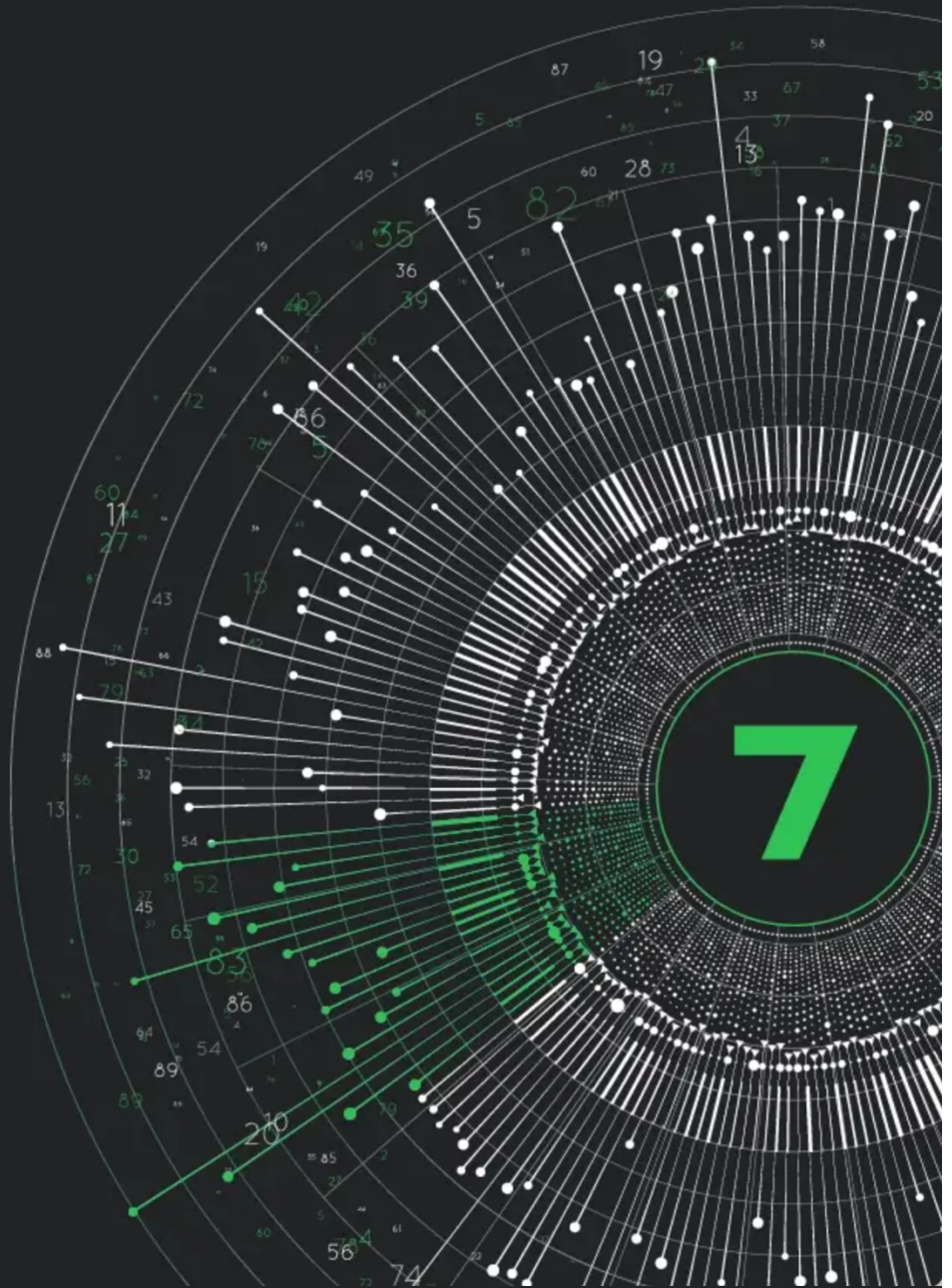


DataParQ - Service Definition

G-Cloud 15 Lot 2b – SaaS



Registered Address

142 Cromwell Road
London
SW7 4EF

Contact information

Phone: +44 20 3151 0307
Email: info@7Dxperts.com

Company Details

Company Reg	07515669
VAT	109841900

Document Control

Purpose

This service definition describes DataParQ, a Software as a Service (SaaS) offering available under G-Cloud 15 Lot 2b. It explains what the service does, what is included, how it is delivered and supported, and the responsibilities of the buyer and supplier.

How to use this document

Buyers can use this document to:

- understand DataParQ’s capabilities and the outcomes it enables;
- confirm the service scope, constraints and prerequisites;
- understand onboarding, support and operational processes;
- understand security, data protection and exit arrangements; and
- support the creation of a call-off contract and onboarding plan.

Document conventions

The following conventions are used throughout this document:

- ‘Buyer’ means the contracting authority purchasing the service.
- ‘Supplier’ means 7Dxperts UK Ltd.
- ‘Service’ means DataParQ as described in this document.
- ‘Tenant’ means an isolated deployment of DataParQ for a buyer.
- Headings are numbered for ease of reference; the numbering does not imply contractual precedence.

Version

Date	Version	Distribution
15th Jan 2026	0A	Internal
30th Jan 2026	1A	Public, Digital Marketplace

Contents

1 Service overview 5

1.1 What DataParQ is 5

1.2 Who the service is for 5

1.3 Key features 5

1.4 Benefits and outcomes 6

1.5 Service categories 6

2 Service scope 6

2.1 In-scope service components 6

2.2 Deployment models 6

2.3 Optional add-ons 7

2.4 Out of scope 7

3 How the service works 7

3.1 User experience 7

3.2 Integrations 7

3.3 System requirements and prerequisites 7

3.4 Service constraints 8

4 Provisioning and onboarding 8

4.1 Getting started 8

4.2 Documentation and training 8

4.3 Free trial / evaluation 8

5 Service management, maintenance and updates 9

5.1 Release management 9

5.2 Maintenance windows 9

5.3 Backup and disaster recovery 9

6 Security and data protection 9

6.1 Security governance 9

6.2 Data residency and processing locations 9

6.3 Encryption and access control 9

6.4 Vulnerability management and testing 9

7 Support and service levels 10

7.1 Support channels 10

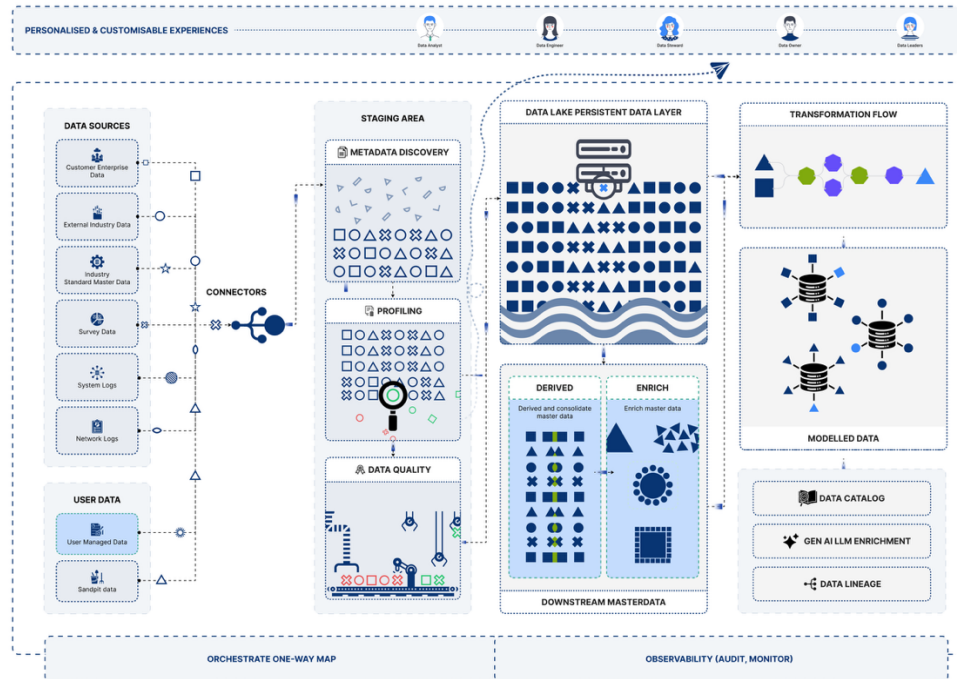
7.2 Support tiers 10

- 7.3 Incident severity and target response 10
 - 7.4 Availability commitments 10
- 8 Data import, export and exit management 11
 - 8.1 Data ownership 11
 - 8.2 Data import and export formats 11
 - 8.3 End-of-contract extraction 11
 - 8.4 Offboarding process 11
 - 8.5 Data deletion and sanitisation 11
- 9 Commercials and licensing (summary) 11
 - 9.1 Subscription model 11
 - 9.2 Usage limits and fair use 11
 - 9.3 Professional services 11
- 10 Buyer responsibilities 12
- 11 Assumptions and dependencies 12
- 12 Glossary 12

1 Service overview

1.1 What DataParQ is

DataParQ is an end-to-end, low-code data management and DataOps platform that helps organisations build, govern and operationalise trusted data across their data ecosystem. It provides centralised metadata, lineage, data quality automation, observability, role-based access controls and scalable governance.



1.2 Who the service is for

DataParQ is intended for organisations that need to improve data maturity and operationalise repeatable DataOps practices, including:

- data and analytics teams responsible for ingestion, transformation and quality;
- business analysts who need to create or modify data pipelines using a low-code approach;
- data governance teams responsible for stewardship, auditability and access controls; and
- platform and operations teams responsible for monitoring, reliability and incident management.

1.3 Key features

- Low-code drag-and-drop interface to accelerate data ingestion, transformation and operational workflows.
- Centralised Meta Store capturing business and technical metadata, ownership and certification.
- Multi-source ingestion to connect existing infrastructure (for example Databricks, BigQuery, S3, Redshift and Azure Synapse) with reusable connectors.
- Data Quality rule creation and monitoring, including attribute-level checks and notifications.
- Transformation Flow with pipeline health visibility, performance analytics and task management.
- AI-assisted auto data modelling to generate schemas, relationships, keys and cardinality.
- End-to-end lineage for impact analysis, dependency mapping and change tracking.
- Enterprise governance controls including RBAC, audit logs and approval workflows.

- User management to administer roles, groups and permissions across modules.
- Operational observability for ingestion and data quality, including anomaly detection and alerts.

1.4 Benefits and outcomes

- Accelerate delivery of data pipelines through low-code workflow automation.
- Reduce manual rework by detecting data issues early with monitoring and automated quality checks.
- Improve decision confidence through consistent definitions, lineage and governance.
- Enable faster onboarding by connecting sources quickly using reusable connectors and templates.
- Standardise transformations to minimise errors and speed releases across teams.
- Increase productivity by enabling analysts to build and manage pipelines without extensive coding.
- Support compliance through access controls, audit logs and policy enforcement.
- Optimise operations by observing pipeline health and resolving incidents rapidly.
- Scale data management by automating modelling, cataloguing and documentation.

1.5 Service categories

DataParQ supports the following Digital Marketplace service categories: application development and deployment; data management; database management systems; data lake management systems; database administration and development; data modelling; data ingestion and transformation; data quality; master data intelligence; and metadata management.

2 Service scope

2.1 In-scope service components

The service includes access to the DataParQ platform modules as agreed in the order, typically including:

- Data Ingestion (connectors, ingestion pipelines and synchronisation).
- Data Quality (rule definition, execution and monitoring).
- Meta Store (centralised business and technical metadata).
- Data Lineage (interactive lineage maps and impact analysis).
- Transformation Flow (visual transformation design and execution metadata).
- Governance (RBAC, policies, approvals and audit).
- Observability (pipeline monitoring, alerts and operational dashboards).
- User Management (users, groups, roles and logging).
- Auto Modelling (AI-assisted modelling of analytical schemas).

2.2 Deployment models

DataParQ can be delivered as a dedicated-tenant SaaS service using one of the following models:

- Buyer cloud tenancy (single-tenant): DataParQ is deployed into the buyer's chosen public, private or hybrid cloud environment. The buyer controls the underlying cloud resources; the supplier provides the software, deployment automation, updates and support. This model is commonly used where buyers require direct control over data residency and networking.
- Supplier-hosted (single-tenant or evaluation tenant): DataParQ is hosted in a supplier-managed environment for trial or, where agreed, production use. This model enables faster evaluation without buyer infrastructure setup.

Unless explicitly agreed otherwise, DataParQ is designed to operate in the buyer's cloud tenancy, with no 'noisy neighbour' effects between buyers because each tenant runs on dedicated infrastructure under buyer control.

2.3 Optional add-ons

Optional add-ons can be purchased at additional cost, including:

- Enhanced or Premium support tiers (extended hours, 24/7 P1 cover, named Technical Account Manager).
- Onsite workshops and training.
- Implementation and integration services (for example, connector configuration, data modelling patterns, governance operating model).
- Health checks, optimisation and performance tuning.
- Evidence packs for assurance activities (for example, tailored security responses or audit support).

2.4 Out of scope

Unless agreed in writing as part of a call-off, the following are out of scope:

- Provisioning and payment of the buyer's underlying cloud infrastructure (for buyer-tenancy deployments).
- Custom software development beyond configuration and standard extension points.
- Operating the buyer's wider data platform and downstream applications.
- Data migration between legacy platforms and DataParQ-managed pipelines beyond agreed onboarding activities.

3 How the service works

3.1 User experience

Users access DataParQ through a web browser interface. No end-user client installation is required. Platform components are deployed as container images and accessed via HTTPS.

3.2 Integrations

DataParQ integrates with common data platform components, subject to buyer environment and connectivity, including:

- Databricks Lakehouse environments.
- Google BigQuery and Google Cloud Storage.
- Amazon S3 and AWS Redshift.
- Azure Synapse Analytics and Azure storage services.
- BI tooling integration, including ThoughtSpot search and analytics (where licensed).
- Identity providers via SAML single sign-on (optional)
- Third Party source platforms that support flat files or API for data ingestion.

3.3 System requirements and prerequisites

For buyer-tenancy deployments, the buyer must provide an environment that meets the following minimum requirements:

- Container runtime: Docker Engine or a compatible Kubernetes platform.
- Compute, memory and storage sized for expected pipeline throughput and data volumes.

- Network connectivity to required source systems, warehouses and cloud storage.
- Outbound internet access for updates, licence validation and support (or an agreed alternative mechanism).
- TLS-enabled connectivity for data transfers between components (TLS 1.2 or above).
- Modern browser for the UI (Chrome, Edge or Firefox).
- Optional: SSO integration via SAML and integration with monitoring/logging tooling.

3.4 Service constraints

Known constraints include:

- Planned maintenance may be required to apply upgrades and updates; maintenance windows are agreed in advance.
- The service is delivered as container images and requires a compatible container runtime and suitable host resources.
- Availability is primarily dependent on the underlying hosting environment and selected architecture (for example single-region vs multi-region)

4 Provisioning and onboarding

4.1 Getting started

Onboarding is tailored to the buyer's technical requirements and typically includes a technical discovery, installation guidance, environment setup support and an enablement plan.

A typical onboarding approach is:

- Kick-off and requirements confirmation (sources, targets, volumes, security and access).
- Environment readiness (networking, IAM, container runtime, certificates and DNS).
- Tenant deployment and baseline configuration.
- Connector setup and first ingestion pipelines.
- Initial data quality rules and observability dashboards.
- Optional: modelling patterns (for example medallion architecture) and AI-assisted modelling enablement.
- Training for administrators and users; handover of runbooks and documentation.

4.2 Documentation and training

Standard documentation is provided in HTML and/or PDF formats. Training can be delivered remotely and, where agreed, onsite.

4.3 Free trial / evaluation

A free, time-limited trial can be provided in a supplier-hosted demonstration tenant for evaluation of core features. Buyers should use sample or anonymised data and must not connect production systems or use real personal data in the trial unless explicitly agreed.

5 Service management, maintenance and updates

5.1 Release management

The supplier provides updates including bug fixes, security patches, minor enhancements and major version upgrades. Release notes are issued with each update along with any prerequisites.

5.2 Maintenance windows

Planned maintenance windows are agreed with the buyer to minimise impact. Emergency maintenance may be required to address critical vulnerabilities or imminent threats.

5.3 Backup and disaster recovery

For buyer-tenancy deployments, the buyer is responsible for implementing backup and disaster recovery for the hosting environment and any platform data stores. The supplier provides guidance and, where agreed, automation templates. For supplier-hosted deployments, backup and recovery arrangements are defined in the service level schedule agreed at call-off.

6 Security and data protection

6.1 Security governance

The supplier operates an information security management system aligned to ISO/IEC 27001, with board-level accountability for service security. Security policies and processes cover access management, encryption, logging and audit, vulnerability management, secure change management and incident response.

6.2 Data residency and processing locations

DataParQ can be deployed to support UK and EEA data residency requirements. For buyer-tenancy deployments, data location is controlled by the buyer's selected cloud region(s). For supplier-hosted deployments, the hosting region(s) are agreed with the buyer.

6.3 Encryption and access control

Security controls include:

- TLS 1.2+ for data in transit between components and networks.
- Role-based access control (RBAC) with least-privilege permissions.
- Multi-factor authentication (MFA) and optional identity federation (SSO) where supported.
- Audit logging of user and administrator activities.

6.4 Vulnerability management and testing

DataParQ is subject to continuous vulnerability scanning and periodic penetration testing (at least every six months). Security fixes are prioritised by severity and deployed through controlled change management.

7 Support and service levels

7.1 Support channels

Support is provided via email and/or an online ticketing portal. Onsite support can be provided at additional cost where agreed.

7.2 Support tiers

Support tiers are agreed at call-off and may include:

- Standard: business-hours remote support via ticketing/email for incidents and service requests.
- Enhanced: extended hours, faster response targets and priority handling for production services.
- Premium/Enterprise: 24/7 support for critical incidents, proactive guidance, named Technical Account Manager and accelerated SLAs.

7.3 Incident severity and target response

Incident targets depend on the agreed support tier and hosting model. An indicative approach is provided below; final targets are confirmed in the call-off.

Severity	Definition	Initial response target	Update frequency
P1 – Critical	Complete service outage or critical function unavailable; no workaround.	Premium: ≤ 1 hour (24/7) Standard: best endeavours (business hours)	Hourly or as agreed
P2 – High	Major functionality impaired; workaround available.	Premium: ≤ 4 hours Standard: ≤ 1 business day	Daily
P3 – Medium	Degraded performance or defect with limited impact.	≤ 1 business day	Weekly
P4 – Low / Request	Minor issue, cosmetic defect, documentation clarification or service request.	≤ 2 business days	On significant change

7.4 Availability commitments

Where DataParQ is supplier-hosted, an availability target (monthly uptime) and any service credit mechanism can be agreed at call-off. Where DataParQ is deployed in the buyer's cloud tenancy, availability is primarily dependent on buyer-controlled infrastructure and architecture; in that model the supplier provides software-level support and guidance.

8 Data import, export and exit management

8.1 Data ownership

The buyer retains ownership of all buyer data processed by the service. The supplier uses buyer data only as necessary to provide the service, support and maintenance, in accordance with the agreed terms and any data processing agreement.

8.2 Data import and export formats

Supported formats for import and export include CSV and structured formats such as JSON and YAML (where applicable to metadata and configuration exports).

8.3 End-of-contract extraction

At the end of contract, buyers can extract their configuration by exporting DataParQ metadata that stores pipeline definitions and operational DataOps information. Exports can include metadata for connected sources, medallion-layer definitions, pipeline configurations and execution metadata. Where applicable, DataParQ can generate reusable artefacts such as SQL scripts or documented logic to assist with re-creating pipelines in another environment.

8.4 Offboarding process

An offboarding plan is agreed to ensure continuity, data extraction and closure. The buyer retains access until the contract end date to export data and configurations. Additional professional services may be required for complex migrations, large-scale exports or extended access beyond the end date.

8.5 Data deletion and sanitisation

For supplier-hosted tenants, data sanitisation follows recognised standards and may include cryptographic erasure and secure deletion. For buyer-tenancy deployments, deletion and sanitisation are performed by the buyer within its own environment.

9 Commercials and licensing (summary)

9.1 Subscription model

DataParQ is licensed on a subscription basis. Pricing and usage metrics are defined in the order and may include limits such as the number of data feeds, environments and aggregate compute capacity.

9.2 Usage limits and fair use

Usage is monitored to support capacity planning and compliance with the subscribed limits. If the buyer anticipates exceeding agreed limits, additional capacity can be purchased.

9.3 Professional services

Implementation, training and specialist support services can be provided on a time-and-materials basis or as a fixed-price package where scoped and agreed. The costs relating to onboarding all data pipelines is assessed on a case-by-case basis but can range between £10,000 and £50,000 depending on the size of the environment

10 Buyer responsibilities

The buyer is responsible for:

- providing timely access to relevant stakeholders and technical contacts;
- ensuring appropriate lawful basis and permissions for any data processed;
- for buyer-tenancy deployments: providing and operating the underlying cloud infrastructure, networking and identity services;
- managing user accounts and access requests in line with the buyer's policies (unless delegated to the supplier as an add-on);
- performing backups and disaster recovery for buyer-tenancy deployments; and
- using the service in accordance with the agreed terms, including usage limits and acceptable use.

11 Assumptions and dependencies

This service definition assumes that:

- the buyer provides suitable cloud connectivity to data sources and targets;
- the buyer provides access to required cloud services (for example managed databases, storage and load balancers) where needed;
- identity integration requirements (SSO, MFA, conditional access) are agreed during onboarding;
- any required third-party licences (for example BI tools) are procured by the buyer unless explicitly included; and
- the buyer provides a nominated service owner for operational decisions and escalation.

12 Glossary

Term	Definition
Data feed	A configured ingestion or pipeline source-to-target flow within DataParQ, counted for subscription purposes where applicable.
Tenant	An isolated deployment of DataParQ for a single buyer.
Metadata	Configuration and descriptive information about data assets, pipelines, rules, lineage and operational events.
RBAC	Role-based access control.
SSO	Single sign-on.