



// THE SHORTEST POSSIBLE DATA STORY

Nothing survives the 24-hour window.

The test access is built so that there is as little to protect as possible. **No test content is stored, no application data is collected, and the access record itself is erased once the 24-hour window closes.** What the session produced lived in memory and ends with the process.

THREE PROPERTIES THAT DO THE WORK

The password *untergeht*

The test password never leaves the neural network / RA. It is not forwarded, not mirrored, not written to any store the gate can reach. It **goes down with the instance** — German: *es geht mit unter*. When the instance stops, the valid relation stops existing; no artefact is left behind from which it could be reconstructed.

Sessions live in RAM only

The Doorman keeps no server-side session file. Seat, source IP, expiry and session id exist as a signed cookie on the tester's side and in memory on the operator's side. **Closing the two windows ends everything** — no residue, no cache, no queued job, no autostart that brings it back.

Deletion after 24 h

A seat runs 24 hours from first login; an unredeemed code expires after 24 hours. Once the window closes the seat is closed and its access record — code, password hash, optional TOTP secret, bound IP — is **deleted**, not archived. Nothing is carried over into a next test round.

PLEASE DO NOT USE REAL CREDENTIALS

Use throwaway passwords and throwaway files only. Enrol the test vault with a password you have never used anywhere else and will never use again, and seal only files you would be comfortable losing. The test instance is a research build under active development, not a hardened production system — it carries no availability promise, no backup and no recovery path. A restart destroys the enrolment by design.

GDPR — WHAT IS PROCESSED, AND WHY

- ▶ **Controller:** Trauth Research LLC · GeoFold AI · info@trauth-research.com. Contact for every request below is that address.
- ▶ **Purpose:** operating and securing a time-limited external test access.
Legal basis: Art. 6(1)(b) GDPR for the test participation you asked for, and Art. 6(1)(f) for the security measures — the legitimate interest being to keep an unpublished research instance from being accessed by anyone else.
- ▶ **Categories:** access code, bcrypt password hash, optional TOTP secret, the IP address bound at first login, timestamps, seat status and lock reason, and login-attempt log entries (time, IP, result). That is the complete list.
- ▶ **Never processed:** no plaintext passwords, no content from the application, no test data, no files, no telemetry, no profiling, no advertising, no third-party analytics and no cookies beyond the one signed session cookie the access itself requires.
- ▶ **Retention:** 24 hours per seat, then deletion. Security log entries are kept only as long as needed to investigate a lockout and are erased with the test round.

PROCESSING, TRANSIT AND YOUR RIGHTS

- ▶ **Where:** the Gate runs on shared hosting at IONOS (Germany); the instance runs on the operator's own machine. Traffic transits a Cloudflare Quick Tunnel, which carries the encrypted connection but is not a storage location for the data above.
- ▶ **Recipients:** none beyond those infrastructure providers acting as processors. No data is sold, shared or handed to third parties for their own purposes.
- ▶ **Your rights:** access (Art. 15), rectification (16), erasure (17), restriction (18), portability (20) and objection (21) — exercised by e-mail to the controller. Given the 24-hour retention, an erasure request will usually find the record already gone.
- ▶ **Complaints:** you may lodge one with your competent supervisory authority.
- ▶ **Voluntary:** participation is voluntary and can be ended at any time by simply not logging in again; the seat then expires on its own.

This page is an information notice for the test programme, not a substitute for the full privacy policy on geofoldai.com. In case of doubt the published policy and the written test agreement prevail.

Threat model, protocol design (handover token, heartbeat signature, nonce handling, key fingerprint) and the reference implementation of Gate and Doorman were developed together with a frontier language model (Anthropic Claude, Opus class) and verified in an automated end-to-end series of **58 checks**: login paths, 2FA setup and choice, token replay, path blocks, foreign IP, remote shutdown, heartbeat authentication, tester and admin lockouts including the unlock path. Domain requirements, architectural boundaries and the separation of application, interface and NN are the operator's.