



G-Cloud 15

Lot 2b: Software as a Service (SaaS)

Data and AI Platform

RM1557.15

Commercial – In Confidence | Subject to Contract

© Scout Group 2026. All rights reserved.

1. Service Overview

The Data and AI Platform is a unified, cloud-agnostic data, integration, and AI platform accelerator designed to support public sector organisations in securely ingesting, integrating, governing, analysing, and operationalising data. The service enables organisations to establish robust data and analytics capabilities quickly, without the need to design and build a platform from first principles.

The platform supports a wide range of analytical, reporting, and AI-enabled use cases while maintaining alignment with UK public sector security, data protection, and operational requirements. It is designed to operate across public, private, and hybrid cloud environments and to integrate with existing systems, data sources, and operating models.

2. Service Description

The Data and AI Platform provides a pre-configured architecture, tooling, and governance framework that accelerates the delivery of modern data and AI solutions. It reduces complexity and implementation risk by applying proven architectural patterns, security controls, and operational practices.

The service supports structured, semi-structured, and unstructured data and enables secure ingestion from multiple internal and external sources. Data can be integrated, transformed, and orchestrated to support analytics, reporting, and AI workloads. The platform is API-first, allowing it to integrate with existing applications, data sources, and services without requiring bespoke development.

The service is cloud-agnostic and can be deployed into the buyer's own cloud environment, ensuring that data ownership, residency, and control remain with the buyer at all times.

3. Service Scope

The Data and AI Platform supports the full end-to-end lifecycle of data and AI workloads. This includes data ingestion, integration, transformation, governance, analytics, and AI enablement.

The service provides capabilities to securely ingest data from multiple sources, including operational systems, third-party platforms, and external data feeds. Data can be processed using batch, near real-time, or streaming patterns, depending on buyer requirements. Integrated data governance controls ensure that data access, usage, and retention align with organisational policies and regulatory obligations.

Analytics and reporting capabilities support both operational and strategic decision-making, while AI and machine learning enablement allows organisations to develop, deploy, and operationalise models within controlled environments. The service can be used as a standalone platform or extended through optional add-ons and professional services.

The platform supports the full lifecycle of data and AI workloads as outlined below.

Capability Area	Description
Data Ingestion	Secure ingestion from internal and external data sources
Data Integration	Transformation, orchestration, and data movement
Governance	Access control, audit logging, and data policies
Analytics & Reporting	Dashboards, reports, and operational insights
AI & ML Enablement	Support for machine learning and AI workloads

4. Service Architecture and Design Principles

The service is designed using cloud-native and cloud-agnostic architecture principles to ensure flexibility, scalability, and portability. Deployments typically operate within the buyer's own cloud environment, allowing buyers to select their preferred cloud provider and maintain control over infrastructure, security, and cost management.

Each buyer operates within a logically and operationally isolated environment, ensuring that workloads, data, and resources are not shared across tenants. This isolation supports security, performance, and compliance requirements. The platform aligns with the shared responsibility model for cloud services, clearly defining supplier and buyer responsibilities.

The architecture is API-first and modular, enabling integration with existing systems and future extensibility without disruption to core services.

5. Intended Users and Use Cases

The Data and AI Platform is intended for public sector organisations seeking to improve their data management, analytics, and AI capabilities. Typical users include data and analytics teams, digital and transformation teams, operational teams, and innovation or AI teams.

Common use cases include enterprise reporting and analytics, data integration and consolidation, secure data sharing across teams or departments, and the enablement of AI and machine learning workloads. The service supports evidence-based decision-making by providing timely, reliable, and governed access to data and analytical insights.

Typical users and example use cases are outlined below.

User Group / Use Case	Description
Data & Analytics Teams	Enterprise reporting, analytics, and data modelling
Digital & Transformation Teams	Data integration and platform modernisation
Operational Teams	Performance monitoring and operational insights
AI & Innovation Teams	Development and deployment of AI/ML workloads

6. Deployment Models

The service supports deployment across public cloud, private cloud, and hybrid cloud environments. Deployments are typically configured within the buyer's own cloud tenancy, enabling buyers to align the service with their existing cloud strategy, security controls, and operational processes.

The platform is designed to operate consistently across deployment models, allowing buyers to scale workloads, adjust performance characteristics, and manage costs in line with organisational requirements.

7. Service Management and Monitoring

The Data and AI Platform provides service usage and operational metrics to support effective service management and optimisation. Metrics include service availability and uptime, performance and response times, data ingestion and processing volumes, and utilisation of analytics, integration, and AI components.

Security and operational metrics are also available, including access activity, authentication events, and error rates, subject to buyer configuration and permissions. Metrics can be accessed through real-time dashboards, APIs, and regular or on-request reports.

Service outages, incidents, and planned maintenance are communicated through agreed notification channels, including email notifications and service status dashboards. Where applicable, buyers can integrate service status information into their own monitoring and service management tools.

8. Onboarding and Offboarding

8.1 Onboarding

Onboarding begins with an initiation phase to confirm use cases, deployment model, security requirements, and success criteria. The supplier configures the service environment, access controls, and integrations in line with buyer requirements.

Users are supported through guided setup, training sessions, and comprehensive documentation. Training can be tailored to different user roles, including technical users, administrators, and business users. During early use, hypercare support is provided to address issues, answer questions, and support effective adoption.

8.2 Offboarding

At contract end, the service enters a managed offboarding phase. Supplier access to the service and associated tools is removed, and access revocation is confirmed. Documentation and operational artefacts are handed over to support continuity.

Optional extended transition support, additional documentation, or migration assistance can be provided by agreement as chargeable services.

9. Data Ownership and Exit Management

All customer data is stored and processed within the buyer's own cloud or hosting environment. The buyer retains full ownership and control of all data, schemas, configurations, and outputs throughout the contract term.

At contract end, buyers retain uninterrupted access to their data and may continue to use, migrate, or archive it independently. Where any supplier-managed configuration or operational metadata exists, this can be exported in standard, open formats. The supplier provides written assurance that no buyer data is retained outside the buyer's environment following contract termination.

10. Support Levels

Support for the Data and AI Platform is provided through tiered support levels aligned to buyer needs.

Standard Support is included in the service price and provides email and ticket-based support during UK business hours, along with access to documentation and knowledge resources. Enhanced Support offers extended support hours, phone support, prioritised incident handling, and access to a Technical Account Manager or Cloud Support Engineer at additional cost. Premium Support provides 24×7×365 support, proactive monitoring, accelerated incident response, and access to named technical resources, with pricing agreed at contract award.

Support response times, coverage, and pricing are agreed as part of the contract.

11. Security, Availability, and Resilience

The service operates under a formal security governance framework aligned to UK public sector best practice. This includes board-level accountability for security, compliance with Cyber Essentials Plus, and annual penetration testing conducted by NCSC-approved providers.

Operational security is supported through controlled change management, vulnerability management, protective monitoring, and formal incident management processes. Data is protected using encryption in transit and at rest, and access is restricted through role-based access controls and strong authentication mechanisms.

The service is designed for high availability using resilient, cloud-native architecture. Supplier-managed components are provided with a target availability of 99.9 percent, measured monthly, excluding agreed planned maintenance. Resilience is achieved through redundancy, automated scaling, health checks, and recovery mechanisms aligned to buyer requirements and the capabilities of the underlying cloud platform.

12. Service Constraints and Dependencies

The Data and AI Platform operates as a Software as a Service (SaaS) offering and is subject to the following constraints and dependencies.

The service requires an existing or provisioned cloud environment where it is deployed into the buyer's own cloud tenancy. Internet connectivity is required for access to SaaS components, management interfaces, and support channels. Service performance, availability, and scalability are dependent on the configuration and capabilities of the underlying cloud infrastructure selected by the buyer.

The service is designed to be configurable rather than bespoke. Customisation is delivered through configuration, policy settings, and templates rather than source code modification. Any optional extensions, enhanced support, or professional services are subject to separate agreement.

No dependency is placed on proprietary buyer technology beyond standard cloud services and modern web browsers.