

Service Definition Document

Service Name: Cloud Data & Analytics Services

Supplier: ClearSky Performance Ltd

Framework: G-Cloud 15

Lot: Lot 3 – Cloud Support

Version: 1.1

Date: January 2026

Table of Contents

1. The Service3

2. Data Backup and Restore, and Disaster Recovery4

3. Onboarding and Offboarding Support4

4. Service Constraints.....5

5. Service Levels5

6. After-Sales Support.....5

7. Technical Requirements6

8. Outage and Maintenance Management6

9. Hosting Options and Locations.....6

10. Security.....6

11. Intellectual Property Rights7

12. Exit & Transition8

A1. Service Level Annex8

A2. Data Processing Annex9

A3. Security & Compliance Annex9

1. The Service

Our Cloud Data & Analytics Transformation Suite delivers specialist consulting, assessment, implementation, and managed services to help public sector organisations build trusted, high-value data ecosystems in the cloud. The suite comprises six interconnected services:

1.1 The Services

1.1.1 Cloud Data Quality Assessment & Data Cleansing

Comprehensive assessment of data quality across key data domains, including profiling, rule definition, scoring, monitoring, cleansing, standardisation, matching, and enrichment of data assets to improve accuracy, completeness, consistency, timeliness, and usability for operational and analytical use.

1.1.2 Cloud Data Analysis, Insights & Decision-Support

Design and delivery of advanced analytics, business intelligence dashboards, self-service reporting, predictive and descriptive modelling, and insight products using cloud-native analytics platforms to support evidence-based decision-making.

1.1.3 Cloud Data Privacy & Secure Anonymisation

Assessment and implementation of privacy-preserving data practices, including data protection impact assessments, pseudonymisation, anonymisation, tokenisation, and differential privacy techniques, supporting compliance with GDPR, UK GDPR, and the Data Protection Act.

1.1.4 Cloud Data Assurance & Validation Services

Independent validation of data pipelines and analytical outputs, including lineage tracking, reconciliation, control checks, auditability, and automated quality gates to provide confidence in data used for operational processes and reporting.

1.1.5 Cloud Data Migration & Modernisation

Planning and delivery of lift-and-shift, re-platform, refactor, or re-architect approaches to migrate data workloads to cloud platforms, including ETL/ELT modernisation, performance optimisation, cost optimisation, and legacy system decommissioning.

1.1.6 Cloud Enterprise Data Architecture & Governance

Definition and implementation of enterprise data strategies, target architectures, standards, governance frameworks, metadata management, stewardship operating models, data catalogues, and policies to support consistent and trusted data across the organisation.

1.2 How We Deliver

- **Discovery** — Understand business objectives, data landscape, stakeholders, constraints, and success measures. Assess current-state data maturity, risks, and opportunities.

- **Design** — Define target-state architecture, data models, quality rules, security and privacy controls, and delivery approach aligned to cloud best practice.
- **Build** — Configure and develop cloud data pipelines, analytics solutions, models, and controls using iterative, agile delivery.
- **Assure** — Validate data quality, security, performance, lineage, and compliance through automated testing, reconciliation, and independent checks.
- **Handover** — Provide documentation, knowledge transfer, and operational artefacts to enable support, maintenance, and ongoing improvement

2. Data Backup and Restore, and Disaster Recovery

2.1 Data Backup & Restore — Customer data processed during engagements is stored in secure, UK-hosted cloud repositories with automated backups (daily incremental + weekly full), a retention period of 30–90 days, and point-in-time restore within 4 hours. Test/cleansed datasets are returned to customer environments.

2.2 Disaster Recovery / Business Continuity — Multi-AZ/region infrastructure (e.g., Azure UK South + secondary region failover) ensures 99.9% availability. RTO <30 minutes, RPO <15 minutes for critical processing. Annual BCP testing, remote team continuity, and documented DR plans aligned with NCSC principles.

3. Onboarding and Offboarding Support

3.1 Onboarding — Free for engagements >10 days: Discovery workshop, data access setup (secure SFTP/VPN/Azure Data Share), environment provisioning, and tailored project plan. Typical: 3–7 working days with dedicated lead.

Day	Main Focus	Key Activities	Deliverables
Pre	Prep	Welcome pack + data questionnaire sent	Client prep requested
1	Kick-off & Access	Kick-off call + accounts / tools access + 2–3 intros	Access granted; summary notes
2	Current State	3–4 sessions: data, BI, processes	Landscape & pain points captured
3	Stakeholders	4–6 short stakeholder meetings	Priority themes & gaps list
4	Discovery Workshop	4 hr: objectives → current state → prioritized use cases & scope	Requirements list + prelim roadmap
5	Workshop Summary & Document	Recap call + final checks + summary document	Week summary + next steps timeline

3.2 Offboarding — Full handover of processed data, models, reports, governance artefacts, and scripts in portable formats (e.g., Parquet, CSV, Git repos, Collibra exports). Data deletion/certification of destruction within 30 days (or sooner). Formal exit report and knowledge transfer included at no extra cost.

4. Service Constraints

4.1 Maintenance Windows — Planned works outside UK business hours (Mon–Fri 09:00–17:00 GMT), with ≥5 working days' notice. Emergency patches may use 48-hour notice.

4.2 Customisation — High flexibility for bespoke rules, models, or integrations. Major custom tool development scoped separately.

4.3 Remote Delivery / On Site - Remote delivery standard; on-site requires agreement. Scalable team size based on availability.

5. Service Levels

5.1 Performance — Data quality scans/cleansing: results within 24–48 hours; analytics insights: daily refreshes; migration cutover: agreed windows with minimal downtime.

5.2 Availability — 99.5% for processing platforms (monthly). Excludes customer source issues.

5.3 Support Hours — 09:00–17:00 Mon–Fri (business hours), excluding UK public holidays.

5.4 Enhanced/Premium support: optional extended or 24/7 coverage

5.5 Response Times: see Annex 13 for P1 to P4 response times (time to first meaningful response).

If P1 response target is missed, escalation to Service Manager is automatic

5.6 Channels: email, phone, Jira ticketing system or equivalent.

5.7 Out-of-hours — Available at additional rates.

6. After-Sales Support

6.1 30 days free post-engagement support for defect resolution and knowledge queries.

6.2 Access Artefacts - reusable templates, best-practice guides, and quarterly data governance webinars.

6.3 Optional ongoing managed services e.g., monthly data health monitoring, governance reviews.

7. Technical Requirements

7.1 Customer provides: Access to source/target environments (e.g., Azure Synapse, AWS Glue, GCP BigQuery), credentials, schemas, and compliance approvals.

7.2 We use: Cloud-native + specialist tools (e.g., Azure Purview, Informatica Cloud Data Quality, Talend, Collibra, Great Expectations, dbt for analytics/modernisation).

7.3 Compatibility: Major clouds (Azure/AWS/GCP), hybrid/on-prem sources, formats (structured/semi/unstructured).

8. Outage and Maintenance Management

8.1 24/7 monitoring with automated alerts.

8.2 Notification via status page/email within 15 minutes.

8.3 RCA for SLA breaches within 5 working days.

8.4 Maintenance with rollback procedures and customer coordination.

9. Hosting Options and Locations

9.1 All processing and data storage in **UK-only regions** (Azure UK South/UK West, AWS London, GCP London/Europe-west2) to meet UK government sovereignty/residency requirements (e.g., OFFICIAL).

9.2 No data transfer outside UK/EEA without approval.

10. Security

10.1 Compliance — Aligns with ISO 27001 standards, Cyber Essentials / Cyber Essentials Plus, GDPR/UK GDPR compliant, NCSC Cloud Security Principles aligned.

10.2 Controls — Encryption (AES-256 at rest, TLS 1.3+ in transit), RBAC, MFA, regular pen testing/vulnerability scanning.

10.3 Personnel — BPSS baseline; SC-eligible staff for sensitive engagements.

10.4 Incident Response — Security incidents notified within 24 hours; full IR plan.

10.5 Data Protection — Processor role; standard DPA available. Sub-processors approved/disclosed.

10.6 Personnel Security All data access is restricted to Senior Consultants/Directors with verified BPSS/SC clearance. We do not offshore data processing or assign unverified junior resources to client data.

11. Intellectual Property Rights

11.1 For the purposes of this Service Definition:

- **Background IPR** means all Intellectual Property Rights owned or developed by either Party prior to the Effective Date or developed independently of the Services, including (without limitation) the Supplier's pre-existing software, code libraries, frameworks, accelerators, analytics methodologies, models, templates, documentation, and tooling.
- **Foreground IPR** means all Intellectual Property Rights in Deliverables created or developed by the Supplier in the performance of the Services, including (without limitation) bespoke software, scripts, data pipelines, analytics models, dashboards, documentation, configurations, and curated data assets.

11.2 The Supplier shall retain ownership of all Supplier Background IPR. The Customer is granted a non-exclusive, perpetual, royalty-free, worldwide licence to use the Supplier Background IPR solely to the extent necessary to receive, use, operate, support, and maintain the Deliverables.

11.3 The ownership and licensing of Foreground IPR will be agreed in writing at the start of each engagement and may follow one of the models below:

Option A – Supplier Ownership (Default)

The Supplier retains ownership of the Foreground IPR. The Customer is granted a non-exclusive, perpetual, royalty-free, worldwide licence (with the right to sub-license to other UK public sector bodies) to use, copy, modify, and exploit the Foreground IPR for its internal business and public sector purposes.

Option B – Buyer (Customer) Ownership

The Customer shall own the Foreground IPR. The Supplier is granted a non-exclusive, perpetual, royalty-free, worldwide licence to use the Foreground IPR for the purposes of delivering the Services and for the Supplier's internal business purposes.

Option C – Bespoke Arrangement

A mutually agreed alternative ownership and licensing position appropriate to the specific engagement.

11.4 Unless otherwise agreed in writing at the start of each engagement, Option A from 12.3 shall apply.

12. Exit & Transition

12.1 The Supplier shall provide reasonable cooperation and assistance to support an orderly transition of the Services to the Customer or a replacement supplier upon expiry or termination of an engagement in open/portable formats.

12.2 The Supplier shall provide access to, and where applicable copies of, all Deliverables, documentation, configurations, and agreed data assets necessary to enable continued operation of the solution.

12.3 The Supplier shall provide knowledge transfer, including walkthrough sessions and reasonable technical clarification, as required to support transition.

12.4 The Customer shall continue to have the benefit of any licences granted to Background IPR and Foreground IPR in accordance with the agreed Intellectual Property Rights terms.

12.5 Any transition assistance beyond that reasonably included within the Services may be provided on a time and materials basis at agreed rates.

12.6 Upon completion of transition, the Supplier shall securely return or delete Customer data in accordance with agreed data protection and information security requirements within 30 days.

A1. Service Level Annex

Priority	Description	Response Target	Resolution Notes
P1 – Critical	Service unavailable / major impact	Within 1 hour	Resolution depends on complexity & dependencies
P2 – High	Significant functionality impaired	Within 4 hours	Workaround or temporary fix may be applied
P3 – Medium	Minor issue / no immediate impact	Within 8 business hours	Full resolution planned
P4 – Low	General enquiries / cosmetic	Within 2 business days	Handled in queue order

A2. Data Processing Annex

Role and Responsibilities

- Supplier acts as **Data Processor** under Customer instruction when handling personal data
- Customer remains **Data Controller**

Personal Data Handling

- Processed strictly per documented instructions
- Secure transmission, storage, and deletion as required
- Access restricted to authorised personnel

Data Retention & Disposal

- Retained only for duration of engagement or as agreed
- Secure disposal or return of customer data at engagement end

Auditing & Compliance

- Cooperation with audits in line with Data Processing Agreement
- Documentation of processing activities maintained

A3. Security & Compliance Annex

Information Security

- Secure access management and authentication controls
- Encrypted data handling and secure storage
- Endpoint security and secure communications
- Regular vulnerability scanning and remediation
- Security awareness training for all staff

Regulatory Compliance

- UK GDPR and Data Protection Act 2018 compliance
- Security audits conducted on request in accordance with Call-Off Contract
- Adherence to CCS Cloud Security Principles where relevant

Risk Management

- Risk assessment and mitigation for all deliverables
- Incident reporting and escalation process