Equalis OpsReg

Security architecture overview

Version 1.0 · 2 November 2026 · EqualisTech OpsReg Limited, CRO 814298

How Equalis OpsReg reads a customer's Azure subscriptions, where the platform runs, which controls protect customer data and how evidence is kept. Written from the published trust centre and product pages; no internal system names.

1. Access model

The platform is read-only by design. It receives three built-in Azure reader roles on the subscriptions you choose and has no write permission. It pushes no policy and changes no resource, and no feature can be enabled to add that ability.

It reads configuration and security metadata through Azure Resource Manager and Azure Resource Graph, including the security recommendations and alerts Azure exposes for those resources. The roles grant no access to the data in your databases, storage accounts or virtual machines. The Reader role also allows queries on log data in Log Analytics workspaces in those subscriptions.

Access is revocable on demand from your own tenant, by removing the role assignments and deleting the enterprise application.

Roles	Reader, Security Reader, Cost Management Reader
Write permissions	None
Data read	Metadata only, never workload content
Azure credentials stored	None

2. Architecture

What runs where, and how data moves: configuration is read from your tenant, read-only, and findings go out only to the tools you connect.

Your Azure tenant

Subscriptions
From 1 to 50, each an audit scope

Role assignments (read-only)
Reader, Security Reader, Cost Management Reader

Multi-tenant application
Admin consent; access revocable on demand from your own tenant

Azure Resource Manager and Azure Resource Graph, read-only

Equalis OpsReg · Azure North Europe, backups in West Europe

Rule engine
437 versioned rules, five frameworks

Evidence store
Write-once records, kept for seven years while subscribed

Dashboards and PDF exports
Per framework, per subscription

Connectors

Microsoft Teams, Slack, Email, Jira, ServiceNow, PagerDuty, Webhook

Findings are sent to the tools your teams use

3. Roles granted

Three built-in reader roles, with no write access to your resources, scoped to the subscriptions you choose.

Role	Why it is needed
Reader	Read the configuration of all resources.
Security Reader	Read the security recommendations, alerts and security states Azure exposes for your resources.
Cost Management Reader	Assigned by the same template for a later capability; the current version reads no cost data. Like the other two roles, it grants no write access to your resources.

4. Hosting and data residency

Item	Location
Azure regions	North Europe (Ireland); geo-redundant backups in West Europe (Netherlands)
Transfers outside the EEA	None by EqualisTech, other than findings sent to the tools you connect. Microsoft documents limited cases in which the Microsoft services we use (Microsoft Azure, including the Azure Front Door edge network, Microsoft Entra External ID, Azure Communication Services and Microsoft 365) may process or access data outside the EU, for example for remote access by Microsoft personnel, global security operations and support; see the data processing agreement.
Legal entity	EqualisTech OpsReg Limited, Dublin, Ireland (CRO 814298)
Governing law	Irish law

5. Security controls

Tenant isolation

Row-level security in the database. Every query on customer data is filtered on the tenant identifier taken from the access token, never from the request body.

Network

Azure Front Door Premium with a web application firewall using Microsoft-managed rule sets (Default Rule Set and Bot Manager), in Prevention mode in production. In production, databases and storage sit behind private endpoints.

Identity

Microsoft Entra External ID for user sign-in and managed identities between platform services. Access to your subscriptions uses the multi-tenant application you consent to, which authenticates with a managed identity as its federated credential: no client secret, certificate or Azure credential is stored.

Evidence integrity

Write-once evidence records, seven-year retention while your subscription is active, evidence reports sealed with a cryptographic hash and tamper-evident audit logs.

Read-only by construction

The code contains no call that writes to your Azure subscriptions. The principle predates the first line of code: Inform, Don't Act.

Business accounts only

Sign-up requires an address on your organisation's own domain. Personal mailbox providers are refused.

6. Evidence integrity and retention

Records are written once and cannot be modified by the application or its users. They are kept for seven years while your subscription is active, and evidence reports are sealed with a cryptographic hash so that any later change can be detected.

Exports are produced per framework and per subscription, so the scope of a report always matches the scope of the audit.

Retention	Seven years while subscribed
Storage	Write-once
Report integrity	Hash-sealed
Export scope	One framework, one subscription
Format	PDF

7. Sub-processors

Sub-processors of the Equalis OpsReg platform at general availability. Customers are informed at least 30 days before any sub-processor is added or replaced and may object. The services used by this website are listed in the privacy policy.

Sub-processor	Service	Location
Microsoft Ireland Operations Limited	Platform hosting (Microsoft Azure), sign-in (Microsoft Entra External ID), notification email (Azure Communication Services) and support email (Microsoft 365)	European Union (platform in Ireland, backups in the Netherlands; other Microsoft services in EU data centres, with the limited exceptions Microsoft documents)

8. Reporting a vulnerability

If you believe you have found a security issue in Equalis OpsReg, write to security@equalistech.com with the details. We acknowledge every report and keep you informed until the issue is resolved.

Please do not access data that is not yours and do not degrade the service while investigating.