SECURITY, PRIVACY AND DATA HANDLING

The boundaries are *architectural.*

Most benefits platforms describe their privacy position as policy. Ours is mostly structure: the data we would have to protect is largely data we chose not to hold, what we must hold to do the job is held for as long as the job takes and no longer, and the rest is separated by the database rather than by the application.

What we hold — and what we don't

Data	Who can see it	Enforced by
Member record — name, date of birth, nationality and residence, with the employer's own reference and the date cover began, plus dependants where the policy covers them. **No medical information, and no claimant detail.**	The member; their employer's HR administrator	Row-level security
Request details — the name, date of birth, nationality and country an insurer needs to action a change. Held on the request, **not on the member record**, and purged once it is settled.	The HR administrator who submitted it; the placing broker; Deronda	Row-level security + retention
Claims — insurer-reported, administrator-entered	Deronda; the placing broker. Employers as aggregates only	Row-level security + API shape
Commission terms	The client and the broker. Never the fund	Row-level security; append-only table
Portfolio financials	The fund, only where the company has consented	Row-level security, gated on a client-owned flag
Assistant conversations	The member; Deronda for audit. Never the employer	Row-level security + full logging

Tested, not asserted

Every boundary above is covered by an automated test. As at the version date on this sheet there are **70 such tests and all of them pass**, run against the live database and, in CI, against one rebuilt from our own migrations. A failing test is a blocking defect.

Examples: an HR administrator cannot read another company's data, see individual claims, or re-point a member's account; a consultant sees only clients assigned to them; a fund sees no financial detail without consent; a member sees only their own record.

The record is append-only

The commission ledger and the audit log cannot be updated or deleted by anyone, including us and including privileged database connections. Corrections are superseding entries and both versions stay visible. This is a trigger and a missing grant, not a rule we follow.

Row-level security decides which rows a session may read; column grants decide which fields it may write. An HR administrator can turn data sharing on and cannot alter their commission rate.

Personal data, and what is done with it

A member's record holds their name, date of birth, nationality, residence, reference and start date — what an insurer requires to put somebody on cover — plus dependants where the policy covers them. The employer and the assigned broker both see it, because both administer the cover. **No medical information, and no claimant detail.** Claims reach either of them as aggregates only, withheld below three. Nothing records what a member reads or asks, and no assistant exchange reaches either of them.

Infrastructure

- Data hosted in London (eu-west-2)
- Encrypted in transit and at rest
- Managed Postgres with point-in-time recovery
- No analytics, no advertising pixels, no third-party trackers

Access

- Role comes from the database, never the browser
- Members set their own passwords; nobody else sees them
- Invitations are single-use, expire in 14 days, stored as a hash
- Every material write is mirrored to the audit log

Artificial intelligence

AI is used in one place: an assistant on the member surface, answering on that member's own cover from a prompt built server-side from their own record. Every response is scope-checked before it is shown, and anything straying into general medical or financial advice is blocked and replaced with a hand-off to a person.

There is a kill switch, global and per-client. Every exchange is logged, blocked ones as visibly as answered, and no client data trains any model.

Assurance — status today

- **Cyber Essentials** — in progress
- **Independent penetration test** — scheduled
- **Independent code and security review** — scheduled
- ISO 27001 — not held. Would follow a client requirement rather than precede one

We will publish outcomes when each completes. We would rather tell you what is in progress than imply what is not.

SECURITY QUESTIONS

Send diligence questionnaires to hello@deronda.works and they will be answered by the person who wrote the code, not a form.