-20) (HOST = smtp.gmail.com, TTL_EXPIRE_TYPE = day, TTL_EXPIRE_VALUE = 7); Google Cloud logging and alerts (read-only check, 2026-10-20) (TTL mail/delivery.expireAt ACTIVE).

CHECKED

2026-10-19

STATEMENT

Google's own system logs for DIANO are kept in Google's global log store for 30 days.

HOW IT WAS CHECKED

Google Cloud logging and alerts (read-only check, 2026-10-20) (_Default: global, 30 days).

CHECKED

2026-10-19

STATEMENT

The web pages themselves are served by Firebase Hosting from Google's worldwide network, so they load quickly everywhere. They contain no business records.

HOW IT WAS CHECKED

DIANO's data-location inventory (3 Oct 2026) (Firebase Hosting: global CDN, no data at rest); DIANO's hosting settings (hosting serves DIANO's records only).

CHECKED

2026-10-19

STATEMENT

Google Cloud (Google LLC and its group companies): hosting, database, sign-in, file storage, backups and e-mail sending.

HOW IT WAS CHECKED

every evidence file above; Google subprocessors page https://cloud.google.com/terms/subprocessors (published sources (see Sources)).

CHECKED

2026-10-19

STATEMENT

PayFast: will take card payments for DIANO subscriptions. PayFast is not used on DIANO yet.

HOW IT WAS CHECKED

Google Cloud server functions (read-only check, 2026-10-20) (no PayFast function on production); this build's report (sub-processors).

CHECKED

2026-10-19

STATEMENT

Anthropic: will power the optional DIANO Assistant. The Assistant is not on DIANO yet.

HOW IT WAS CHECKED

Google Cloud server functions (read-only check, 2026-10-20) (no assistant function on production); build T report (assistant codebase built, off by default, not deployed).

CHECKED

2026-10-19

2. Who can see your data

> **IN SHORT**
>
> People can only see their own company's records. The database rules refuse everything else. Every request is checked on Google's servers: by DIANO's database rules and by the server code. The web browser is never trusted to say who you are or what you may do.

Roles inside your company

- Each person in your company has one role: Company Admin, Finance User, Sales, Delivery, Procurement, Accountant, Auditor or HR Payroll. The role decides what they can see and change.
- Some steps need a set role. For example, only a Company Admin or Finance User can issue an invoice, and only a Company Admin can export all the company's data.

Give each person the smallest role that lets them do their work. A Company Admin can change a person's role.

Signing in

- Passwords must be at least 8 characters long.
- Since 19 October 2026, the Administration area asks every DIANO platform owner account for two-step sign-in: a password or Google sign-in, plus a code from an authenticator app. The older administration page (/admin-classic) does not ask for the code yet, and DIANO's servers do not yet refuse an owner account that signed in without it.
- Two-step sign-in is not available yet for the people in your company. Today they sign in with a password or with Google sign-in.
- Every sign-in is recorded with the time, the account and the internet (IP) address.

DIANO's own staff

- DIANO's staff access is held by one person: the platform owner, Jonathan Diale, Director of DIALE Consulting. He uses three owner accounts, one of them kept only for emergencies.
- The platform owner can read your company's records. This is needed to set up companies and to help when you ask. DIANO's pages do not let the platform owner read your audit trail or your users' private details.
- As the owner of DIANO's Google Cloud project, the platform owner could also reach all data with Google's own tools.

- Changes are logged, whoever makes them, but reading a record is not logged one record at a time yet.

Zero trust, in plain words

Zero trust means nothing is believed just because it says so. Every request is checked on Google's servers: by DIANO's database rules and by the server code. The web browser is never trusted to say who you are or what you may do. People can only see their own company's records. The database rules refuse everything else.

Roadmap: planned, not true yet

Planned — target October 2026: DIANO's servers refuse a platform owner account that did not sign in with the authenticator code, and the older administration page asks for the code too.

Planned — target November 2026: Two-step sign-in comes to the people in your company: required for Company Admins, with 7 days to set it up, and open to every user.

Planned — target October 2026: Each time the platform owner reads your company's records, it is logged in the locked archive.

Planned — target January 2027: The platform owner reads a company's records only through a support grant that the company approves, with each read logged.

Targets can move. When an item is done, it moves up into the page with its proof. The whole roadmap.

For your IT team / auditor

Each statement on this page, how it was checked and when. Every check was read-only. The full evidence (commands and their output) is available to auditors on request.

STATEMENT
People can only see their own company's records. The database rules refuse everything else.

HOW IT WAS CHECKED
DIANO's live database rules (sameCompany(companyId) on every company path; rules gate DIANO's deploy tools).

CHECKED
2026-10-19

STATEMENT
Every request is checked on Google's servers: by DIANO's database rules and by the server code. The web browser is never trusted to say who you are or what you may do.

HOW IT WAS CHECKED
DIANO's live database rules (request.auth: Google-verified sign-in token); callables check request.auth (e.g. DIANO's live server code, DIANO's live server code exportAuditLog).

CHECKED
2026-10-19

STATEMENT
Each person in your company has one role: Company Admin, Finance User, Sales, Delivery, Procurement, Accountant, Auditor or HR Payroll. The role decides what they can see and change.

HOW IT WAS CHECKED
DIANO's live database rules (roleIsAnyOf with these eight role names).

CHECKED
2026-10-19

STATEMENT
Some steps need a set role. For example, only a Company Admin or Finance User can issue an invoice, and only a Company Admin can export all the company's data.

HOW IT WAS CHECKED
DIANO's live database rules (invoiceIssuer: Company Admin, Finance User); DIANO's live server code (EXPORT_ROLES = Company Admin).

CHECKED
2026-10-19

STATEMENT
Passwords must be at least 8 characters long.

HOW IT WAS CHECKED

Google Cloud sign-in and access settings (read-only check, 2026-10-20) (password policy ENFORCE, minPasswordLength 8).

CHECKED
2026-10-19

STATEMENT
Since 19 October 2026, the Administration area asks every DIANO platform owner account for two-step sign-in: a password or Google sign-in, plus a code from an authenticator app. The older administration page (/admin-classic) does not ask for the code yet, and DIANO's servers do not yet refuse an owner account that signed in without it.

HOW IT WAS CHECKED
release/production DIANO's records live through the deploy guard on 19 Oct 2026 at 19:47 UTC (21:50 SAST): DIANO's release record of 2026-10-19 ("A3 owners LIVE on production (19 Oct, 21:50 SAST)": end-to-end enrolment 11/11; an owner account enrolled at 20:14 UTC; the two other owner accounts not enrolled); the page's check: DIANO's published pages (DIA_TWO_STEP_V1: "every platform-owner account needs two-step sign-in"). Not enforced by the servers: DIANO's live server code (DIA_TWO_STEP_ENFORCE=off "until Stage A4"), DIANO's live database rules (isPlatformOwner(): no second-step check); DIANO's published pages (/admin-classic: no two-step script). Build X, 20 Oct 2026 (corrects build U's "not required yet", Jonathan's brief: "live on production since 19 Oct 21:50").

CHECKED
2026-10-20

STATEMENT
Two-step sign-in is not available yet for the people in your company. Today they sign in with a password or with Google sign-in.

HOW IT WAS CHECKED
DIANO's release record of 2026-10-19 (A3 for platform owners only; an enrolled Company Admin "cannot sign in to the client portal or /admin-classic once enrolled, until full A3"; enrolled second factors on production: 0).

CHECKED
2026-10-19

STATEMENT
Every sign-in is recorded with the time, the account and the internet (IP) address.

HOW IT WAS CHECKED
Google Cloud logging and alerts (read-only check, 2026-10-20) (sink audit-logs-to-storage: identitytoolkit requests + diano_security); DIANO's live server code.

CHECKED
2026-10-19

STATEMENT

DIANO's staff access is held by one person: the platform owner, Jonathan Diale, Director of DIALE Consulting. He uses three owner accounts, one of them kept only for emergencies.

HOW IT WAS CHECKED

DIANO's release record of 2026-10-19 (owner claim: 3 accounts, all Jonathan's, Jonathan 19 Oct; one is the break-glass owner); Google Cloud sign-in and access settings (read-only check, 2026-10-20) (roles/owner: 1 user).

CHECKED

2026-10-19

STATEMENT

The platform owner can read your company's records. This is needed to set up companies and to help when you ask. DIANO's pages do not let the platform owner read your audit trail or your users' private details.

HOW IT WAS CHECKED

DIANO's live database rules (companies/{id} and records: DIANO's records; auditLog and users: no platform-owner clause, comments "support grant later").

CHECKED

2026-10-19

STATEMENT

As the owner of DIANO's Google Cloud project, the platform owner could also reach all data with Google's own tools.

HOW IT WAS CHECKED

Google Cloud sign-in and access settings (read-only check, 2026-10-20) (roles/owner: 1 user).

CHECKED

2026-10-19

STATEMENT

Changes are logged, whoever makes them, but reading a record is not logged one record at a time yet.

HOW IT WAS CHECKED

Google Cloud server functions (read-only check, 2026-10-20) (audit* triggers on writes only); data-access logging is on for Cloud Storage only (DIANO's release record of 2026-10-17, "Access logging ON … for Cloud Storage").

CHECKED

2026-10-19

3. Encryption

> **IN SHORT**
>
> DIANO's web addresses accept only secure connections using TLS 1.2 or 1.3. Older, weaker versions are refused. Google encrypts all stored data, backups included, with AES-256. Google manages the keys.

On the way to and from DIANO

- DIANO's web addresses accept only secure connections using TLS 1.2 or 1.3. Older, weaker versions are refused.
- Browsers are told to always use the secure connection to diano.co.za (HSTS).

While it is stored

- Google encrypts all stored data, backups included, with AES-256. Google manages the keys.
- DIANO does not use its own encryption keys (customer-managed keys).

How Google does it: How Google encrypts stored data.

Files you download

- A company backup that a Company Admin downloads has passwords and secret keys taken out.

Keep downloaded exports and backups somewhere safe, such as an encrypted drive. Once a file leaves DIANO, its safety is in your hands.

For your IT team / auditor

Each statement on this page, how it was checked and when. Every check was read-only. The full evidence (commands and their output) is available to auditors on request.

STATEMENT

DIANO's web addresses accept only secure connections using TLS 1.2 or 1.3. Older, weaker versions are refused.

HOW IT WAS CHECKED

Google Cloud connection test (read-only check, 2026-10-20) (tls1, tls1_1: refused by the server; tls1_2 accepted; default TLSv1.3).

CHECKED

2026-10-19

STATEMENT

Google encrypts all stored data, backups included, with AES-256. Google manages the keys.

HOW IT WAS CHECKED

Google default encryption page (published sources (see Sources), B: "encrypted at the storage layer using … AES-256"); Google Cloud storage settings (read-only check, 2026-10-20) (customer key: none (Google-managed)); Google Cloud database settings (read-only check, 2026-10-20) (cmekConfig: None).

CHECKED

2026-10-19

STATEMENT

Browsers are told to always use the secure connection to diano.co.za (HSTS).

HOW IT WAS CHECKED

Google Cloud connection test (read-only check, 2026-10-20) (strict-transport-security: max-age=31556926).

CHECKED

2026-10-19

STATEMENT

DIANO does not use its own encryption keys (customer-managed keys).

HOW IT WAS CHECKED

Google Cloud database settings (read-only check, 2026-10-20) (cmekConfig: None); Google Cloud storage settings (read-only check, 2026-10-20) (no default_kms_key on any bucket).

CHECKED

2026-10-19

STATEMENT

A company backup that a Company Admin downloads has passwords and secret keys taken out.

HOW IT WAS CHECKED

DIANO's live server code and DIANO's live server code (SECRET); staging test DIANO's records 12/12 on 8 Oct 2026 ("downloads with secrets removed", DIANO's records on release/staging).

CHECKED

2026-10-19

4. Backups and restore

IN SHORT

A full backup of the database is made every day and kept for 14 days. Since 18 October 2026, DIANO can also take the database back to how it was at any minute in the last 7 days. This is called point-in-time recovery.

What is backed up, and how often

- A weekly backup is made every Sunday and kept for 8 weeks.
- Every night at 03:00 South African time, a full copy is also saved to separate storage in africa-south1 and kept for 90 days.
- That nightly copy is copied again to europe-west1 (Belgium) every day and kept there for 30 days.
- Each company also gets its own backup every night, kept for 90 days.
- When an uploaded file is replaced or deleted, the old version is kept, and a deleted file can be recovered for 7 days.
- The database is protected so that it cannot be deleted by mistake.

Where the copies are

- The daily and weekly backups, the nightly copies and each company's own backup are kept in africa-south1.
- One more copy of the nightly backup is kept in Google's europe-west1 region in Belgium, in case the whole South African region fails.

What is locked, and what is not

- The audit trail archive is locked for 7 years. Until then nobody can change or delete it, not even DIANO.
- The other backups are not locked yet. Someone with full control of DIANO's Google Cloud project could delete them.

How to get records back

- To get records back, a Company Admin asks in Settings, under Backups, and gives a reason. The platform owner checks and approves the request.
- A restore makes a new copy of your company. Your live company is not changed, so you can compare before anything is copied back.

In your request, say what is wrong, which records, and the date and time it went wrong. If you are not sure, e-mail info@diale.co.za and we will help.

Tested restores

- On 10 October 2026 a full copy of the live database was restored into a separate test database. All 22 kinds of records matched the original exactly, and the test database was then deleted.
- That test restore of 478 records took under 3 minutes. A larger database takes longer.
- On 8 October 2026 a company restore was tested on DIANO's test system. The new copy matched the original record for record, and the original was unchanged.
- A restore from point-in-time recovery or from the scheduled backups has not been tested yet.

Roadmap: planned, not true yet

Planned — target December 2026: Our lawyer advises on SARS's rule about where tax records must be kept. Then the backup copy in Belgium is either locked, so nobody can delete it early, or moved.

Planned — target October 2026: Restores from point-in-time recovery and from the scheduled backups are tested, and the results are published here.

Planned — target November 2026: Written times for restore requests are added to this page.

Targets can move. When an item is done, it moves up into the page with its proof. The whole roadmap.

For your IT team / auditor

Each statement on this page, how it was checked and when. Every check was read-only. The full evidence (commands and their output) is available to auditors on request.

STATEMENT
A full backup of the database is made every day and kept for 14 days.

HOW IT WAS CHECKED
Google Cloud backup schedules (read-only check, 2026-10-20) (daily: retention 14 days).

CHECKED
2026-10-19

STATEMENT
Since 18 October 2026, DIANO can also take the database back to how it was at any minute in the last 7 days. This is called point-in-time recovery.

HOW IT WAS CHECKED
Google Cloud database settings (read-only check, 2026-10-20) (POINT_IN_TIME_RECOVERY_ENABLED, versionRetentionPeriod 604800s, earliestVersionTime 2026-10-18T14:19:00Z).

CHECKED
2026-10-19

STATEMENT
A weekly backup is made every Sunday and kept for 8 weeks.

HOW IT WAS CHECKED
Google Cloud backup schedules (read-only check, 2026-10-20) (weekly SUNDAY: retention 56 days).

CHECKED
2026-10-19

STATEMENT
Every night at 03:00 South African time, a full copy is also saved to separate storage in africa-south1 and kept for 90 days.

HOW IT WAS CHECKED
Google Cloud scheduled jobs (read-only check, 2026-10-20) (dia-firestore-export 0 1 * * * UTC = 03:00 SAST); Google Cloud storage settings (read-only check, 2026-10-20) (firestore-exports: lifecycle Delete age 90).

CHECKED
2026-10-19

STATEMENT
That nightly copy is copied again to europe-west1 (Belgium) every day and kept there for 30 days.

HOW IT WAS CHECKED

Google Cloud scheduled jobs (read-only check, 2026-10-20) (dia-firestore-export-dr, 86400s); Google Cloud storage settings (read-only check, 2026-10-20) (dr-europe-west1: retention 30 days, lifecycle Delete age 31).

CHECKED

2026-10-19

STATEMENT

Each company also gets its own backup every night, kept for 90 days.

HOW IT WAS CHECKED

Google Cloud scheduled jobs (read-only check, 2026-10-20) (dia-company-backups 30 1 * * *; 20 Oct 01:30 UTC run: "companyBackup: done" 10 times, 0 failed, for the 10 companies of that night; 11 at the 02:25 UTC collection -- a test company of the running production gate set -- so the next run backs up 11). Reread 20 Oct 02:30 SAST (MAIN): claim holds.

CHECKED

2026-10-19

STATEMENT

When an uploaded file is replaced or deleted, the old version is kept, and a deleted file can be recovered for 7 days.

HOW IT WAS CHECKED

Google Cloud storage settings (read-only check, 2026-10-20) (dia-accounting.firebasestorage.app: versioning True, soft delete 7 days).

CHECKED

2026-10-19

STATEMENT

The database is protected so that it cannot be deleted by mistake.

HOW IT WAS CHECKED

Google Cloud database settings (read-only check, 2026-10-20) (DELETE_PROTECTION_ENABLED).

CHECKED

2026-10-19

STATEMENT

The daily and weekly backups, the nightly copies and each company's own backup are kept in africa-south1.

HOW IT WAS CHECKED

Google Cloud backup schedules (read-only check, 2026-10-20) (backups in africa-south1); Google Cloud storage settings (read-only check, 2026-10-20) (firestore-exports, company-backups: AFRICA-SOUTH1). Google: "A backup resides in the same location as the source database."

CHECKED

2026–10–19

STATEMENT

One more copy of the nightly backup is kept in Google's europe-west1 region in Belgium, in case the whole South African region fails.

HOW IT WAS CHECKED

Google Cloud scheduled jobs (read-only check, 2026–10–20) (transfer job dia-firestore-export-dr: firestore-exports → dr-europe-west1, daily); Google Cloud storage settings (read-only check, 2026–10–20) (dr-europe-west1: EUROPE-WEST1). europe-west1 = St. Ghislain, Belgium (Google regions page).

CHECKED

2026–10–19

STATEMENT

The audit trail archive is locked for 7 years. Until then nobody can change or delete it, not even DIANO.

HOW IT WAS CHECKED

Google Cloud storage settings (read-only check, 2026–10–20) (dia-accounting-audit-logs: retention 2556 days LOCKED); Google Bucket Lock page ("permanently preventing the policy from being reduced or removed").

CHECKED

2026–10–19

STATEMENT

The other backups are not locked yet. Someone with full control of DIANO's Google Cloud project could delete them.

HOW IT WAS CHECKED

Google Cloud storage settings (read-only check, 2026–10–20) (dr-europe-west1: 30 days not locked; firestore-exports, company-backups: retention none); Firestore backups have no lock option.

CHECKED

2026–10–19

STATEMENT

To get records back, a Company Admin asks in Settings, under Backups, and gives a reason. The platform owner checks and approves the request.

HOW IT WAS CHECKED

DIANO's published pages (requestCompanyRestore with a reason; the platform owner approves); Google Cloud server functions (read-only check, 2026–10–20) (requestCompanyRestore, ownerApproveCompanyRestore on production).

CHECKED

2026–10–19

STATEMENT

A restore makes a new copy of your company. Your live company is not changed, so you can compare before anything is copied back.

HOW IT WAS CHECKED

DIANO's live server code (restoreToNewCompany: "the source is never written"); DIANO's records 12/12 (8 Oct 2026, staging).

CHECKED

2026-10-19

STATEMENT

On 10 October 2026 a full copy of the live database was restored into a separate test database. All 22 kinds of records matched the original exactly, and the test database was then deleted.

HOW IT WAS CHECKED

DIANO's release record of 2026-10-12 (B5: restore-test-202610100703, 478 documents, "22 collections compared, 0 differ", scratch database deleted).

CHECKED

2026-10-19

STATEMENT

That test restore of 478 records took under 3 minutes. A larger database takes longer.

HOW IT WAS CHECKED

DIANO's release record of 2026-10-12 (B5 07:02–07:05 UTC: export finished 07:03:03, import and comparison done by 07:05).

CHECKED

2026-10-19

STATEMENT

On 8 October 2026 a company restore was tested on DIANO's test system. The new copy matched the original record for record, and the original was unchanged.

HOW IT WAS CHECKED

DIANO's release record of 2026-10-08 (backup-restore.mjs 12/12).

CHECKED

2026-10-19

STATEMENT

A restore from point-in-time recovery or from the scheduled backups has not been tested yet.

HOW IT WAS CHECKED

DIANO's backup and recovery plan (Layer 6 restore drill: "to do"); both were switched on 18 Oct 2026.

CHECKED

2026-10-19

5. Disaster recovery

IN SHORT

Disaster recovery means getting DIANO and your records back after something big goes wrong. We only give figures we have tested. Tested so far: DIANO can bring back your records as they were at the last nightly copy. So at most about one day of work could be lost.

If one data centre fails

- Google keeps the database in more than one data centre inside the Johannesburg region, so one data centre failing does not stop DIANO.

How much work could be lost

- Tested so far: DIANO can bring back your records as they were at the last nightly copy. So at most about one day of work could be lost.
- Since 18 October 2026, DIANO can also take the database back to how it was at any minute in the last 7 days. This is called point-in-time recovery.
- A restore from point-in-time recovery or from the scheduled backups has not been tested yet.

How long it takes

- That test restore of 478 records took under 3 minutes. A larger database takes longer.

If the whole South African region fails

- If Google's South African region fails, the written plan is to rebuild the database in another region from the copy in Belgium, then point DIANO at it.
- One more copy of the nightly backup is kept in Google's europe-west1 region in Belgium, in case the whole South African region fails.

Roadmap: planned, not true yet

Planned — target October 2026: Restores from point-in-time recovery and from the scheduled backups are tested, and the results are published here.

Planned — target January 2027: The region-failure plan is tested by rebuilding a copy of the test system from the Belgium copy.

Planned — target December 2026: Our lawyer advises on SARS's rule about where tax records must be kept. Then the backup copy in Belgium is either locked, so nobody can delete it early, or moved.

Targets can move. When an item is done, it moves up into the page with its proof. The whole roadmap.

For your IT team / auditor

Each statement on this page, how it was checked and when. Every check was read-only. The full evidence (commands and their output) is available to auditors on request.

STATEMENT

Tested so far: DIANO can bring back your records as they were at the last nightly copy. So at most about one day of work could be lost.

HOW IT WAS CHECKED

rs-drill (export restore tested 10 Oct 2026); Google Cloud scheduled jobs (read-only check, 2026-10-20) (export daily).

CHECKED

2026-10-19

STATEMENT

Google keeps the database in more than one data centre inside the Johannesburg region, so one data centre failing does not stop DIANO.

HOW IT WAS CHECKED

Google Cloud database settings (read-only check, 2026-10-20) (africa-south1 is a regional location); Google regions page: zones africa-south1-a, -b, -c (published sources (see Sources)); Firestore regional locations replicate across zones in the region.

CHECKED

2026-10-19

STATEMENT

Since 18 October 2026, DIANO can also take the database back to how it was at any minute in the last 7 days. This is called point-in-time recovery.

HOW IT WAS CHECKED

Google Cloud database settings (read-only check, 2026-10-20) (POINT_IN_TIME_RECOVERY_ENABLED, versionRetentionPeriod 604800s, earliestVersionTime 2026-10-18T14:19:00Z).

CHECKED

2026-10-19

STATEMENT

A restore from point-in-time recovery or from the scheduled backups has not been tested yet.

HOW IT WAS CHECKED

DIANO's backup and recovery plan (Layer 6 restore drill: "to do"); both were switched on 18 Oct 2026.

CHECKED

2026-10-19

STATEMENT

That test restore of 478 records took under 3 minutes. A larger database takes longer.

HOW IT WAS CHECKED

DIANO's release record of 2026-10-12 (B5 07:02–07:05 UTC: export finished 07:03:03, import and comparison done by 07:05).

CHECKED

2026-10-19

STATEMENT

If Google's South African region fails, the written plan is to rebuild the database in another region from the copy in Belgium, then point DIANO at it.

HOW IT WAS CHECKED

DIANO's written region-failure plan (this build).

CHECKED

2026-10-19

STATEMENT

One more copy of the nightly backup is kept in Google's europe-west1 region in Belgium, in case the whole South African region fails.

HOW IT WAS CHECKED

Google Cloud scheduled jobs (read-only check, 2026-10-20) (transfer job dia-firestore-export-dr: firestore-exports → dr-europe-west1, daily); Google Cloud storage settings (read-only check, 2026-10-20) (dr-europe-west1: EUROPE-WEST1). europe-west1 = St. Ghislain, Belgium (Google regions page).

CHECKED

2026-10-19

6. Audit trail and evidence in court

IN SHORT

Each entry shows who made the change and their role, what changed (the values before and after) and when. Nobody can edit or delete entries in the audit trail. Only DIANO's server writes them.

What each entry shows

- Every change to your records is written to your audit trail. This covers your company details, customers, quotes, sales orders, invoices, delivery notes, credit notes, statements, payments and users.
- Every sign-in is recorded with the time, the account and the internet (IP) address.

Kept and protected

- Each audit entry is also copied to the archive that is locked for 7 years.
- The audit trail archive is locked for 7 years. Until then nobody can change or delete it, not even DIANO.
- Every 30 minutes a check looks for any change that has no audit entry and adds the missing entry. The platform owner gets an e-mail alert when that happens.

Document numbers

- Quotes, sales orders, invoices, delivery notes, credit notes, statements and payments are numbered in order. A number is never skipped or used twice, and these documents cannot be deleted.

Getting a copy

- A Company Admin or Auditor can download the audit trail for a chosen period, as a spreadsheet file (CSV) or as JSON.
- A Company Admin can download all the company's records at any time as one ZIP file. Each kind of record is in it twice, as a CSV spreadsheet and as JSON, with a list of every file and its SHA-256 check value.

Electronic records and South African law

This is not legal advice. It explains how DIANO's records can support their weight as evidence. Ask your attorney how the law applies to your case.

- South African law says information does not lose its legal force just because it is electronic. (ECTA, Act 25 of 2002, section 11.) Source
- A court may not refuse an electronic record just because it is electronic, and must give it due weight. To judge its weight, the court looks at how reliably it was made, stored and sent, how its integrity was kept, and how the person who made it was identified. (ECTA section 15(1) to 15(3).) Source
- A record made in the ordinary course of business, or a copy certified as correct by an officer of the business, can be used in court as proof of its contents unless someone proves otherwise. (ECTA section 15(4).) Source
- Electronic records meet a duty to keep records if they stay readable, stay in their original format or one shown to be accurate, and show where they came from and when. (ECTA sections 14 and 16.) Source

How DIANO's records support their weight

What a court looks at	What DIANO does
How the record was made and stored	Every request is checked on Google's servers: by DIANO's database rules and by the server code. The web browser is never trusted to say who you are or what you may do. Nobody can edit or delete entries in the audit trail. Only DIANO's server writes them.
How its integrity was kept	The audit trail archive is locked for 7 years. Until then nobody can change or delete it, not even DIANO. Quotes, sales orders, invoices, delivery notes, credit notes, statements and payments are numbered in order. A number is never skipped or used twice, and these documents cannot be deleted.
Who made it	Each entry shows who made the change and their role, what changed (the values before and after) and when. Every sign-in is recorded with the time, the account and the internet (IP) address.

Ask your attorney who in your business should sign a certificate for a printout or an export.

How long to keep your records

- Tax records must be kept for 5 years after the return is submitted, and longer during a SARS audit, objection or appeal. (Tax Administration Act 28 of 2011, sections 29 and 32; VAT Act section 55.) Source
- Company records and accounting records generally have to be kept for 7 years. (Companies Act 71 of 2008, sections 24 and 28.) Source

- Employers must keep records of each employee's time worked and pay for 3 years. (Basic Conditions of Employment Act 75 of 1997, section 31.) Source
- SARS's rule says electronic tax records must be kept at a place in South Africa, unless a senior SARS official gives permission to keep them elsewhere. (Government Notice 787 of 1 October 2012, rule 4, made under Tax Administration Act section 30.) Source

Download an export every year and keep it for as long as the law asks you to, also after you stop using DIANO.

Roadmap: planned, not true yet

Planned — target January 2027: The platform owner reads a company's records only through a support grant that the company approves, with each read logged.

Targets can move. When an item is done, it moves up into the page with its proof. The whole roadmap.

For your IT team / auditor

Each statement on this page, how it was checked and when. Every check was read-only. The full evidence (commands and their output) is available to auditors on request.

STATEMENT

Each entry shows who made the change and their role, what changed (the values before and after) and when.

HOW IT WAS CHECKED

DIANO's live server code (columns at, actorName, actorEmail, actorRole, actorUid, changed, before, after).

CHECKED

2026-10-19

STATEMENT

Nobody can edit or delete entries in the audit trail. Only DIANO's server writes them.

HOW IT WAS CHECKED

DIANO's live database rules (companies/{id}/auditLog: allow write: if false).

CHECKED

2026-10-19

STATEMENT

Every change to your records is written to your audit trail. This covers your company details, customers, quotes, sales orders, invoices, delivery notes, credit notes, statements, payments and users.

HOW IT WAS CHECKED

Google Cloud server functions (read-only check, 2026-10-20) (auditCompanyWrite, auditCustomerWrite, auditQuoteWrite, auditSalesOrderWrite, auditInvoiceWrite, auditDeliveryNoteWrite, auditCreditNoteWrite, auditStatementWrite, auditPaymentWrite, auditCompanyUserWrite).

CHECKED

2026-10-19

STATEMENT

Every sign-in is recorded with the time, the account and the internet (IP) address.

HOW IT WAS CHECKED

Google Cloud logging and alerts (read-only check, 2026-10-20) (sink audit-logs-to-storage: identitytoolkit requests + diano_security); DIANO's live server code.

CHECKED

2026-10-19

STATEMENT

Each audit entry is also copied to the archive that is locked for 7 years.

HOW IT WAS CHECKED

Google Cloud logging and alerts (read-only check, 2026-10-20) (sink audit-logs-to-storage filter includes jsonPayload.logType="diano_audit"); DIANO's live server code (logType "diano_audit").

CHECKED

2026-10-19

STATEMENT

The audit trail archive is locked for 7 years. Until then nobody can change or delete it, not even DIANO.

HOW IT WAS CHECKED

Google Cloud storage settings (read-only check, 2026-10-20) (dia-accounting-audit-logs: retention 2556 days LOCKED); Google Bucket Lock page ("permanently preventing the policy from being reduced or removed").

CHECKED

2026-10-19

STATEMENT

Every 30 minutes a check looks for any change that has no audit entry and adds the missing entry. The platform owner gets an e-mail alert when that happens.

HOW IT WAS CHECKED

Google Cloud scheduled jobs (read-only check, 2026-10-20) (dia-audit-reconcile */30); Google Cloud logging and alerts (read-only check, 2026-10-20) (alert "reconcile repaired a missing entry", 1 e-mail channel).

CHECKED

2026-10-19

STATEMENT

Quotes, sales orders, invoices, delivery notes, credit notes, statements and payments are numbered in order. A number is never skipped or used twice, and these documents cannot be deleted.

HOW IT WAS CHECKED

DIANO's live database rules (counters move by one only together with the document they number; "no skipped, reused or forged numbers"; allow delete: if false on each of these collections).

CHECKED

2026-10-19

STATEMENT

A Company Admin or Auditor can download the audit trail for a chosen period, as a spreadsheet file (CSV) or as JSON.

HOW IT WAS CHECKED

DIANO's live server code (exportAuditLog: "Only a Company Admin or Auditor"); DIANO's live server code (format csv or json, from/to dates).

CHECKED

2026-10-19

STATEMENT

A Company Admin can download all the company's records at any time as one ZIP file. Each kind of record is in it twice, as a CSV spreadsheet and as JSON, with a list of every file and its SHA-256 check value.

HOW IT WAS CHECKED

DIANO's live server code (csv + json per type, manifest.json with record counts and SHA-256); DIANO's live server code (Company Admin); Google Cloud server functions (read-only check, 2026-10-20) (exportCompanyData on production).

CHECKED

2026-10-19

STATEMENT

Every request is checked on Google's servers: by DIANO's database rules and by the server code. The web browser is never trusted to say who you are or what you may do.

HOW IT WAS CHECKED

DIANO's live database rules (request.auth: Google-verified sign-in token); callables check request.auth (e.g. DIANO's live server code, DIANO's live server code exportAuditLog).

CHECKED

2026-10-19

7. Data protection (POPIA)

> **IN SHORT**
>
> For the records you keep in DIANO, your business is the responsible party and DIALE Consulting is the operator. DIANO does not sell personal information and does not use your records for marketing.

Who is who

- For the records you keep in DIANO, your business is the responsible party and DIALE Consulting is the operator.
- An operator must have a written contract with the responsible party and must tell it immediately if there are reasonable grounds to believe personal information was accessed by someone without permission. (POPIA, Act 4 of 2013, section 21.) Source

The Information Officer

- DIALE Consulting's Information Officer is Jonathan Diale (Director). Contact: info@diale.co.za, 087 265 3889.

When people ask about their own information

- The draft Operator Agreement says DIANO passes on to you any request from your customers or staff about their personal information, and helps you answer it.
- For DIANO's own records about you, you can ask the Information Officer for access, correction or deletion, and you can complain to the Information Regulator.

You can also contact the Information Regulator: The Information Regulator (South Africa).

If something goes wrong

- If DIANO learns of a security compromise affecting your records, DIANO will tell you, and the Information Regulator as POPIA section 22 requires.
- The draft Operator Agreement proposes that DIANO tells you as soon as it has reasonable grounds to believe your records were reached by someone without permission, and in any case within 24 hours.
- The responsible party must tell the Information Regulator and the people affected as soon as reasonably possible after a security compromise is found. (POPIA section 22.) Source
- Since 1 April 2025 the Information Regulator requires security compromises to be reported through its eServices portal, and the Information Officer must be registered there first. Source

The Operator Agreement

- A draft Operator Agreement is ready for review by DIANO's lawyer. It is not signed or in force yet.

Read the draft on the Downloads page. Please tell us what your own lawyer would change.

Sending data to other countries

- Personal information may be sent to another country only under the conditions of POPIA section 72, for example where the receiver is bound by rules that protect it as well as POPIA does. Source

The places outside South Africa are listed on Where your data lives.

Roadmap: planned, not true yet

Planned — target November 2026: The Operator Agreement is reviewed by a lawyer and offered to every company.

Targets can move. When an item is done, it moves up into the page with its proof. The whole roadmap.

For your IT team / auditor

Each statement on this page, how it was checked and when. Every check was read-only. The full evidence (commands and their output) is available to auditors on request.

STATEMENT

For the records you keep in DIANO, your business is the responsible party and DIALE Consulting is the operator.

HOW IT WAS CHECKED

DIANO's published pages (clause 3).

CHECKED

2026-10-19

STATEMENT

DIANO does not sell personal information and does not use your records for marketing.

HOW IT WAS CHECKED

DIANO's published pages (clause 4).

CHECKED

2026-10-19

STATEMENT

DIALE Consulting's Information Officer is Jonathan Diale (Director). Contact: info@diale.co.za, 087 265 3889.

HOW IT WAS CHECKED

DIANO's published pages (clause 1); confirmed by Jonathan on 19 Oct 2026 (DIANO's records).

CHECKED

2026-10-19

STATEMENT

The draft Operator Agreement says DIANO passes on to you any request from your customers or staff about their personal information, and helps you answer it.

HOW IT WAS CHECKED

the draft Operator Agreement (clause 6).

CHECKED

2026-10-19

STATEMENT

For DIANO's own records about you, you can ask the Information Officer for access, correction or deletion, and you can complain to the Information Regulator.

HOW IT WAS CHECKED

DIANO's published pages (clause 8).

CHECKED

2026-10-19

STATEMENT

If DIANO learns of a security compromise affecting your records, DIANO will tell you, and the Information Regulator as POPIA section 22 requires.

HOW IT WAS CHECKED

DIANO's published pages (clause 6).

CHECKED

2026-10-19

STATEMENT

The draft Operator Agreement proposes that DIANO tells you as soon as it has reasonable grounds to believe your records were reached by someone without permission, and in any case within 24 hours.

HOW IT WAS CHECKED

the draft Operator Agreement (clause 8); POPIA section 21(2) ("immediately").

CHECKED

2026-10-19

STATEMENT

A draft Operator Agreement is ready for review by DIANO's lawyer. It is not signed or in force yet.

HOW IT WAS CHECKED

the draft Operator Agreement (this build).

CHECKED

2026-10-19

8. Security practices

IN SHORT

Releases go through a deploy guard: a tool that builds from a recorded version, runs the checks first and stops if anything differs from what was reviewed. DIANO's server code runs on Node.js 24, a supported version, and Google applies security updates to it automatically.

Updates and patches

- DIANO's server code runs on Node.js 24, a supported version, and Google applies security updates to it automatically.
- Software libraries are updated by hand when DIANO releases changes. There is no automatic alert for weak libraries yet.

Testing before release

- New work is tested on a separate test system (staging) before it goes live. The database rules are checked against hundreds of test cases before every rules release.
- Releases go through a deploy guard: a tool that builds from a recorded version, runs the checks first and stops if anything differs from what was reviewed.

Watching for problems

- The platform owner gets e-mail alerts if the audit trail misses a change or its functions fail.
- There is no automatic check yet that warns when DIANO is down.

When something goes wrong

- DIANO's incident steps are written down: contain the problem, find out what was affected, tell the companies affected, fix it, and write up what happened.

Report a security problem

- To report a security problem, e-mail info@diale.co.za with "Security" in the subject line.

Please tell us before you tell anyone else, give us time to fix it, and never open or change other people's records while you look.

Not done yet

- No outside firm has tested DIANO's security yet (a penetration test).

- Some browser safety settings, such as a content security policy, are not switched on yet.

Roadmap: planned, not true yet

Planned — target October 2026: An automatic outage check that alerts the platform owner.

Planned — target December 2026: Automatic alerts for weak software libraries.

Planned — target December 2026: More browser safety settings are switched on, such as a content security policy.

Planned — target March 2027: An outside firm tests DIANO's security, and a summary letter is published here.

Planned — target November 2026: A dedicated address for security reports: security@diano.co.za.

Targets can move. When an item is done, it moves up into the page with its proof. The whole roadmap.

For your IT team / auditor

Each statement on this page, how it was checked and when. Every check was read-only. The full evidence (commands and their output) is available to auditors on request.

STATEMENT

Releases go through a deploy guard: a tool that builds from a recorded version, runs the checks first and stops if anything differs from what was reviewed.

HOW IT WAS CHECKED

DIANO's deploy tools; DIANO's release checklist.

CHECKED

2026-10-19

STATEMENT

DIANO's server code runs on Node.js 24, a supported version, and Google applies security updates to it automatically.

HOW IT WAS CHECKED

Google Cloud server functions (read-only check, 2026-10-20) (by runtime: nodejs24 99); Google Cloud logging and alerts (read-only check, 2026-10-20) (automaticUpdatePolicy present).

CHECKED

2026-10-19

STATEMENT

Software libraries are updated by hand when DIANO releases changes. There is no automatic alert for weak libraries yet.

HOW IT WAS CHECKED

no .github folder and no dependabot or renovate configuration in the repository (git ls-files .github is empty, 19 Oct 2026); DIANO's Node.js 24 upgrade plan (manual upgrade).

CHECKED

2026-10-19

STATEMENT

New work is tested on a separate test system (staging) before it goes live. The database rules are checked against hundreds of test cases before every rules release.

HOW IT WAS CHECKED

DIANO's release checklist; DIANO's deploy tools (rules gate, 688 cases on the staging line, build T report); release/staging run reports.

CHECKED

2026-10-19

STATEMENT

The platform owner gets e-mail alerts if the audit trail misses a change or its functions fail.

HOW IT WAS CHECKED

Google Cloud logging and alerts (read-only check, 2026-10-20) (4 alert policies, enabled, 1 e-mail channel).

CHECKED

2026-10-19

STATEMENT

There is no automatic check yet that warns when DIANO is down.

HOW IT WAS CHECKED

Google Cloud logging and alerts (read-only check, 2026-10-20) (uptime checks: 0).

CHECKED

2026-10-19

STATEMENT

DIANO's incident steps are written down: contain the problem, find out what was affected, tell the companies affected, fix it, and write up what happened.

HOW IT WAS CHECKED

DIANO's written incident steps (this build).

CHECKED

2026-10-19

STATEMENT

To report a security problem, e-mail info@diale.co.za with "Security" in the subject line.

HOW IT WAS CHECKED

DIANO's published pages (contact an owner account); DIANO's written incident steps.

CHECKED

2026-10-19

STATEMENT

No outside firm has tested DIANO's security yet (a penetration test).

HOW IT WAS CHECKED

no penetration-test report in the repository or the run reports (19 Oct 2026); Jonathan to confirm (this build's report, decisions).

CHECKED

2026-10-19

STATEMENT

Some browser safety settings, such as a content security policy, are not switched on yet.

HOW IT WAS CHECKED

Google Cloud connection test (read-only check, 2026-10-20) (no content-security-policy, x-frame-options or x-content-type-options header).

CHECKED

2026-10-19

9. Physical security

IN SHORT

DIANO has no servers of its own. Your records are kept in Google's data centres.

Google's data centres

- Google guards its data centres with several layers of security. They include fences, guards, cameras, metal detectors, vehicle barriers and biometric checks.

Read Google's own pages: Google's data-centre security page and How Google secures its infrastructure and data centres.

For your IT team / auditor

Each statement on this page, how it was checked and when. Every check was read-only. The full evidence (commands and their output) is available to auditors on request.

STATEMENT

DIANO has no servers of its own. Your records are kept in Google's data centres.

HOW IT WAS CHECKED

every location in Google Cloud storage settings (read-only check, 2026-10-20), Google Cloud database settings (read-only check, 2026-10-20) and Google Cloud server functions (read-only check, 2026-10-20) is a Google Cloud region.

CHECKED

2026-10-19

STATEMENT

Google guards its data centres with several layers of security. They include fences, guards, cameras, metal detectors, vehicle barriers and biometric checks.

HOW IT WAS CHECKED

Google infrastructure security design page and data-centre page (published sources (see Sources), B: "biometric identification, metal detection, cameras, vehicle barriers, and laser-based intrusion detection"; "Our six layers of physical security").

CHECKED

2026-10-19

10. Compliance and certificates

IN SHORT

DIANO itself does not hold ISO 27001, SOC 2 or any other security certificate. Google's certificates cover Google's part, not DIANO's own work. DIANO runs on Google Cloud. For the services DIANO uses (the database, sign-in, server functions and file storage), Google holds ISO/IEC 27001, 27017 and 27018 certificates and SOC 1, SOC 2 and SOC 3 reports. Firebase Hosting holds ISO/IEC 27001 and SOC 1, 2 and 3.

What Google Cloud holds

- DIANO runs on Google Cloud. For the services DIANO uses (the database, sign-in, server functions and file storage), Google holds ISO/IEC 27001, 27017 and 27018 certificates and SOC 1, SOC 2 and SOC 3 reports. Firebase Hosting holds ISO/IEC 27001 and SOC 1, 2 and 3.

See Google Cloud's list of certificates and reports and Firebase's privacy and security page, with its certificates per service and where each service runs.

POPIA

- There is no official POPIA certificate for any cloud service, so DIANO does not claim one.
- For the records you keep in DIANO, your business is the responsible party and DIALE Consulting is the operator.
- DIALE Consulting's Information Officer is Jonathan Diale (Director). Contact: info@diale.co.za, 087 265 3889.

Google's page about the POPI Act: Google Cloud's POPI Act page.

What DIANO does

- DIANO's policies are published: privacy, terms, refunds and cancellation. Sign-up asks you to accept them.
- Releases go through a deploy guard: a tool that builds from a recorded version, runs the checks first and stops if anything differs from what was reviewed.
- Nobody can edit or delete entries in the audit trail. Only DIANO's server writes them.

What DIANO does not hold yet

- DIANO itself does not hold ISO 27001, SOC 2 or any other security certificate. Google's certificates cover Google's part, not DIANO's own work.
- No outside firm has tested DIANO's security yet (a penetration test).

Roadmap: planned, not true yet

Planned — target March 2027: An outside firm tests DIANO's security, and a summary letter is published here.

Planned — target November 2026: The Operator Agreement is reviewed by a lawyer and offered to every company.

Targets can move. When an item is done, it moves up into the page with its proof. The whole roadmap.

For your IT team / auditor

Each statement on this page, how it was checked and when. Every check was read-only. The full evidence (commands and their output) is available to auditors on request.

STATEMENT

DIANO itself does not hold ISO 27001, SOC 2 or any other security certificate. Google's certificates cover Google's part, not DIANO's own work.

HOW IT WAS CHECKED

no certificate held (Jonathan to confirm in review, this build's report); DIANO's market scan (gap table).

CHECKED

2026-10-19

STATEMENT

DIANO runs on Google Cloud. For the services DIANO uses (the database, sign-in, server functions and file storage), Google holds ISO/IEC 27001, 27017 and 27018 certificates and SOC 1, SOC 2 and SOC 3 reports. Firebase Hosting holds ISO/IEC 27001 and SOC 1, 2 and 3.

HOW IT WAS CHECKED

Firebase privacy page table; Google compliance offerings (published sources (see Sources)).

CHECKED

2026-10-19

STATEMENT

There is no official POPIA certificate for any cloud service, so DIANO does not claim one.

HOW IT WAS CHECKED

Google's POPI page offers contractual support, not a certification; the /security/compliance/popia address returns 404 (published sources (see Sources)).

CHECKED

2026-10-19

STATEMENT

For the records you keep in DIANO, your business is the responsible party and DIALE Consulting is the operator.

HOW IT WAS CHECKED

DIANO's published pages (clause 3).

CHECKED

2026-10-19

STATEMENT

DIALE Consulting's Information Officer is Jonathan Diale (Director). Contact: info@diale.co.za, 087 265 3889.

HOW IT WAS CHECKED

DIANO's published pages (clause 1); confirmed by Jonathan on 19 Oct 2026 (DIANO's records).

CHECKED

2026-10-19

STATEMENT

DIANO's policies are published: privacy, terms, refunds and cancellation. Sign-up asks you to accept them.

HOW IT WAS CHECKED

DIANO's published pages; DIANO's published pages (sign-up checkbox: "I have read and accept the Terms and Conditions, …").

CHECKED

2026-10-19

STATEMENT

Releases go through a deploy guard: a tool that builds from a recorded version, runs the checks first and stops if anything differs from what was reviewed.

HOW IT WAS CHECKED

DIANO's deploy tools; DIANO's release checklist.

CHECKED

2026-10-19

STATEMENT

Nobody can edit or delete entries in the audit trail. Only DIANO's server writes them.

HOW IT WAS CHECKED

DIANO's live database rules (companies/{id}/auditLog: allow write: if false).

CHECKED

2026-10-19

STATEMENT

No outside firm has tested DIANO's security yet (a penetration test).

HOW IT WAS CHECKED

no penetration-test report in the repository or the run reports (19 Oct 2026); Jonathan to confirm (this build's report, decisions).

CHECKED

2026-10-19

11. Your data's lifecycle

IN SHORT

A Company Admin can download all the company's records at any time as one ZIP file. Each kind of record is in it twice, as a CSV spreadsheet and as JSON, with a list of every file and its SHA-256 check value.

While you use DIANO

- A Company Admin can download all the company's records at any time as one ZIP file. Each kind of record is in it twice, as a CSV spreadsheet and as JSON, with a list of every file and its SHA-256 check value.
- A Company Admin or Auditor can download the audit trail for a chosen period, as a spreadsheet file (CSV) or as JSON.

When you cancel

- The current Cancellation Policy says: after the paid period ends, your records stay available to read and export for 90 days, then they are deleted unless the law requires longer. This wording is under review.
- Deletion is done by hand today. There is no automatic deletion job yet.

Before you cancel, download an export and the audit trail, and check that they open.

When backups run out

- After your records are deleted, the copies in backups expire on their own by date: point-in-time copies after 7 days, daily backups after 14 days, weekly backups after 8 weeks, the copy in Belgium after about 31 days, and the nightly and company backups after 90 days. Google then keeps deleted backup files for 7 more days.
- Three things are kept longer. The audit trail archive is kept for 7 years and holds the values before and after each change. Old versions of uploaded files are kept until they are deleted by hand. One manual copy of the database, made on 1 October 2026 before an upgrade, has no expiry date yet.

Proof of deletion

- On request, DIANO confirms in writing what was deleted and when, and what is still kept and until when.

Roadmap: planned, not true yet

Planned — target January 2027: Deletion after the export window happens on its own, with an e-mail to you first.

Planned — target November 2026: The manual copy of 1 October 2026 is deleted.

Targets can move. When an item is done, it moves up into the page with its proof. The whole roadmap.

For your IT team / auditor

Each statement on this page, how it was checked and when. Every check was read-only. The full evidence (commands and their output) is available to auditors on request.

STATEMENT

A Company Admin can download all the company's records at any time as one ZIP file. Each kind of record is in it twice, as a CSV spreadsheet and as JSON, with a list of every file and its SHA-256 check value.

HOW IT WAS CHECKED

DIANO's live server code (csv + json per type, manifest.json with record counts and SHA-256); DIANO's live server code (Company Admin); Google Cloud server functions (read-only check, 2026-10-20) (exportCompanyData on production).

CHECKED

2026-10-19

STATEMENT

A Company Admin or Auditor can download the audit trail for a chosen period, as a spreadsheet file (CSV) or as JSON.

HOW IT WAS CHECKED

DIANO's live server code (exportAuditLog: "Only a Company Admin or Auditor"); DIANO's live server code (format csv or json, from/to dates).

CHECKED

2026-10-19

STATEMENT

The current Cancellation Policy says: after the paid period ends, your records stay available to read and export for 90 days, then they are deleted unless the law requires longer. This wording is under review.

HOW IT WAS CHECKED

DIANO's published pages (clause 3, marked "Wording under revision").

CHECKED

2026-10-19

STATEMENT

Deletion is done by hand today. There is no automatic deletion job yet.

HOW IT WAS CHECKED

Google Cloud server functions (read-only check, 2026-10-20) (no deletion/purge function on production; export/backup/restore/audit list only).

CHECKED

2026-10-19

STATEMENT

After your records are deleted, the copies in backups expire on their own by date: point-in-time copies after 7 days, daily backups after 14 days, weekly backups after 8 weeks, the copy in Belgium after about 31 days, and the nightly and company backups after 90 days. Google then keeps deleted backup files for 7 more days.

HOW IT WAS CHECKED

Google Cloud database settings (read-only check, 2026-10-20); Google Cloud backup schedules (read-only check, 2026-10-20); Google Cloud storage settings (read-only check, 2026-10-20) (lifecycle ages 31 and 90; soft delete 7 days).

CHECKED

2026-10-19

STATEMENT

Three things are kept longer. The audit trail archive is kept for 7 years and holds the values before and after each change. Old versions of uploaded files are kept until they are deleted by hand. One manual copy of the database, made on 1 October 2026 before an upgrade, has no expiry date yet.

HOW IT WAS CHECKED

Google Cloud storage settings (read-only check, 2026-10-20) (audit-logs 2556 days LOCKED; firebasestorage.app versioning, no lifecycle; firestore-export-za: no lifecycle, one folder phase2-pre-promotion-20261001T152726).

CHECKED

2026-10-19

STATEMENT

On request, DIANO confirms in writing what was deleted and when, and what is still kept and until when.

HOW IT WAS CHECKED

DIANO's deletion confirmation template (this build); Jonathan to confirm the commitment (this build's report, decisions).

CHECKED

2026-10-19

12. Status and incidents

IN SHORT

DIANO does not have a public status page yet. Service notices are sent by e-mail. Planned maintenance is on Sundays from 22:00 to 02:00 South African time.

Past incidents

We list problems that affected the safety of your records here, also those we found and fixed ourselves.

A purchase order could look saved when it was not

On 17 October 2026 DIANO found that a new purchase order could look saved while it had not reached the server, if the page did not yet know the user's role. It was fixed on the live system on 18 October 2026: DIANO now waits for the role, refuses out loud, and reads each new purchase order back from the server.

One more incident, under review

One more incident, found and fixed by DIANO, is waiting for a review by DIANO's lawyer. After that review it is listed here.

Roadmap: planned, not true yet

Planned — target October 2026: An automatic outage check that alerts the platform owner.

Planned — target November 2026: A public status page.

Targets can move. When an item is done, it moves up into the page with its proof. The whole roadmap.

For your IT team / auditor

Each statement on this page, how it was checked and when. Every check was read-only. The full evidence (commands and their output) is available to auditors on request.

STATEMENT
DIANO does not have a public status page yet. Service notices are sent by e-mail.

HOW IT WAS CHECKED
no status page in DIANO's hosting settings or DIANO's records (19 Oct 2026); DIANO's published pages footer notice ("we notify you at least 72 hours in advance by email").

CHECKED
2026-10-19

STATEMENT
Planned maintenance is on Sundays from 22:00 to 02:00 South African time.

HOW IT WAS CHECKED
DIANO's published pages footer (diaNoticeMaintenance).

CHECKED
2026-10-19

STATEMENT
On 17 October 2026 DIANO found that a new purchase order could look saved while it had not reached the server, if the page did not yet know the user's role. It was fixed on the live system on 18 October 2026: DIANO now waits for the role, refuses out loud, and reads each new purchase order back from the server.

HOW IT WAS CHECKED
DIANO's release record of 2026-10-17 (lost PO: records bridge dropped new records when canWrite() was false; DIA_NO_SILENT_SAVE_V1; production live 005e308bead17915, 18 Oct 07:13 SAST).

CHECKED
2026-10-19

STATEMENT
One more incident, found and fixed by DIANO, is waiting for a review by DIANO's lawyer. After that review it is listed here.

HOW IT WAS CHECKED
Jonathan's decision, 19 Oct 2026 (DIANO's records): publish the incidents page, but keep the 1 Jun – 18 Oct storage incident (inc-storage, "Held back" below) off it until the lawyer has reviewed it (DIANO's records).

CHECKED
2026-10-19

Roadmap

- **Planned — target October 2026:** Uploaded files move from us-east1 to africa-south1, so they are kept in South Africa too.
- **Planned — target October 2026:** The e-mail sending function moves from us-central1 to africa-south1.
- **Planned — target October 2026:** DIANO's servers refuse a platform owner account that did not sign in with the authenticator code, and the older administration page asks for the code too.
- **Planned — target November 2026:** Two-step sign-in comes to the people in your company: required for Company Admins, with 7 days to set it up, and open to every user.
- **Planned — target December 2026:** Our lawyer advises on SARS's rule about where tax records must be kept. Then the backup copy in Belgium is either locked, so nobody can delete it early, or moved.
- **Planned — target January 2027:** The platform owner reads a company's records only through a support grant that the company approves, with each read logged.
- **Planned — target October 2026:** Restores from point-in-time recovery and from the scheduled backups are tested, and the results are published here.
- **Planned — target January 2027:** The region-failure plan is tested by rebuilding a copy of the test system from the Belgium copy.
- **Planned — target November 2026:** Written times for restore requests are added to this page.
- **Planned — target October 2026:** An automatic outage check that alerts the platform owner.
- **Planned — target November 2026:** A public status page.
- **Planned — target October 2026:** Each time the platform owner reads your company's records, it is logged in the locked archive.
- **Planned — target December 2026:** Automatic alerts for weak software libraries.
- **Planned — target December 2026:** More browser safety settings are switched on, such as a content security policy.
- **Planned — target March 2027:** An outside firm tests DIANO's security, and a summary letter is published here.
- **Planned — target November 2026:** A dedicated address for security reports: security@diano.co.za.
- **Planned — target January 2027:** Deletion after the export window happens on its own, with an e-mail to you first.
- **Planned — target November 2026:** The manual copy of 1 October 2026 is deleted.
- **Planned — target November 2026:** The Operator Agreement is reviewed by a lawyer and offered to every company.
- **Planned — target December 2026:** PayFast takes card payments for subscriptions. DIANO will never see or store your full card number.
- **Planned — target December 2026:** The optional DIANO Assistant, powered by Anthropic. It is off until a Company Admin turns it on, and it only answers from DIANO's help pages.

Security questions and answers

ID	Question	Answer	Detail
GOV-01	Does the vendor hold its own ISO 27001 certificate?	**No**	DIANO itself does not hold ISO 27001, SOC 2 or any other security certificate. Google's certificates cover Google's part, not DIANO's own work.
GOV-02	Does the vendor have a SOC 2 report of its own?	**No**	DIANO itself does not hold ISO 27001, SOC 2 or any other security certificate. Google's certificates cover Google's part, not DIANO's own work.
GOV-03	Does the hosting provider hold recognised security certificates for the services used?	**Yes**	DIANO runs on Google Cloud. For the services DIANO uses (the database, sign-in, server functions and file storage), Google holds ISO/IEC 27001, 27017 and 27018 certificates and SOC 1, SOC 2 and SOC 3 reports. Firebase Hosting holds ISO/IEC 27001 and SOC 1, 2 and 3.
GOV-04	Is the vendor certified for POPIA?	**Not applicable**	There is no official POPIA certificate for any cloud service, so DIANO does not claim one.
GOV-05	Are the privacy policy, terms and cancellation policy published?	**Yes**	DIANO's policies are published: privacy, terms, refunds and cancellation. Sign-up asks you to accept them.
GOV-06	Has an independent penetration test been done?	**Planned**	No outside firm has tested DIANO's security yet (a penetration test). Planned — target March 2027: An outside firm tests DIANO's security, and a summary letter is published here.

ID	Question	Answer	Detail
DSP-01	In which country and region are business records stored?	**Answered**	Your business records (customers, quotes, invoices, users and the audit trail) are stored in Google Cloud's Johannesburg region, called africa-south1.
DSP-02	Does the server code run in the same region?	**Partly**	DIANO's server code runs in africa-south1 too, with one exception: the function that sends e-mail runs in Google's us-central1 region in the United States. Planned — target October 2026: The e-mail sending function moves from us-central1 to africa-south1.
DSP-03	Are uploaded files (logos, signatures, documents) stored in South Africa?	**No**	Files you upload, such as your company logo, signatures and stored documents, are kept in Google's us-east1 region in the United States. Planned — target October 2026: Uploaded files move from us-east1 to africa-south1, so they are kept in South Africa too.
DSP-04	Where are backups stored?	**Answered**	The daily and weekly backups, the nightly copies and each company's own backup are kept in africa-south1. One more copy of the nightly backup is kept in Google's europe-west1 region in Belgium, in case the whole South African region fails.
DSP-05	Where are sign-in identities processed?	**Answered**	Sign-in is handled by Firebase Authentication, which Google runs only from data centres in the United States. It holds each user's name, e-mail address and a protected form of the password, not your business records.
DSP-06	Which sub-processors are used, and for what?	**Answered**	Google Cloud (Google LLC and its group companies): hosting, database, sign-in, file storage, backups and e-mail sending. PayFast: will take card payments for DIANO subscriptions. PayFast is not used on DIANO yet. Anthropic: will power the optional DIANO Assistant. The Assistant is not on DIANO yet.

ID	Question	Answer	Detail
DSP-07	How are e-mails sent, and how long are copies kept?	**Answered**	E-mails that DIANO sends, such as invitations and password links, go out through Google Workspace (Gmail). A copy of each e-mail is kept in the database for 7 days, then deleted automatically.
DSP-08	Can electronic tax records be kept outside South Africa?	**Partly**	SARS's rule says electronic tax records must be kept at a place in South Africa, unless a senior SARS official gives permission to keep them elsewhere. (Government Notice 787 of 1 October 2012, rule 4, made under Tax Administration Act section 30.) Files you upload, such as your company logo, signatures and stored documents, are kept in Google's us-east1 region in the United States. One more copy of the nightly backup is kept in Google's europe-west1 region in Belgium, in case the whole South African region fails.
IAM-01	Is access based on roles?	**Yes**	Each person in your company has one role: Company Admin, Finance User, Sales, Delivery, Procurement, Accountant, Auditor or HR Payroll. The role decides what they can see and change.
IAM-02	Is each customer's data separated from other customers?	**Yes**	People can only see their own company's records. The database rules refuse everything else.
IAM-03	Are permissions enforced on the server, not only in the browser?	**Yes**	Every request is checked on Google's servers: by DIANO's database rules and by the server code. The web browser is never trusted to say who you are or what you may do.
IAM-04	Are some steps limited to set roles (segregation of duties)?	**Yes**	Some steps need a set role. For example, only a Company Admin or Finance User can issue an invoice, and only a Company Admin can export all the company's data.

ID	Question	Answer	Detail
IAM-05	Is multi-factor sign-in required for the vendor's administrators?	**Partly**	Since 19 October 2026, the Administration area asks every DIANO platform owner account for two-step sign-in: a password or Google sign-in, plus a code from an authenticator app. The older administration page (/admin-classic) does not ask for the code yet, and DIANO's servers do not yet refuse an owner account that signed in without it. Planned — target October 2026: DIANO's servers refuse a platform owner account that did not sign in with the authenticator code, and the older administration page asks for the code too.
IAM-06	Is multi-factor sign-in available for customer users?	**Planned**	Two-step sign-in is not available yet for the people in your company. Today they sign in with a password or with Google sign-in. Planned — target November 2026: Two-step sign-in comes to the people in your company: required for Company Admins, with 7 days to set it up, and open to every user.
IAM-07	Is there a password policy?	**Yes**	Passwords must be at least 8 characters long.
IAM-08	Who at the vendor can access customer data?	**Answered**	DIANO's staff access is held by one person: the platform owner, Jonathan Diale, Director of DIALE Consulting. He uses three owner accounts, one of them kept only for emergencies. The platform owner can read your company's records. This is needed to set up companies and to help when you ask. DIANO's pages do not let the platform owner read your audit trail or your users' private details. As the owner of DIANO's Google Cloud project, the platform owner could also reach all data with Google's own tools.
IAM-09	Is vendor access to customer data approved by the customer each time?	**Planned**	The platform owner can read your company's records. This is needed to set up companies and to help when you ask. DIANO's pages do not let the platform owner read your audit trail or your users' private details. Planned — target October 2026: Each time the platform owner reads your company's records, it is logged in the locked archive. Planned — target January 2027: The platform owner reads a

ID	Question	Answer	Detail
			company's records only through a support grant that the company approves, with each read logged.
IAM-10	Are sign-ins logged?	**Yes**	Every sign-in is recorded with the time, the account and the internet (IP) address.
EKM-01	Is data encrypted in transit?	**Yes**	DIANO's web addresses accept only secure connections using TLS 1.2 or 1.3. Older, weaker versions are refused. Browsers are told to always use the secure connection to diano.co.za (HSTS).
EKM-02	Are old TLS versions refused?	**Yes**	DIANO's web addresses accept only secure connections using TLS 1.2 or 1.3. Older, weaker versions are refused.
EKM-03	Is data encrypted at rest, including backups?	**Yes**	Google encrypts all stored data, backups included, with AES-256. Google manages the keys.
EKM-04	Can the customer manage the encryption keys?	**No**	DIANO does not use its own encryption keys (customer-managed keys).
EKM-05	Are secrets removed from downloadable backups?	**Yes**	A company backup that a Company Admin downloads has passwords and secret keys taken out.
BCR-01	How often is the database backed up, and how long are backups kept?	**Answered**	A full backup of the database is made every day and kept for 14 days. A weekly backup is made every Sunday and kept for 8 weeks.
BC	Is point-in-time recovery	**Yes**	Since 18 October 2026, DIANO can also take the database back to how it was at any minute in the last 7 days. This is

ID	Question	Answer	Detail
R-02	available?		called point-in-time recovery.
BCR-03	Is there a backup copy in a second region?	**Yes**	That nightly copy is copied again to europe-west1 (Belgium) every day and kept there for 30 days.
BCR-04	Are backups immutable (locked against deletion)?	**Partly**	The audit trail archive is locked for 7 years. Until then nobody can change or delete it, not even DIANO. The other backups are not locked yet. Someone with full control of DIANO's Google Cloud project could delete them. Planned — target December 2026: Our lawyer advises on SARS's rule about where tax records must be kept. Then the backup copy in Belgium is either locked, so nobody can delete it early, or moved.
BCR-05	Is the database protected against accidental deletion?	**Yes**	The database is protected so that it cannot be deleted by mistake.
BCR-06	Are old versions of uploaded files kept?	**Yes**	When an uploaded file is replaced or deleted, the old version is kept, and a deleted file can be recovered for 7 days.
BCR-07	Can a single company be restored without affecting others?	**Yes**	Each company also gets its own backup every night, kept for 90 days. A restore makes a new copy of your company. Your live company is not changed, so you can compare before anything is copied back.
BCR-	How does a customer ask for a restore?	**Answered**	To get records back, a Company Admin asks in Settings, under Backups, and gives a reason. The platform owner checks and approves the request.

ID	Question	Answer	Detail
08			
BCR-09	Has a restore been tested, and when?	**Yes**	On 10 October 2026 a full copy of the live database was restored into a separate test database. All 22 kinds of records matched the original exactly, and the test database was then deleted. On 8 October 2026 a company restore was tested on DIANO's test system. The new copy matched the original record for record, and the original was unchanged.
BCR-10	Have all restore methods been tested?	**Planned**	A restore from point-in-time recovery or from the scheduled backups has not been tested yet. Planned — target October 2026: Restores from point-in-time recovery and from the scheduled backups are tested, and the results are published here.
BCR-11	What recovery point and time have been shown in tests?	**Answered**	Tested so far: DIANO can bring back your records as they were at the last nightly copy. So at most about one day of work could be lost. That test restore of 478 records took under 3 minutes. A larger database takes longer.
BCR-12	Is there a plan for the loss of a whole region?	**Partly**	If Google's South African region fails, the written plan is to rebuild the database in another region from the copy in Belgium, then point DIANO at it. Planned — target January 2027: The region-failure plan is tested by rebuilding a copy of the test system from the Belgium copy.
BCR-13	Does the service survive the loss of one data centre?	**Yes**	Google keeps the database in more than one data centre inside the Johannesburg region, so one data centre failing does not stop DIANO.
BCR-14	Is there a published restore time commitment?	**Planned**	Planned — target November 2026: Written times for restore requests are added to this page.
LOG	Are changes to business	**Yes**	Every change to your records is written to your audit trail. This covers your company details, customers, quotes, sales orders, invoices, delivery notes, credit notes, statements,

ID	Question	Answer	Detail
-01	records logged?		payments and users. Each entry shows who made the change and their role, what changed (the values before and after) and when.
LOG-02	Can audit entries be changed or deleted by users?	**No**	Nobody can edit or delete entries in the audit trail. Only DIANO's server writes them.
LOG-03	How long are audit logs kept, and are they tamper-proof?	**Answered**	Each audit entry is also copied to the archive that is locked for 7 years. The audit trail archive is locked for 7 years. Until then nobody can change or delete it, not even DIANO.
LOG-04	Is the completeness of the audit trail checked?	**Yes**	Every 30 minutes a check looks for any change that has no audit entry and adds the missing entry. The platform owner gets an e-mail alert when that happens.
LOG-05	Can the customer export the audit trail?	**Yes**	A Company Admin or Auditor can download the audit trail for a chosen period, as a spreadsheet file (CSV) or as JSON.
LOG-06	Is read access to records logged?	**No**	Changes are logged, whoever makes them, but reading a record is not logged one record at a time yet.
LOG-07	Are document numbers sequential and protected?	**Yes**	Quotes, sales orders, invoices, delivery notes, credit notes, statements and payments are numbered in order. A number is never skipped or used twice, and these documents cannot be deleted.

ID	Question	Answer	Detail
DSI-01	Can the customer export all data, and in which formats?	**Answered**	A Company Admin can download all the company's records at any time as one ZIP file. Each kind of record is in it twice, as a CSV spreadsheet and as JSON, with a list of every file and its SHA-256 check value.
DSI-02	What happens to data after cancellation?	**Partly**	The current Cancellation Policy says: after the paid period ends, your records stay available to read and export for 90 days, then they are deleted unless the law requires longer. This wording is under review. Deletion is done by hand today. There is no automatic deletion job yet. Planned — target January 2027: Deletion after the export window happens on its own, with an e-mail to you first.
DSI-03	When do copies in backups expire after deletion?	**Answered**	After your records are deleted, the copies in backups expire on their own by date: point-in-time copies after 7 days, daily backups after 14 days, weekly backups after 8 weeks, the copy in Belgium after about 31 days, and the nightly and company backups after 90 days. Google then keeps deleted backup files for 7 more days. Three things are kept longer. The audit trail archive is kept for 7 years and holds the values before and after each change. Old versions of uploaded files are kept until they are deleted by hand. One manual copy of the database, made on 1 October 2026 before an upgrade, has no expiry date yet.
DSI-04	Can the vendor confirm deletion in writing?	**Yes**	On request, DIANO confirms in writing what was deleted and when, and what is still kept and until when.
SEF-01	Is there a written incident response procedure?	**Yes**	DIANO's incident steps are written down: contain the problem, find out what was affected, tell the companies affected, fix it, and write up what happened.
SEF-02	Will the customer be told about a security	**Partly**	If DIANO learns of a security compromise affecting your records, DIANO will tell you, and the Information Regulator as POPIA section 22 requires. The draft Operator Agreement proposes that DIANO tells you as soon as it has

ID	Question	Answer	Detail
	compromise, and how fast?		reasonable grounds to believe your records were reached by someone without permission, and in any case within 24 hours. An operator must have a written contract with the responsible party and must tell it immediately if there are reasonable grounds to believe personal information was accessed by someone without permission. (POPIA, Act 4 of 2013, section 21.)
SEF-03	Is there a public status page and incident history?	**Partly**	DIANO does not have a public status page yet. Service notices are sent by e-mail. Planned — target November 2026: A public status page.
SEF-04	Have there been security incidents in the past?	**Yes**	On 17 October 2026 DIANO found that a new purchase order could look saved while it had not reached the server, if the page did not yet know the user's role. It was fixed on the live system on 18 October 2026: DIANO now waits for the role, refuses out loud, and reads each new purchase order back from the server. One more incident, found and fixed by DIANO, is waiting for a review by DIANO's lawyer. After that review it is listed here.
SEF-05	How can a security problem be reported?	**Answered**	To report a security problem, e-mail info@diale.co.za with "Security" in the subject line. Planned — target November 2026: A dedicated address for security reports: security@diano.co.za.
TVM-01	Is the server runtime supported and patched?	**Yes**	DIANO's server code runs on Node.js 24, a supported version, and Google applies security updates to it automatically.
TVM-02	Are third-party libraries scanned for weaknesses automatically?	**Planned**	Software libraries are updated by hand when DIANO releases changes. There is no automatic alert for weak libraries yet. Planned — target December 2026: Automatic alerts for weak software libraries.
TVM	Are changes tested before release?	**Yes**	New work is tested on a separate test system (staging) before it goes live. The database rules are checked against hundreds of test cases before every rules release. Releases

ID	Question	Answer	Detail
-03			go through a deploy guard: a tool that builds from a recorded version, runs the checks first and stops if anything differs from what was reviewed.
TVM-04	Is there monitoring and alerting?	**Partly**	The platform owner gets e-mail alerts if the audit trail misses a change or its functions fail. There is no automatic check yet that warns when DIANO is down.
TVM-05	Are browser security headers (such as CSP) set?	**Planned**	Some browser safety settings, such as a content security policy, are not switched on yet. Planned — target December 2026: More browser safety settings are switched on, such as a content security policy.
PHY-01	Does the vendor run its own servers or data centres?	**No**	DIANO has no servers of its own. Your records are kept in Google's data centres.
PHY-02	How are the data centres physically protected?	**Answered**	Google guards its data centres with several layers of security. They include fences, guards, cameras, metal detectors, vehicle barriers and biometric checks.
PRV-01	What is the vendor's role under POPIA?	**Answered**	For the records you keep in DIANO, your business is the responsible party and DIALE Consulting is the operator.
PRV-02	Who is the Information Officer?	**Answered**	DIALE Consulting's Information Officer is Jonathan Diale (Director). Contact: info@diale.co.za, 087 265 3889.
PRV-03	Is there an operator agreement (DPA)?	**Planned**	A draft Operator Agreement is ready for review by DIANO's lawyer. It is not signed or in force yet. Planned — target November 2026: The Operator Agreement is reviewed by a lawyer and offered to every company.

ID	Question	Answer	Detail
PRV-04	How are requests from data subjects handled?	**Partly**	The draft Operator Agreement says DIANO passes on to you any request from your customers or staff about their personal information, and helps you answer it. For DIANO's own records about you, you can ask the Information Officer for access, correction or deletion, and you can complain to the Information Regulator.
PRV-05	Is personal information sold or used for marketing?	**No**	DIANO does not sell personal information and does not use your records for marketing.
PRV-06	Is personal information sent outside South Africa?	**Yes**	Files you upload, such as your company logo, signatures and stored documents, are kept in Google's us-east1 region in the United States. Sign-in is handled by Firebase Authentication, which Google runs only from data centres in the United States. It holds each user's name, e-mail address and a protected form of the password, not your business records. One more copy of the nightly backup is kept in Google's europe-west1 region in Belgium, in case the whole South African region fails. Personal information may be sent to another country only under the conditions of POPIA section 72, for example where the receiver is bound by rules that protect it as well as POPIA does.

Sources

- South African law says information does not lose its legal force just because it is electronic. (ECTA, Act 25 of 2002, section 11.) https://www.gov.za/sites/default/files/gcis_document/201409/a25-02.pdf (checked 2026-10-19)
- A court may not refuse an electronic record just because it is electronic, and must give it due weight. To judge its weight, the court looks at how reliably it was made, stored and sent, how its integrity was kept, and how the person who made it was identified. (ECTA section 15(1) to 15(3).) https://www.gov.za/sites/default/files/gcis_document/201409/a25-02.pdf (checked 2026-10-19)
- A record made in the ordinary course of business, or a copy certified as correct by an officer of the business, can be used in court as proof of its contents unless someone proves otherwise. (ECTA section 15(4).) https://www.gov.za/sites/default/files/gcis_document/201409/a25-02.pdf (checked 2026-10-19)
- Electronic records meet a duty to keep records if they stay readable, stay in their original format or one shown to be accurate, and show where they came from and when. (ECTA sections 14 and 16.) https://www.gov.za/sites/default/files/gcis_document/201409/a25-02.pdf (checked 2026-10-19)
- Tax records must be kept for 5 years after the return is submitted, and longer during a SARS audit, objection or appeal. (Tax Administration Act 28 of 2011, sections 29 and 32; VAT Act section 55.) https://www.sars.gov.za/lapd-lprim-act-2012-01-tax-administration-act-2011 (checked 2026-10-19)
- SARS's rule says electronic tax records must be kept at a place in South Africa, unless a senior SARS official gives permission to keep them elsewhere. (Government Notice 787 of 1 October 2012, rule 4, made under Tax Administration Act section 30.) https://www.sars.gov.za/gen-gen-23-pol02-manage-taxpayer-record-retention-authorisation-external-policy (checked 2026-10-19)
- Company records and accounting records generally have to be kept for 7 years. (Companies Act 71 of 2008, sections 24 and 28.) https://www.gov.za/documents/companies-act (checked 2026-10-19)
- Employers must keep records of each employee's time worked and pay for 3 years. (Basic Conditions of Employment Act 75 of 1997, section 31.) https://www.gov.za/documents/basic-conditions-employment-act (checked 2026-10-19)
- An operator must have a written contract with the responsible party and must tell it immediately if there are reasonable grounds to believe personal information was accessed by someone without permission. (POPIA, Act 4 of 2013, section 21.) https://www.gov.za/documents/protection-personal-information-act (checked 2026-10-19)
- The responsible party must tell the Information Regulator and the people affected as soon as reasonably possible after a security compromise is found. (POPIA section 22.)

https://www.gov.za/documents/protection-personal-information-act (checked 2026–10–19)
- Since 1 April 2025 the Information Regulator requires security compromises to be reported through its eServices portal, and the Information Officer must be registered there first. https://inforegulator.org.za/wp-content/uploads/2025/04/MEDIA-STATEMENT-INVITATION-TO-REPORT-SECURITY-COMPROMISES-THROUGH-THE-eSERVICES-PORTAL-.pdf (checked 2026–10–19)
- Personal information may be sent to another country only under the conditions of POPIA section 72, for example where the receiver is bound by rules that protect it as well as POPIA does. https://www.gov.za/documents/protection-personal-information-act (checked 2026–10–19)
- Google Cloud's list of certificates and reports. https://cloud.google.com/security/compliance/offerings (checked 2026–10–19)
- Firebase's privacy and security page, with its certificates per service and where each service runs. https://firebase.google.com/support/privacy (checked 2026–10–19)
- How Google encrypts stored data. https://docs.cloud.google.com/docs/security/encryption/default-encryption (checked 2026–10–19)
- How Google secures its infrastructure and data centres. https://docs.cloud.google.com/docs/security/infrastructure/design (checked 2026–10–19)
- Google's data-centre security page. https://datacenters.google/advancing-security/ (checked 2026–10–19)
- Google Cloud's Data Processing Addendum. https://cloud.google.com/terms/data-processing-addendum (checked 2026–10–19)
- Google Cloud's own list of sub-processors. https://cloud.google.com/terms/subprocessors (checked 2026–10–19)
- Google Cloud's POPI Act page. https://cloud.google.com/security/compliance/south-africa-popi (checked 2026–10–19)
- Anthropic's commercial terms. https://www.anthropic.com/legal/commercial-terms (checked 2026–10–19)
- PayFast's security page. https://payfast.io/security-fraud/ (checked 2026–10–19)
- The Information Regulator (South Africa). https://inforegulator.org.za (checked 2026–10–19)