

Aristo — Compliance Pack (v1, 2026-07-10)

The four papers procurement asks for, in one file (split + letterhead at send time). Every claim below is true of the shipped platform today; nothing aspirational is stated as present. (Blind spot #3; SOC 2 certification itself is a separate money decision — posture stated honestly below.)

1 • Data Processing Addendum (DPA) — core terms

- **Roles.** Customer = data controller. PhoenixHalo Inc. (Aristo) = processor.
- **What is processed.** Read-only Microsoft Graph aggregates: Copilot usage signals, license inventory, Message Center posts, directory department groupings; user principal names for licensed users (lowercased identifiers, no message content); Teams conversation references for users who talk to Aristo; the user's own answers to Aristo's questions. **Never processed:** email/file/chat content (unless the customer explicitly enables the optional inbox capability, scoped by their own Exchange Application Access Policy — OFF by default, fail-closed).
- **Purpose limitation.** Solely to operate the customer's Copilot-adoption service. **No training of AI models on customer data. No sale, sharing, or secondary use. Ever.**
- **Security measures.** Read-only Graph scopes; k-anonymous (≥ 5) aggregation on every leader surface; encryption in transit (TLS 1.2+) and at rest (Azure-managed); admin-curated role gating (leadership views); audit trail on operator actions; per-user erasure ("forget me") honored immediately.
- **AI inference boundary.** Inference runs on Azure (Azure OpenAI) inside the Microsoft boundary by DEFAULT. Cross-boundary fallback (Anthropic) is disabled unless the customer explicitly opts in per tenant (fail-closed).
- **Subprocessors.** Per §2; changes notified 30 days ahead.
- **Deletion.** On termination or on request: full tenant purge per §3 with written attestation within 30 days.
- **Breach notice.** Without undue delay, within 72 hours of confirmation.

2 · Subprocessor list (as of 2026-07-10)

Subprocessor	Purpose	Data reached	Region
Microsoft Azure (Container Apps, Cosmos DB, ACR)	Hosting + data store	All processed data	East US 2 (store geo-redundant)
Azure OpenAI (Microsoft)	AI inference (default path)	Prompt content composed from aggregates	Azure boundary
Anthropic	AI inference fallback — per-tenant explicit opt-in only; disabled by default	Same as above, only when opted in	US
Cloudflare	Public website (phoenixhalo.com) only	No customer/tenant data	Global edge
GitHub (Microsoft)	Source code hosting	No customer data	US

3 · Retention & tenant-offboarding attestation

- **Cold-cohort documents auto-expire at 30 days** (TTL on the record) — a "who's cold" list never lingers.
- **Per-user erasure:** any user can say "forget me" to Aristo; their lifecycle, conversation reference, and personal records are deleted immediately.
- **Tenant offboarding:** on request, ALL tenant-partitioned records (registrations, configs, plans, runs, wins, cohort, agent packages, conversation references) are purged; a signed deletion attestation letter is provided. Backups age out fully within the backup retention window thereafter.
- **What survives offboarding:** nothing tenant-identifiable. Aggregate, de-identified operational metrics (e.g., "N tenants used feature X") only.

4 · Security & SOC 2 posture statement (honest)

- **Today:** not SOC 2 certified. Controls in operation: least-privilege read-only scopes; default-deny leadership gating (admin-curated, never self-asserted titles); k-anonymity ≥ 5 on all people-adjacent views; fail-closed cross-boundary AI egress; operator audit trail; secrets in platform vault (never in code); every deploy from version-controlled source; documented backup/DR runbook with stated RPO/RTO; public /status page running real per-request checks.

- **Roadmap:** SOC 2 Type I engagement is a commercial decision scheduled with our first enterprise contracts requiring it (typical timeline 3–4 months from engagement).
 - **Verification offered:** the live security-review page (posture + exact scopes + real grant state) at `/trust/review`; architecture walk-through with the customer's security team on request.
-

5 · HR & works-council note (blind spot #6 — ships with this pack for EU-touching customers)

- **What employees experience.** Aristo sends at most ONE gentle, role-relevant Copilot suggestion per day, only to employees whose seat is inactive; anyone can say "stop" once and is never messaged again (the pause is not logged against them and is invisible to leadership). No individual usage is ever shown to managers — every leadership view is aggregate and k-anonymous (five or more).
- **What Aristo is not.** Not monitoring, not scoring individuals, not a performance tool. It cannot answer "how is employee X doing" — by design, for anyone.
- **Per-geo defaults.** Proactive outreach can be disabled org-wide or scoped to a pilot group (both are existing tenant controls); for works-council jurisdictions (e.g., Germany), recommended rollout = information session → pilot group opt-in → org-wide, with this note attached to the consultation file.
- **Data:** see §1–§3 — read-only, aggregate, erasable, never trained on.