DATA ENGINEERING AND PLATFORM DEVELOPMENT

Service Definition

19 JANUARY 2026

TRIDENT INTELLIGENT SOLUTONS
Regus Atterbury Lakes Fairbourne Drive, Atterbury, Milton Keynes, Buckinghamshire, England, MK10 9RG

Contents

Service overview

The Data Engineering and Platform Development service provides end-to-end design, build, and operationalisation of modern data platforms. The service covers discovery and data readiness through to development, deployment, optimisation, and on-going support of scalable, secure, and reliable data architectures.

The service includes the design and implementation of data pipelines, data warehouses, data lakes, and lakehouse solutions for both structured and unstructured data. Capabilities include ETL and ELT development, data integration, data quality and validation frameworks, platform optimisation, and cloud-based scalable architectures to ensure data is reliable, accessible, and ready for analytics, reporting, or AI and machine learning applications.

The service is delivered through a structured, project-based engagement model. Activities may include requirements definition, data source assessment, data modelling, pipeline development, platform configuration, system integration, testing, deployment, development of supporting services (including APIs where required), and transition to operational use. Solutions may be deployed in customer-managed, service provider-managed, or third-party cloud environments, depending on agreed requirements and constraints.

Data backup, restore, and disaster recovery

Backups of data, code, configurations, schemas, and platform metadata are performed at predefined intervals and protected through access controls and encryption in line with ISO/IEC 27001 standards. Backup intervals and retention periods are defined on a project-by-project basis according to business, regulatory, and contractual requirements.

Disaster recovery and business continuity plans define roles, responsibilities, and recovery procedures and are reviewed periodically to reflect changes in service scope or risk. Where third-party data platforms or cloud services are used, their resilience and continuity controls are incorporated under a shared responsibility model. These measures collectively support ISO 27001 requirements for information availability and continuity.

For each project, the following is documented:

- What data, code, and configurations are backed up
- Backup frequency
- Storage location
- Restoration procedures
- Backup and restore testing schedule
- Roles and responsibilities

Onboarding and offboarding support

Onboarding

Following contract agreement, a Delivery Manager and appropriate delivery team are assigned to the engagement. Delivery is conducted using either a structured waterfall or Agile methodology, depending on the scale, complexity, and scope of the project.

A kick-off workshop is held to introduce key stakeholders, confirm the agreed scope, and establish governance, communication, and delivery arrangements. A Project Initiation Document (or Discovery Initiation Document where applicable) is produced and approved by key stakeholders. This document defines aims and objectives, scope, delivery plan, roles and responsibilities, governance arrangements, and key risks and dependencies, and serves as the primary reference throughout delivery.

During onboarding, the service provider works with the customer to provision secure access to required data sources, systems, tools, and environments necessary to deliver the services. Alignment is also achieved on data governance principles, data usage constraints, information security expectations, and any relevant legal or regulatory considerations.

Offboarding

At the conclusion of the engagement, a formal offboarding workshop and handover session is conducted to support transition of the data platform and associated components to the customer. This session covers platform architecture, data flows, operational considerations, and agreed next steps, and may include training for relevant customer teams where required.

All solution artefacts, including pipeline code, data models, infrastructure-as-code, configurations, and technical and operational documentation, are formally handed over to the customer, except where the platform is hosted and operated by the service provider under an ongoing agreement.

In the event of early termination, a closure workshop is held to assess the status of all in-scope items and agree required actions. A Project Closure Document is provided to support an orderly and controlled exit.

Service constraints

Service delivery depends on access to client systems, datasets, and subject-matter experts. Platform performance and pipeline reliability are influenced by data quality, source system complexity, and volume. Cloud infrastructure costs may vary depending on client requirements. Scheduled maintenance, updates, or platform optimisation may temporarily affect availability. Large-scale deployments or integration with legacy systems may require phased delivery. Ongoing support, monitoring, and optimisation are provided under separate agreements unless specified. Clients must provide access, permissions, and engagement to achieve full service benefits.

Service levels

We provide full lifecycle support for data engineering and platform development projects, tailored to client requirements, with SLAs defined per engagement. Standard Support covers

remote assistance during business hours, issue logging, troubleshooting, and guidance on data pipelines, warehouses, or lakehouse platforms. Suitable for development or non-critical environments. Enhanced Support provides extended business-hours coverage, defined response times, proactive monitoring, pipeline optimisation, and a named technical contact familiar with the client's platforms. Costs are agreed as a project-based or annual support arrangement. Premium Support is designed for mission-critical data platforms, offering priority response, extended or 24/7 coverage by agreement, proactive monitoring, and rapid escalation. Clients receive a dedicated Data Engineering Lead and access to technical specialists as required. Premium SLAs are bespoke and agreed per client. Severity Classifications:

- Severity 1 (Critical): Platform or pipeline failure severely impacting operations; immediate response.
- Severity 2 (High): Major issues affecting data delivery; rapid resolution required.
- Severity 3 (Medium): Partial functionality limitations; addressed during standard response times.
- Severity 4 (Low): Minor queries or adjustments; handled during normal business hours. Support is primarily delivered remotely, with onsite assistance available by arrangement.

Unless otherwise agreed in writing, the service and ongoing support shall be provided during standard business hours (9-5), Monday to Friday. Support outside of these hours, including 24/7 support, may be provided subject to a separately agreed arrangement.

After-sales support

Following delivery of the data platform, a formal handover is conducted to support transition to operational use. This includes comprehensive documentation covering platform architecture, data pipelines, schemas, configurations, security controls, and operational procedures. Knowledge transfer sessions may be provided to ensure customer teams are able to operate, monitor, and maintain the platform effectively.

Ongoing maintenance and support services are available where required and are agreed on a case-by-case basis. These services may be provided under a retainer-based support arrangement or on a time-and-materials basis. Maintenance activities may include pipeline enhancements, performance optimisation, platform upgrades, data quality improvements, and minor schema or integration changes.

Technical and client-side requirements

The customer is responsible for identifying appropriate business, technical, security, and governance stakeholders to support decision-making, approvals, and day-to-day coordination throughout the engagement. The service provider will advise on required roles and responsibilities to support successful delivery.

Depending on the agreed delivery and deployment model, the service provider requires appropriate access to customer-managed environments, including cloud tenants, development

and testing environments, data platforms, or on-premises infrastructure. Access requirements, permissions, and security controls are agreed in advance and provisioned in accordance with customer security policies and the principle of least privilege.

Any additional technical prerequisites, such as network connectivity, identity and access integration, data availability, or third-party tools, are identified and agreed during onboarding to ensure timely and effective delivery.

Outage and maintenance management

In the event of a service outage or operational issue attributable to defects within the scope of the delivered data pipelines or platform components and under the service provider's responsibility, remediation will be undertaken at no additional cost. This includes investigation, fault isolation, and corrective action necessary to restore normal operation, subject to agreed scope and acceptance criteria.

Where outages or issues arise from factors outside the agreed scope of responsibility, such as changes to customer-managed infrastructure, upstream data source failures, third-party platform outages, or enhancement requests, support may be provided under an agreed maintenance arrangement on a retainer or time-and-materials basis.

Planned maintenance activities, including updates, patches, or optimisations, are scheduled in coordination with the customer wherever practicable to minimise disruption. Roles, responsibilities, escalation paths, and service boundaries are defined per engagement to ensure effective incident and maintenance management.

Hosting options and locations

Data platforms may be deployed within the customer's existing infrastructure, including customer-managed cloud environments or on-premises systems. In these scenarios, the service provider supports design, deployment, and configuration within agreed scope, while the customer retains responsibility for the underlying infrastructure under a shared responsibility model.

Where required, the service provider can host the data platform on behalf of the customer for an additional fee. Hosted deployments utilise cloud-based infrastructure selected to meet functional, security, regulatory, and data residency requirements. Hosting provider, geographic location, resilience characteristics, and security controls are agreed and documented per engagement.

Data access on exit

Customers retain full ownership of all customer-provided data, derived datasets, schemas, code, configurations, and solution artefacts developed during the engagement. The service provider acts as a data processor and does not retain customer data beyond what is required to deliver the services.

Upon service exit, all agreed datasets, pipelines, infrastructure definitions, and documentation are made available to the customer in mutually agreed, industry-standard formats to support continued operation or migration. Reasonable assistance is provided during a defined transition period, subject to engagement terms. Any residual customer data retained by the service provider is securely deleted or anonymised in accordance with agreed retention schedules and applicable regulations.

Security

Security is embedded throughout the service lifecycle and aligned with recognised information security standards, including ISO/IEC 27001, and applicable cloud shared responsibility models. This includes:

- **Information Security Governance**
  Defined security roles, responsibilities, and decision-making authority per engagement.
- **Risk-Based Security Controls**
  Controls selected based on data sensitivity, platform architecture, and deployment model.
- **Access Control**
  Role-based access controls and least-privilege principles applied to data and platforms.
- **Data Protection and Encryption**
  Encryption in transit and at rest where appropriate.
- **Monitoring, Logging, and Auditability**
  Logging of security-relevant events to support monitoring, investigation, and audit.
- **Supplier and Shared Responsibility Management**
  Clear allocation of security responsibilities where third-party platforms are used.
- **Information Lifecycle and Exit Management**
  Secure data handling, retention, and deletion processes on service exit.

Security responsibilities are shared between the service provider, the customer, and any third-party infrastructure or platform providers. Control ownership and responsibilities are defined and agreed for each engagement to ensure proportionate risk management and compliance with contractual, regulatory, and operational requirements.