



Bramble Hub
Connecting SMEs and the Public Sector

Crown
Commercial
Service
Supplier

G-Cloud 15 Lots 2a&b

Bramble Hub

eXate Data Security Platform

Service Definition

Contact:

Geoff Couling

+44 (0) 20 7735 0030

contact@bramblehub.co.uk

Service Definition — eXate Data Privacy & Protection Platform

Service: Data Privacy, Protection, and Access Management Software (platform)

1. Service Overview

The **eXate Platform** is a distributed software platform that enables organisations to automate data privacy, data protection, and fine-grained access controls across structured and unstructured data environments. The service integrates discovery, policy enforcement, and audit capabilities to support secure and compliant data usage across internal systems and external integrations.

The platform supports protection of sensitive data:

- **In motion** (data flowing between systems or services).
- **At rest** (data stored in databases, files, or data lakes).
- **Through context-aware access controls** that enforce policies down to individual records or data attributes.

Deployment models include SaaS, on-premise, or hybrid hosting, allowing integration with existing infrastructure.

2. Scope of the Service

In scope

The eXate service includes the following core capabilities:

a. Data Discovery & Classification

- Automated discovery and classification of sensitive data across repositories.
- Intelligent tagging of data by sensitivity, jurisdiction, or regulatory category.

b. Policy Management & Enforcement

- Central policy repository for data handling and access rules.
- Automatic enforcement of data protection policies across APIs, databases, and applications.

c. Data Protection Mechanisms

- Fine-grained access control (attribute-based and role-based).
- Dynamic data masking, obfuscation, and encryption options.

d. Real-time Audit & Reporting

- Monitoring and logging of data access, policy application, and compliance status.

e. Data Sovereignty Controls

- Jurisdiction-aware policy enforcement to maintain control of data across geographic and regulatory boundaries.

f. Integration & Extensibility

- APIs and connectors for integration with enterprise applications, cloud platforms, and data pipelines.

Out of scope

- Custom software development services not part of the standard platform offering.
- Third-party infrastructure costs or managed hosting outside of the agreed hosting model.
- Manual compliance or consultancy services unless separately contracted.

3. Delivery Model

The eXate Platform is delivered as software deployed in one of the following models:

- **Software as a Service (SaaS):** Hosted and managed by the supplier.
- **On-Premise:** Installed within the customer's controlled infrastructure.
- **Hybrid:** Combination of SaaS, Cloud and on-premise components, depending on customer architecture.

Platform components operate via embedded controls that integrate with existing systems (e.g., API gateways, databases, application layers) to enforce consistent data protection policies.

4. Key Features & Capabilities

The service provides the following capabilities:

Data Privacy & Protection

- Protects sensitive data at attribute, record, and dataset level.
- Aligns data handling with organisational policies and regulatory requirements (e.g., GDPR, CCPA).

Centralised Policy-Driven Controls

- Unified policy engine for defining and enforcing rules across sources and consumers.

Access Governance

- Attribute-based and role-based access control to ensure only authorised access.
- Dynamic masking and obfuscation to enable safe data usage while preserving utility.

Auditability

- Logging and reporting of data access and policy application for compliance and oversight.

Sovereignty & Regulatory Support

- Controls that support data location and jurisdiction requirements in global operations.

5. Customer Responsibilities

To receive the service, the customer is responsible for:

- Providing access to relevant data sources for discovery, classification, and enforcement.
- Allocating internal resources for onboarding and configuration tasks.
- Ensuring network connectivity and compliance with security prerequisites for the chosen deployment model.
- Defining data protection and access policies in collaboration with eXate implementation resources.

6. Supplier Responsibilities

We will:

- Provide the eXate Platform software and associated documentation.
- Support onboarding, configuration, and initial integration activities.
- Offer standard product support aligned to the chosen support tier (details provided in the support schedule).
- Maintain the platform according to industry-standard security practices.
- Implement updates, patches, and upgrades in line with the supplier's product lifecycle.

7. Support & Service Management

Support services are available as part of the subscription/licence and include:

- **Helpdesk access** during published support hours.
- **Incident logging and tracking** via the supplier's support portal.
- **Maintenance and software updates** in accordance with product release policies.

Specific service levels (response times, escalation paths) will be provided in the supplier's **Support Schedule**, appended to this Service Definition as required.

8. Security and Data Handling

The eXate Platform is designed to meet recognised information security standards. The supplier holds **ISO 27001 and ISO 27701 certifications**, which provide a framework for secure management of information and privacy risk.

Data processed through the platform remains subject to customer governance and policy decisions, with controls designed to minimise exposure of sensitive information.

9. Onboarding & Offboarding

Onboarding

- Defined onboarding plan with milestones.
- Setup of policies, connectors, and security configurations.
- Knowledge transfer and handover to customer teams.

Offboarding

- Decommissioning configuration and secure extraction of metadata if required.
- Revocation of access and termination of hosted service accounts in line with contractual terms.

10. Dependencies & Assumptions

- Customer will provide authorised access to systems required for platform integration.
- Customer environment meets the technical preconditions for the selected deployment model.
- Any third-party infrastructure or cloud hosting services are provisioned and maintained by the customer where applicable.