

Atlantic Data - DBS Registered Body Service

1. Service Overview

The DBS Registered Body Services provide cloud-based software capabilities that support organisations in meeting their safeguarding, compliance, and governance obligations relating to Disclosure and Barring Service (DBS) checks.

The services support the full lifecycle of DBS-related safeguarding activities, including DBS application processing, identity and eligibility management, DBS Update Service status checking, and safeguarding assurance activities designed to maintain visibility of DBS status over time.

The services are delivered by a specialist DBS technology provider with extensive experience supporting public sector, education, healthcare, voluntary, and regulated organisations. The services are used in safeguarding-critical environments where accuracy, consistency, auditability, and proportionality of decision-making are essential.

This service description applies to the **DBS Registered Body (RB)** service, where **the customer acts as the DBS Registered Body** and is responsible for DBS application submission and interaction with the Disclosure and Barring Service. Atlantic Data provides and supports the cloud-based software platform that enables customers to manage DBS activity.

2. Service Scope

This service description covers the DBS Registered Body service operating model, where the customer acts as the DBS Registered Body and Atlantic Data provides a secure, cloud-based DBS application and case management platform.

DBS Registered Body (RB) service – Software-Led DBS Service

A software-led DBS service designed for organisations that wish to retain operational control of DBS activity by acting as the DBS Registered Body.

This service includes:

- Private Cloud-based DBS application and case management software
- Capture and management of applicant data and consent
- Support for manual and digital identity verification methods in line with DBS requirements
- Validation tools to support application completeness and accuracy
- Workflow and case management to support DBS processing
- Management information and audit reporting to support safeguarding oversight

Under this service, the customer acts as the DBS Registered Body and is responsible for DBS application submission, countersigning, and interaction with the Disclosure and Barring Service. Atlantic Data is responsible for providing, maintaining, and supporting the software platform.

Exclusions

Optional items or services referenced in this document, including those listed at the end (Digital ID, Update Service, Right to Work services), are excluded from the scope of this service unless explicitly stated as included.

3. Customer Journey (End-to-End Workflow)

The DBS Registered Body Services support a structured end-to-end journey for managing DBS checks and ongoing safeguarding assurance.

Core DBS Journey

The DBS journey typically follows the stages set out below.

3.1 Service Setup and Configuration

The service is configured in line with the selected Digital Platform item. This includes organisational structure, user access, role definitions, safeguarding requirements, and the agreed approach to identity verification.

3.2 Application Initiation

DBS applications are initiated by the customer using the service. Applicants are invited to provide the required information and consent to support the DBS checking process.

3.3 Identity Verification (ID Check)

The applicant's identity is verified in accordance with DBS requirements. Identity verification may be completed using:

- a manual identity checking process; or
- a digital identity verification process, where this has been selected as part of the service configuration.

Responsibility for completing identity verification rests with the customer acting as the DBS Registered Body.

3.4 Data Capture and Validation

Applicant information and identity evidence are captured and validated using the service to support completeness, accuracy, and eligibility prior to submission.

3.5 DBS Submission

Eligible applications are submitted electronically to the Disclosure and Barring Service by the customer acting as the DBS Registered Body, using Atlantic Data's e-Bulk e-Broker DBS submission channels.

3.6 DBS Processing and Queries

The Disclosure and Barring Service processes the application. Any queries, exceptions, or clarification requests raised during processing are managed directly by the customer in their role as DBS Registered Body.

3.7 Result Receipt and Reporting

DBS results are received and made available through the service. Management information, audit records, and reporting are updated to support safeguarding oversight and governance.

3.8 Ongoing Safeguarding and Update Service (Where Applicable)

Where the DBS Update Service is included:

- Consent for status checking is managed
- Eligibility for status checks is monitored
- DBS Update Service status checks are performed in line with customer configuration
- Changes, lapses, or loss of eligibility are reported to the customer

The Update Service operates alongside the DBS application process and does not replace the requirement for a new DBS application where required.

3.9 Safeguarding Oversight

The customer reviews DBS outcomes and safeguarding information and takes any employment or safeguarding decisions informed by the service outputs. The service supports, but does not replace, customer decision-making responsibilities.

4. Service Features and Capabilities

The DBS Registered Body Services provide a set of core software features that support customer-led DBS processing and safeguarding oversight.

Core DBS Features

The following features are available:

- Private Cloud-based DBS application and case management
- Secure capture and management of applicant data and consent
- Support for manual and digital identity verification methods in line with DBS requirements
- Validation and quality checks to reduce application errors prior to submission

- Workflow management to support DBS processing
- Tracking of application status throughout the DBS lifecycle
- Secure receipt and handling of DBS results
- Management information and audit reporting to support safeguarding oversight
- Role-based access controls and segregation of duties
- Configurable workflows to align with organisational safeguarding processes

5. Service Delivery Model

The DBS Registered Body Services are delivered as a cloud-based software service. Atlantic Data provides, maintains, and supports the software platform used by customers to manage DBS activity.

Private Cloud-Based Software Delivery

The service is delivered through a secure, private cloud-hosted platform accessed via standard web browsers. The platform enables customers to initiate and manage DBS applications, monitor progress, and access reporting and audit information.

The software is maintained, updated, and supported by Atlantic Data. Updates and improvements are applied centrally without requiring customer-side installation or maintenance.

6. Support and Service Management

Support Channels

Support is provided through the following channels:

- Service Desk Support – for day-to-day operational queries, user assistance, and system usage support
- Email Support – for non-urgent requests, reporting queries, and follow-up communication
- Telephone Support – for time-sensitive issues relating to system availability or use

Support channels are available during published support hours. Contact details and access arrangements are provided during onboarding.

Incident Escalation

Incidents and service issues are managed using a defined incident management process. Issues are assessed, prioritised, and progressed based on their impact and urgency.

Escalation routes are in place for:

- Issues affecting system availability or performance
- Safeguarding-critical incidents impacting DBS processing

Where appropriate, incidents are escalated internally to specialist teams to ensure timely investigation and resolution.

Service Monitoring and Management

The service is actively monitored to support availability and performance. Atlantic Data maintains oversight of platform operation and support demand to identify trends and areas for improvement.

7. Service Availability and Performance

The DBS Registered Body Services are designed to provide reliable and consistent availability to support safeguarding-critical operations. Availability and performance are managed to ensure customers can access the service when required.

Service Availability

The service is delivered via a cloud-hosted platform that is available to authorised users through standard web browsers, subject to planned maintenance and external dependencies.

Dependencies and External Services

Certain aspects of the service depend on third-party systems and external bodies, including the Disclosure and Barring Service. Availability and processing times for these external services are outside Atlantic Data's direct control.

8. Security and Compliance

The DBS Registered Body Services are designed and operated with security, data protection, and regulatory compliance as core principles. Controls are in place to protect personal data and support safeguarding obligations.

Information Security

Atlantic Data maintains an information security management framework aligned with recognised standards, including ISO/IEC 27001.

Data Protection and Privacy

The service is operated in compliance with UK GDPR and the Data Protection Act 2018. Atlantic Data acts as a data processor on behalf of customers.

9. Hosting and Data Residency

The **DBS Registered Body (RB)** services are delivered using a secure, private cloud-hosted infrastructure designed to support availability, resilience, and compliance with UK data protection and public sector expectations.

Hosting Environment

The services are hosted within a managed private cloud environment that supports the secure operation of the software platform and associated managed service components.

The hosting environment is managed and maintained by Atlantic Data. Infrastructure is monitored and maintained to support service availability, security, and performance.

Data Residency

Personal data processed as part of the DBS Registered Body Services is hosted within the United Kingdom.

Data residency arrangements are designed to support compliance with UK data protection legislation and public sector requirements, including those applicable to safeguarding organisations.

Access and Connectivity

The service is accessed via the public internet using secure connections. Access is restricted to authorised users through authentication and role-based controls.

Backup and Recovery

Backup and recovery processes are in place to support data integrity and service continuity. Backups are managed in line with defined retention and recovery procedures and are tested periodically.

10. Data Management and Retention

The DBS Registered Body Services manage personal and operational data in a controlled and transparent manner to support DBS processing, safeguarding oversight, and compliance with legal and regulatory obligations.

Data Categories

The services may process the following categories of data:

- Applicant personal information required for DBS applications
- Identity verification information and supporting evidence
- DBS application status and outcome data
- Consent records and audit information

- Service usage, reporting, and management information

Data processed is limited to what is necessary to deliver the selected service and support safeguarding and governance requirements

11. Onboarding and Implementation

Onboarding typically includes:

- Confirmation of the selected Digital Platform item and service configuration
- Set-up of organisational details, user roles, and access controls
- Configuration of workflows, safeguarding requirements, and reporting
- Agreement of identity verification methods and operational processes

The onboarding process is managed collaboratively to ensure clarity of roles and responsibilities.

12. Offboarding and Exit Planning

Offboarding from the DBS Registered Body Services is managed in a controlled and transparent manner to support continuity, data protection, and safeguarding obligations. Offboarding arrangements are designed to minimise disruption and support an orderly transition at the end of the contract period.

Offboarding Approach

Offboarding is initiated in line with contractual arrangements and agreed timelines. The approach is proportionate to the selected service configuration and the nature of the customer's DBS activity.

Offboarding activities may include:

- Confirmation of offboarding scope and timetable
- Controlled closure of user access
- Agreement of data handling and transfer requirements
- Coordination of any required transition support

Data Handling on Exit

On exit, personal and operational data is handled in accordance with:

- Applicable data protection legislation
- DBS audit and record-keeping requirements
- Customer-defined retention instructions, where permitted

Data may be:

- Returned to the customer in an agreed format
- Retained where legally required
- Securely deleted or anonymised in line with defined procedures

A record of data handling actions may be provided to support audit and governance requirements.

13. Customer Responsibilities

Customers are responsible for acting as the DBS Registered Body, including lawful DBS application submission, identity verification, and safeguarding decision-making.

14. Optional Modules

The Atlantic Update Service

The DBS Update Service may be included as an optional module alongside this service, where the customer has also selected the separate G-Cloud service titled **“The Atlantic Update Service”**. When configured, this module enables ongoing status checking of eligible DBS certificates using the Disclosure and Barring Service Update Service, subject to individual consent and eligibility requirements. The module supports organisations in maintaining ongoing safeguarding oversight by identifying changes to DBS status over time, without removing the need for a new DBS application where required. The scope and operation of the DBS Update Service are defined by the Atlantic Update Service G-Cloud listing and the agreed service configuration.

Digital Identity Service

A Digital Identity capability may be included as an optional module alongside this service, where the customer has also selected the separate G-Cloud service titled **“Atlantic Data Digital Identity Services”**. When configured, this module supports the verification and controlled reuse of digital identity evidence in line with UK government standards, subject to individual consent and applicable eligibility requirements. For organisations, this can support more efficient identity verification processes and reduce unnecessary repeat identity checks, while maintaining appropriate safeguarding, governance, and audit controls. The scope and operation of digital identity functionality are defined by the Atlantic Data Digital Identity Services G-Cloud listing and the agreed service configuration.

Right to Work Service

A Right to Work checking capability may be included as an optional module alongside this service, where the customer has also selected the separate G-Cloud service titled **“Right to**

Work Services". When configured, this module supports the verification of an individual's right to work in the UK in accordance with Home Office requirements, using appropriate checking methods based on nationality and eligibility. For organisations, this can support compliant workforce onboarding and assurance processes, while maintaining appropriate governance, auditability, and separation from DBS decision-making. The scope and operation of Right to Work functionality are defined by the Right to Work Services G-Cloud listing and the agreed service configuration.