

Unify - Service Definition Document

About this document

This document describes the Unify platform for G-Cloud 15 procurement.

What the service is

Unify is a data operations platform. It helps organisations manage data from multiple sources.

We deploy Unify to your own Microsoft Azure cloud account. This means you keep full control of your data.

What Unify does

Unify lets you:

- upload data files (CSV and Excel formats)
- validate data against business rules you define
- transform and process data automatically
- manage data through a web portal
- control who can access what data

How we deploy Unify

We deploy Unify entirely within your Azure account. You get dedicated resources that are not shared with other organisations.

Your deployment includes:

- web applications for the portal
- serverless functions for data processing
- databases for storing your data
- storage accounts for your files

- security and monitoring tools

No other organisation can access your resources or affect your performance.

Backup, restore and disaster recovery

Automatic backups

We configure automatic backups for all databases.

PostgreSQL databases keep backups for 7 to 14 days depending on environment.

Azure SQL databases keep backups for 7 to 21 days depending on environment.

Snowflake databases support time travel recovery for 7 to 21 days.

Storage accounts have soft delete enabled for file recovery.

Disaster recovery

All infrastructure is defined as code using Terraform. This means we can rebuild your environment quickly if needed.

Container images are stored in Azure Container Registry for fast recovery.

You can restore databases to any point within the backup period.

You can configure geo-redundancy for additional protection if required.

Onboarding support

Documentation

We provide documentation at our online portal. The address is unifydocs.vizify.co.uk.

Public documentation is freely available. It includes overviews and getting started guides.

Client documentation requires login access. It includes detailed deployment and administration guides.

Deployment support

We work with your Azure team to deploy Unify.

We offer remote onboarding sessions on request.

We provide guided walkthroughs for administrators and users.

Offboarding support

Unify runs in your own Azure account. You own all your data and infrastructure throughout the contract.

What happens when you leave

When the contract ends:

- You keep full access to all your data
- You keep full access to your infrastructure
- We revoke access to software updates
- We revoke access to client documentation
- Your existing deployment continues working

You do not need to extract data. You already own everything.

Service constraints

Maintenance

We deploy updates during business hours after internal testing.

We notify you before planned updates.

We may deploy emergency security patches outside normal schedules.

What you can customise

Through the web portal you can customise:

- business rules and validation logic
- portal branding and styling
- navigation menus
- user roles and permissions

At deployment you can choose:

- which database to use (Azure SQL, or Snowflake)
- which Azure region to use
- network security settings

Limitations

Unify works in web browsers only. There are no desktop or mobile apps.

Unify works on Azure only. We do not support other cloud providers currently.

We do not provide a public API for external systems.

The interface works best on desktop screens. Mobile access is limited.

Service levels

Availability

Unify uses Microsoft Azure services. These have the following availability targets:

- Azure App Service: 99.95 percent
- Azure Functions: 99.95 percent
- Azure SQL Database: 99.99 percent
- Azure PostgreSQL: 99.99 percent
- Azure Storage: 99.9 percent or higher

We do not offer a separate availability target for the application itself.

Support hours

We provide support Monday to Friday, 9am to 5pm UK time.

We do not provide routine weekend support. We address critical issues on a best efforts basis.

Response time

We typically respond to support queries within one hour during business hours.

After sales support

What is included

Support is included with your maintenance agreement. This covers:

- technical issue resolution
- configuration guidance
- product updates
- security patches
- deployment assistance

How support works

You contact us by email.

We verify your identity before discussing account details.

The developer who builds the platform handles support directly. This means quick responses and no escalation delays.

Incident handling

You report incidents by email.

We acknowledge and prioritise by severity.

We resolve critical issues first.

We provide post-incident summaries on request.

Technical requirements

What you need

To use Unify you need:

- an active Microsoft Azure subscription
- an Azure Active Directory tenant
- a modern web browser (Chrome, Edge, Firefox, or Safari)
- Azure permissions to deploy resources
- network access to Azure services

Supported browsers

We support Chrome, Edge, Firefox, Safari, and Opera.

We do not support Internet Explorer.

Supported file formats

For importing data we support CSV and Excel (XLSX) files.

For exporting data you can use CSV, Excel, or any format your database tools support.

We do not support ODF format.

Outage and maintenance management

How we report outages

Microsoft reports Azure infrastructure outages at status.azure.com.

You can configure Azure Service Health alerts in your Azure account.

You can configure email alerts using Azure Monitor.

We contact affected clients directly by email for application issues.

Monitoring access

You have direct access to Azure Monitor and Application Insights in your own account.

You can create custom alerts for any metrics you need.

Hosting options and locations

Cloud provider

We use Microsoft Azure only. We do not support other cloud providers.

Available regions

You can choose any Azure region for your deployment.

For UK public sector we recommend UK South or UK West regions.

European and other regions are also available.

Your choice

You specify the region when we deploy. All your resources go in that region.

Your data does not leave your chosen region.

Access to data on exit

You own your data

All data stays in your Azure account. We do not hold any of your data.

How to access your data

You can access your data using:

- database tools like Azure Data Studio
- Azure Storage Explorer for files

- Azure Data Factory for bulk exports
- any SQL compatible tools

After the contract ends

You continue to have full access to your data.

You can export or migrate data using standard Azure tools.

No extraction from us is needed because we never held your data.

Security

Data protection

All data in transit uses TLS 1.2 or higher encryption.

All data at rest uses AES-256 encryption.

Databases use transparent data encryption.

We store secrets in Azure Key Vault.

Authentication

Users sign in with their Azure Active Directory credentials.

You can require multi-factor authentication through your Azure AD settings.

We use role-based access control. Users only access what they are authorised for.

Physical security

Azure datacentres meet international security standards including:

- ISO 27001
- SOC 1, SOC 2, and SOC 3
- CSA Cloud Controls Matrix
- UK Cyber Essentials Plus

Our security practices

We scan all code changes for vulnerabilities using Snyk.

We review all code changes before merging.

We follow OWASP security principles.

We never store secrets in code.

Audit logs

All user actions are logged with timestamps and user identity.

You can access audit logs in real time through your Azure account.

Logs are retained for 30 to 90 days by default. You can extend this.

Current limitations

We have not completed formal penetration testing. This is planned for future.

We do not hold ISO 27001 certification for our application. Azure infrastructure is certified.

Document information

This document was prepared for G-Cloud 15.

Version 1.0

Date: January 2026