EVERSCOPE

PREFILLED SECURITY QUESTIONNAIRE

Generated 2026-08-03T22:00:11.155Z | Version 1.0

1. What does Everscope process?

Power BI and Microsoft Fabric metadata, deterministic findings, ownership and governance workflow records. It never requests dataset rows or customer query results.

2. Can Everscope change our Microsoft tenant?

No. Product behaviour is read-only. Everscope never modifies or deletes customer Microsoft content.

3. How is tenant isolation enforced?

Every customer query is resolved from the authenticated connection and tenant identifier. Tenant isolation checks run in CI and tenant tables use row-level-security protection.

4. Where is production processing?

Application and worker workloads run in Amsterdam. The primary managed PostgreSQL project is configured in the EEA. Transactional email and billing use the published subprocessors and transfer safeguards.

5. How are Microsoft credentials protected?

The MSAL token cache is encrypted before database storage. Disconnecting Microsoft deletes the connection record and encrypted token material immediately.

6. What is retained?

Anonymous scan results: 7 days. Completed tenant scans: 730 days. Failed scans and account project scans: 90 days under the current production setting. Exact category-level retention is published in the Trust Center.

7. Can customers export and delete data?

Yes. A machine-readable JSON export is available in account settings. A separate two-step deletion flow removes customer records and Microsoft tokens and records privacy-preserving completion evidence.

8. Are rules reproducible?

Yes. One deterministic C# rule engine is used. Every finding records the rule ID, rule version and bundle version; reproducibility tests run in CI.

9. Does Everscope use AI for findings?

No. Finding logic makes no AI or LLM calls. The same metadata and rule bundle produces the same result.

10. Which subprocessors are used?

Fly.io, Supabase, Microsoft, Stripe and Resend. Their function, data categories and countries/regions are maintained at everscope.app/subprocessors.

11. Which certifications are currently held?

Everscope does not currently claim SOC 2 or ISO 27001 certification. Current controls and roadmap status are stated plainly in the Trust Center.

12. How can access be revoked?

An authorised user can disconnect Microsoft in Settings. This deletes the stored connection and encrypted token cache immediately; Microsoft administrators can also revoke enterprise-app consent in Microsoft Entra.

Current, machine-readable detail: https://everscope.app/security