

Service Definition

Data, AI and Modern Operational Data Platform as a Service (Resold SaaS)

G-Cloud 15 - Lot 2b (Software as a Service)

Supplier: 7Dxperts UK Limited

Version: 1.0

Date: 30 January 2026

Underlying platform providers (Vendors): Databricks, Snowflake, AWS, Microsoft Azure, Microsoft Fabric

Version control

Version	Date	Author	Description of change
1.0	30 January 2026	7Dxperts UK Limited	Initial issue for G-Cloud 15 Lot 2b submission

Purpose

This document describes how buyers can purchase and use Data, AI and Modern Operational Data Platform capabilities via 7Dxperts UK Limited as a resold SaaS service under G-Cloud 15 Lot 2b. It clarifies what is provided by the underlying platform providers (Vendors) and what is provided by 7Dxperts as the reseller (including onboarding, enablement, operational guidance, and escalation management).

How to use this document

- Understand the scope of the resold SaaS service and where 7Dxperts adds value.
- Identify buyer responsibilities versus supplier and vendor responsibilities.
- Plan onboarding, security, governance, and offboarding activities.
- Align support and resilience expectations to the selected platform and tier.

Document conventions

- Buyer: the contracting authority purchasing via G-Cloud.
- Supplier: 7Dxperts UK Limited (reseller plus agreed additional support).
- Vendor: Databricks, Snowflake, AWS, Microsoft Azure, or Microsoft Fabric.
- Tenant: the buyer's cloud account/subscription and platform workspace(s) configured within it.
- Call-off: the G-Cloud call-off contract for the service.

1. Service overview

1.1 What the service is

A cloud-native data and AI platform capability enabling ingestion, storage, governance, analytics, and AI/ML operations delivered using one or more underlying Vendor SaaS platforms selected by the Buyer.

1.2 Reseller model

- The Vendors provide the SaaS platform services, including their service architecture, security controls, and service availability commitments.
- 7Dxperts resells the SaaS and provides additional support such as onboarding, enablement, governance guidance, and operational advisory, as agreed in the call-off.
- Availability, resilience, and platform security assurances align primarily to the relevant Vendor commitments and the Buyer's chosen tier/edition.

1.3 Typical public sector use cases

- Unified data platform for cross-department operational and analytical workloads.
- Real-time reporting and operational analytics.
- Governed self-service analytics and data sharing.
- AI/ML model development, deployment, and monitoring pipelines.

2. Service features

The service supports the following capabilities, depending on the chosen Vendor(s), region, tier and edition:

- Cloud-native data ingestion (batch and streaming) from edge to cloud.
- Real-time analytics and reporting with scalable compute and low latency.
- AI/ML development, deployment, and monitoring with governed pipelines.
- Modern operational data services for transactional workloads and rapid application enablement.
- Secure remote access with SSO, RBAC, MFA and conditional access.
- Encryption in transit and at rest; customer-managed keys where supported.
- Governance capabilities including catalogue, lineage, policy-based access controls, and masking/classification settings.
- API-driven integrations and connectors for ETL/ELT and operational workflows.
- High availability options, backup and disaster recovery patterns aligned to RPO/RTO needs.
- Centralised monitoring, alerting, audit logging, and incident workflows.

3. Service benefits

- Create a single trusted view of data across departments and partners.
- Reduce manual preparation through automated ingestion and transformation.
- Enable secure self-service analytics to answer questions faster.
- Scale compute on demand and reduce time-to-insight.
- Deploy AI models faster to improve operational outcomes.

- Monitor data quality continuously to prevent downstream impact.
- Reduce operational overhead using managed services and automated maintenance.
- Improve incident response using centralised logs, alerts and dashboards.
- Optimise costs using usage insight and workload tuning.

4. Scope of service

4.1 Included

- Subscription access to the selected platform(s) (as resold SaaS).
- Access to standard documentation and knowledge base (Vendor-provided).
- Remote onboarding and enablement as described in Section 9.
- Support interface (email/ticket) and escalation management as described in Section 10.

4.2 Optional (by call-off)

- Onsite workshops and training.
- Migration discovery, planning and rehearsals.
- Templates and reference architectures (for example landing zone patterns and governance configuration guidance).
- Operating model design, governance workshops, and service management integration.
- Enhanced operational support and optimisation cycles.

4.3 Add-ons and extensions

No software add-ons or extensions are included by default. Any additional modules or features depend on Vendor editions and are quoted as part of subscription selection.

5. Deployment model and multi-cloud

- Deployment model: Public cloud.
- Multi-cloud: Yes (choice of platform and hyperscaler).
- The service is deployed into and consumed from the Buyer's cloud tenant/subscription, subject to Vendor architecture and configuration options.

6. Service constraints and assumptions

Constraints depend on the chosen platform, edition, region and tenant configuration. Buyers should plan for:

- Planned maintenance windows and periodic updates that may briefly affect performance.
- Region-dependent features and data residency considerations.
- Connectivity requirements (VPN/private connectivity where required) and supported browsers/APIs.
- Platform quotas (throughput, storage, API rate limits) that vary by edition.
- Additional configuration for specific third-party connectors and legacy formats.
- Buyer responsibility for identity integration, data classification and access policy decisions.

7. System requirements

Typical requirements include:

- Supported modern browser (Chrome, Edge, Firefox, Safari).
- Buyer cloud tenant/subscription and appropriate administrative access.
- Outbound HTTPS to platform endpoints; TLS 1.2+.
- Identity provider integration (for example Microsoft Entra ID / cloud IAM).
- Workstation OS: Windows, macOS, or Linux.
- Private connectivity (VPN/private link) where required.
- Runtime/tooling for integrations (for example Python, Java, .NET, Node.js) where applicable.
- Appropriate role permissions to create workspaces, policies and service accounts.
- Endpoint security maintained on user devices to organisational standards.

8. How buyers use the service

8.1 Access methods

- Web browser interface.
- APIs and SDKs for provisioning, automation and operations.

8.2 API capability

APIs can generally be used to:

- Create workspaces/projects, configure storage/compute, set identities and connectivity.
- Manage users/roles and rotate keys/secrets.
- Deploy pipelines/jobs and register or serve models (where applicable).
- Retrieve logs and metrics for monitoring and audit.

Limitations apply by RBAC, tenant administrative rights, edition/feature entitlements, quotas and regional constraints.

8.3 Customisation

Buyers can customise within their tenant, subject to Vendor capabilities, typically including:

- Workspace/project structure and environments (development/test/production).
- Storage locations and data zone structures.
- Network connectivity (public endpoints, private link/VPN).
- Identity and access policies (SSO, roles, conditional access).
- Encryption and key management options.
- Governance settings (catalogue, retention, masking).
- Monitoring and alerting integrations.
- Deployment of pipelines, analytics assets and models.

Underlying managed infrastructure and patching schedules are not customer customisable.

9. Onboarding

7Dxperts provides structured onboarding and enablement. A typical onboarding approach includes:

- Kick-off and access review.
- Tenant/workspace setup guidance.
- Identity and network integration guidance.
- Baseline security and governance configuration guidance.
- Role-based walkthroughs (administrators, engineers, analysts, data scientists).
- Workshops on ingestion, pipelines, analytics, AI/ML, monitoring and cost controls.
- Optional starter templates and sandbox patterns to accelerate adoption.
- Hypercare (Q&A clinics/office hours) and handover to steady-state support with agreed runbooks.

10. Support model (reseller plus vendor escalation)

10.1 Support channels

- Email and ticketing support (default).
- Onsite support (optional, extra cost where agreed).

10.2 How support works in a reseller model

- First-line (Supplier): 7Dxperts triages and supports Buyer users with guidance on configuration, usage, and agreed operating model items.
- Second/third line (Vendor): platform defects, vendor outages, and underlying SaaS issues are escalated to the relevant Vendor support, subject to the Buyer's subscribed support tier.
- 7Dxperts provides escalation management including case packaging, severity validation, coordination and communications back to the Buyer.

10.3 Support levels

Support tiers are aligned to Vendor offerings and may include:

- Standard: business-hours support via email/ticketing for queries and incidents triage only.
- Enhanced: extended hours, faster response targets, and priority handling.
- Premium/Enterprise: 24/7 cover for critical incidents, accelerated SLAs, and proactive guidance.

Enhanced and premium support are charged additionally

10.4 Response times

Initial response targets vary by plan and incident severity. Where a premium tier is selected, critical incidents may have 24/7 coverage. Non-critical cases are handled in published business hours unless otherwise agreed.

11. Data importing and exporting

11.1 Export at contract end

Buyers can extract data using standard platform export capabilities (UI/API/CLI/jobs) to buyer-controlled storage or alternative cloud environments, subject to platform features and permissions.

11.2 Constraints

Export may be constrained by quotas, rate limits, retention settings, region/residency controls, and cloud egress charges.

12. Offboarding and end-of-contract process

At contract end:

- Buyer retains access until the end date to export data, configuration and supported metadata.
- Supplier supports planning and scheduling offboarding activities.
- Access is disabled or closed after completion and termination steps are confirmed.

Additional costs may apply for complex migrations, large-scale exports, evidence packs, extended access, or out-of-hours offboarding. Vendors notice periods and termination actions are followed where applicable.

13. Security and governance

13.1 Data in transit

TLS 1.2+ is used for data in transit between networks. Private connectivity options (for example VPN/private link) may be used where required.

13.2 Data at rest and sanitisation

Security controls are primarily provided by the underlying Vendor platforms and typically include encryption at rest and secure sanitisation methods appropriate to the Vendor environment.

13.3 Data location and residency

Data storage and processing locations are determined by the selected Vendor platform, edition and region. Buyers select regions to meet their data residency requirements where supported.

13.4 Identity and access management

- MFA, SSO/federation, RBAC and conditional access (where supported).
- Administrative actions controlled by least privilege and (where available) privileged access workflows.
- Support access is time-bound, approved by the Buyer, scoped to the request, and logged for audit.

13.5 Audit logging

Audit information is available within the platform and can be integrated with buyer monitoring and SIEM tooling where supported. Retention and export options depend on platform features and buyer configuration.

14. Availability and resilience

14.1 Availability

Availability commitments align to the underlying Vendor platform SLA and the Buyer's selected tier/edition.

14.2 Resilience

Resilience is delivered using cloud-native redundancy patterns (for example multi-AZ deployment, replication and backups) and may include multi-region patterns where required, aligned to the Buyer's RPO/RTO requirements and architecture choices.

14.3 Outage reporting

Outages are communicated via Vendor status dashboards and alerts, with Supplier communications to the Buyer where relevant.

15. Buyer responsibilities

- Maintain the buyer cloud tenant/subscription and associated billing arrangements unless otherwise agreed.
- Select platform(s), region(s), editions and support tier(s).
- Configure identity integration, user lifecycle, and access policies.
- Make decisions on data classification, retention, and lawful basis for processing.
- Configure network connectivity (firewalls, VPN/private link) and maintain endpoint security on devices.
- Approve Supplier or Vendor support access to environments as needed.
- Pay cloud provider costs (consumption, egress, storage, compute) as applicable.

16. Supplier responsibilities (7Dxperts UK Limited)

- Provide the commercial route to purchase the resold SaaS via G-Cloud.
- Support onboarding and enablement (baseline plus options as agreed).
- Provide first-line support and operational guidance within the agreed scope.
- Coordinate and manage escalation to Vendor support.
- Provide optional advisory or professional services where included in the call-off.
- Provide operational handover support and runbooks where agreed.

17. Pricing approach (summary)

- Pricing is based on selected Vendor(s), tier/edition, region and consumption model.
- Support tier (standard/enhanced/premium) and any additional Supplier services.
- Any additional cloud provider charges incurred in the Buyer tenant.

Free trials may be available depending on Vendor policies and are typically time/credit/feature limited and not intended for production.

18. Service boundaries and important clarifications

- Platform SLAs and service credits are those of the selected Vendor platform unless explicitly stated in the call-off.
- Underlying platform security controls (datacentre, patching, core SaaS operations) are operated by the Vendor. 7Dxperts provides governance guidance and configuration support as agreed.
- The service is delivered into the Buyer's tenant (where applicable). Configuration choices are controlled by Buyer administrators, with Supplier support where agreed.