Equalis OpsReg

Data processing agreement

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

Summary

This agreement applies from general availability of the platform, planned for February 2027. Before general availability, any proof of concept involving a customer's Azure subscriptions is covered by a separate written agreement that includes Article 28 GDPR terms. For platform customers, EqualisTech OpsReg Limited acts as a processor of the Azure subscription metadata processed through the service, under Article 28 GDPR terms; account data is processed as a controller, as set out in the privacy policy. Data subjects: the customer's personnel and other individuals whose identifiers appear in Azure configuration (for example role assignments, resource tags and alert contacts). Personal data: names, user principal names, email addresses, object identifiers and IP addresses contained in that metadata (including security alerts) and in evidence records. Purpose: evaluating Azure configuration against the platform's rules and producing evidence and reports. Duration: the term of the contract. The key commitments:

- Location: platform data is processed and stored in Azure North Europe (Ireland), with geo-redundant backups in West Europe (Netherlands), and support correspondence is held in Microsoft 365 with data stored in the EU. EqualisTech makes no transfer outside the EEA other than delivering findings to the destinations the customer configures. Microsoft documents limited circumstances 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; these transfers are covered by the EU Standard Contractual Clauses in Microsoft's Data Protection Addendum. Findings are delivered only to the destinations the customer configures; where a connected tool stores findings is set by the customer's contract with its provider.
- Read-only access to customer Azure subscriptions; no customer Azure credentials stored. Connector keys supplied by the customer are encrypted in Azure Key Vault.
- Sub-processor: Microsoft Ireland Operations Limited, for platform hosting (Microsoft Azure), sign-in (Microsoft Entra External ID), notification email (Azure Communication Services) and support email (Microsoft 365), together with the Microsoft affiliates and sub-processors Microsoft lists for these services. We inform customers at least 30 days in advance of any intended addition or replacement of a sub-processor, and customers may object on reasonable grounds; if no solution is agreed, the customer may terminate the affected service. We impose on each sub-processor the same data protection obligations as those set out in this agreement and remain fully liable to the customer for its performance.

- Evidence records are write-once and never modified. While the contract is in force, each record is kept for seven years from its creation. At the end of the contract, the customer may retrieve its exports for 30 days; all customer personal data is then deleted, including from backups within a further 35 days, unless Union or Member State law requires storage.
- At general availability, technical and organisational measures include tenant isolation enforced at the database layer, managed identity authentication, private networking for data services, and a public surface protected by a web application firewall (Azure Front Door Premium).
- We process customer personal data only on the customer's documented instructions, including with regard to transfers, unless Union or Member State law requires otherwise, in which case we inform the customer first unless that law prohibits it; inform the customer immediately if, in our opinion, an instruction infringes data protection law; ensure that everyone authorised to process it is bound by confidentiality; implement the security measures required by Article 32 GDPR; assist the customer in responding to data subject requests and in meeting its obligations under Articles 32 to 36 GDPR; notify the customer of a personal data breach without undue delay after becoming aware of it, and in any event within 48 hours; and make available the information needed to demonstrate compliance, and allow for and contribute to audits.

Executing the DPA

The full DPA forms part of the terms of service and applies to every platform customer from account creation. Its full text, including the Article 28 clauses, the description of processing and the technical and organisational measures annex, is provided before you subscribe; a countersigned copy is available to customers and prospects on request: contact@equalistech.com.