INTERMIND

# Security & Data Protection

Where meeting data goes, at every hop — and what we do not have

**Version date:** —

**Service operator and contracting entity:** Golden Fish CSP LLC (UAE)

**Publisher and IP owner:** MindMeeting OÜ (Estonia)

**EU representative (Art. 27 GDPR):** MindMeeting OÜ, Juhkentali 8, Tallinn 10132, Estonia

**Contact:** privacy@mind.com · intermind.com/trust

**Entity.** Service Operator and Contracting Entity: Golden Fish CSP LLC (UAE). Publisher and Intellectual Property Owner: MindMeeting OÜ (Estonia). EU/EEA representative under Article 27 GDPR: MindMeeting OÜ, Juhkentali 8, Tallinn 10132, Estonia — privacy@mind.com.

---

## 1. What InterMIND is, in data terms

InterMIND is a browser and mobile meeting product with realtime speech translation. In processing terms it does four things with customer content:

1. **Carries meeting media** — audio and video, in transit, over WebRTC.
2. **Turns speech into text** — word-level transcripts, and translated voice audio streamed back to participants.
3. **Stores meeting artifacts** — transcripts, chat, attachments, documents, and recordings when a host chooses to record.
4. **Runs AI over meeting content** — post-meeting summaries, shared-document summaries.

The security posture below is organised around those four flows, because that is where customer personal data actually lives.

---

## 2. Where data goes — every hop

InterMIND runs on EU infrastructure across France, Germany and Ireland. Each hop and its region:

| Hop | Provider | Region | Evidence |
|---|---|---|---|
| Web app and API | Vercel | Frankfurt ( `fra1` ) | `vercel.json:2` |
| Realtime server — chat, presence, transcript words in transit | Fly.io | Paris ( `cdg` ) | `fly.toml:6` |
| Meeting media, speech recognition, live voice translation | Own engine (Mind API, intra-group) | OVH, France | Engine hosted FR/DE; ws-server pinned `cdg` for the short route |
| Post-meeting AI summaries, document summaries | Mistral | EU API, zero data retention | Hard pin in every call site (§3) |
| Document translation | DeepL | Cologne, Germany | Contractual (DeepL DPA); not pinned in code |
| Database | Neon (Postgres) | Frankfurt (AWS `eu-central-1` ) | Verified via `neonctl` 2026-08-16 |
| Recordings, attachments, documents | Tigris object storage | EU multi-region (Frankfurt + Amsterdam) | Bucket `object_regions: eur` set 2026-06-10 |

| Hop | Provider | Region | Evidence |
|---|---|---|---|
| Transactional and inbound email | Resend | Ireland ( `eu-west-1` ) | Contractual claim, reviewed 2026-06-17 |
| Product analytics | PostHog | EU Cloud | `https://eu.i.posthog.com` hard-coded in all four clients |
| Error monitoring | Sentry | EU (Germany) | `*.ingest.de.sentry.io` |
| Cache / pub-sub | Upstash Redis | Frankfurt | Contractual claim, reviewed 2026-06-17 |

**Stated plainly:** some of these providers are US-domiciled companies operating EU regions. We do not claim otherwise and we do not disqualify them on that basis. Each transfer is covered by a DPA plus Standard Contractual Clauses and/or the EU–US Data Privacy Framework. The full registry is published at intermind.com/legal/subprocessors.

**One scoping caveat, stated rather than hidden:** the object-storage EU pin was applied 2026-06-10 and is forward-only. Objects written before that date remain where they were originally placed. For a contract that must promise EU-only storage *including history*, that legacy tail is rewritten before signature rather than papered over.

---

## 3. AI on customer content

This is the flow buyers ask about first, so it is stated precisely.

- **Speech recognition and voice translation run on our own engine**, hosted at OVH in France. This is not a third-party AI cloud — it is intra-group infrastructure (MindMeeting OÜ).
- **Every AI call on meeting content is pinned in code to Mistral's EU API with zero data retention.** The pin is `only: ["mistral"], zeroDataRetention: true`, present at every one of the four call sites — post-meeting digest, shared-document summary, editor assistance, and support reply drafting. This is a hard-coded constraint on each call, not a policy someone has to remember. Prompts are not stored by the provider and are not used for training.
- **Document translation** goes to DeepL (Cologne) under a DPA that excludes training use.
- **No meeting audio is ever stored.** Speech persists as text only. Translated voice audio is streamed to participants and never written to disk. This was verified by searching every audio-mime and upload path in the codebase.
- **Recordings do exist when a host records.** The mp4 is written as a *private* object and deleted with the session's artifacts or with the account. We never claim "we don't record" — we claim the recording is private, host-controlled, and deletable.

**Scope of these claims: meeting content.** Our public documentation chat widget and the public translation-benchmark demo send visitor-typed text to non-EU models without a ZDR flag. That is a deliberate, documented decision for volunteered input to public widgets, not an oversight, and it is why every AI claim above is scoped to meeting content rather than stated blanket.

## 4. What is stored, and for how long

| Data | Retention |
|---|---|
| Meeting audio and video | Not stored. If the host records, the mp4 is a private object kept until the host deletes the session's artifacts or the account is deleted |
| Transcripts, chat, documents | Kept until deleted by the user, host, or account deletion. **There is no automatic age-based expiry** — stated plainly rather than implied |
| Guest accounts | `expireAt` set to creation + 24h; hard-deleted by a sweep that runs every 6 hours. Worst-case lifetime ≈30h, and we state it that way rather than as a flat "24 hours" |
| Calendar and drive OAuth tokens | Encrypted at rest (AES-256-GCM); removed when the integration is disconnected |
| Unreferenced chat attachments | Swept daily, 48 hours after they become unreferenced |
| Expired sign-in codes | Swept every 6 hours |
| Account data export | ZIP with a 7-day TTL |

**Deletion is a hard delete, not a flag.** Account deletion is email-confirmed and runs in a fixed order: object-storage blobs are removed first, then recordings and previews, then a transactional database cascade, then the billing customer at the payment provider is deleted. Hosts can irreversibly delete a single session's artifacts without deleting the account.

**Data portability.** A full account export is self-service and produces open formats — no support ticket, no request form.

## 5. Access control and cryptography

- **No passwords are stored.** Authentication is OIDC (Google, Microsoft) or one-time email codes. There is no password database to breach.
- **Transport is encrypted everywhere** — HTTPS and WSS with no plaintext fallback.
- **Encryption at rest** is provided by the database and object-storage platforms. OAuth integration tokens carry an additional application-layer encryption (AES-256-GCM) on top of that.
- **Roles are assigned server-side.** Participant roles are resolved on the server; the client cannot assert its own privilege level.
- **Webhook authenticity is verified** for every inbound provider webhook, and the inbound-email endpoint is deny-by-default: with its signing secret unset, the endpoint is locked rather than open.
- **Object ACLs are re-asserted, not assumed.** A sweep runs every 5 minutes flipping recording and transcript blobs to private, so a mis-set ACL is corrected rather than persisting.

## 6. Monitoring, and what our telemetry deliberately does not see

- **Error monitoring** (Sentry, EU) carries explicit content-leak guards: transcript content is excluded from error payloads by design, and infrastructure errors are logged as codes rather than message bodies.
- **Product analytics** (PostHog, EU Cloud) is opt-out by default and gated behind a consent management platform. Session recording is off by default and inputs are masked.
- **Availability monitoring** probes each core service path continuously from an EU region and publishes results publicly at status.intermind.com — the SLA commitment is externally verifiable rather than self-reported.
- **Audit events survive account deletion by design** — the audit table intentionally holds no foreign key to the user, so an erasure request cannot silently destroy the security audit trail.

---

## 7. Change control and resilience

- **Every change passes an automated gate** before it can reach production: lint, a unit suite of ~4,500 tests, and integration and smoke suites run against a real preview deployment.
- **Schema changes are enforced backward-compatible.** A CI gate blocks drops, renames, NOT-NULL additions and type changes on new migrations, so a rolling deploy or a rollback never meets a schema it cannot read. A genuine contract step requires an explicit, reviewed exemption.
- **Production deploys are smoke-tested and roll back automatically** on smoke failure.
- **Backups.** The managed database platform provides point-in-time recovery. Object storage keeps continuous object versions on both buckets, queryable to an arbitrary point in time, and the restore procedure was exercised end-to-end on staging (2026-05-15) across all three recovery models rather than being documented and left untested.

---

## 8. What we do not have yet

Stated directly, because a procurement reviewer will find out anyway and a straight answer is worth more than a hedge:

- **No ISO 27001 and no SOC 2.** We do not hold them. We also do not write "in progress" — we will not use that phrase until an audit has actually started.
- **No formal written information-security policy set** (security policy, incident-response plan, security-awareness training, background-check procedure) as standalone approved documents. The technical controls described above are real and verifiable; the governance paperwork around them is not yet written. Our completed CAIQ answers this "No" question by question rather than implying otherwise.
- **No third-party penetration test** on record.

What we offer in place of certificates is **verifiability**: the claims in this document are enforced in code and configuration, our subprocessor registry is public, our uptime is publicly measured, and our completed

CAIQ is available for review.

## 9. Regulatory position

- **GDPR.** We act as processor for customer content; the controller is the customer organisation. A DPA reflecting Article 28(3) is available. An Article 30 record of processing activities is maintained internally. Erasure and portability are implemented as self-service endpoints, not manual processes.
- **EU AI Act (Regulation 2024/1689).** InterMIND's AI does speech recognition, translation, and meeting summarisation. None is a prohibited practice, and none falls under an Annex III high-risk use. We do not perform biometric identification or categorisation, and we do not perform emotion recognition — the engine transcribes and translates what is said; it does not profile who says it. Transcription, translation and AI recaps are explicit features a user switches on, not silent processing.
- **NIS2.** We are below the entity thresholds and are not a regulated entity under NIS2. Customers who *are* in scope pass their obligations down through vendor questionnaires; our readiness to answer those — this document, the completed CAIQ, the DPA and the public subprocessor registry — is what our NIS2 coverage consists of. We do not claim to be NIS2-certified, because no such certification exists.
- **Payments.** Card data never touches InterMIND servers. Checkout and card handling are fully hosted by our payment providers (Stripe; Paddle as merchant of record in selected countries).

## 10. Contact

Security questions, questionnaire requests, or a signed copy of the DPA and transfer safeguards: **privacy@mind.com**.

Vulnerability reports are accepted at the same address and are read by an engineer, not a ticket queue.