

The Atlantic Update Service

1. Service Overview

The Update Service provides a cloud-based safeguarding and assurance service that supports organisations in maintaining ongoing visibility of an individual's Disclosure and Barring Service (DBS) certificate status over time. The service enables organisations to identify whether a DBS certificate remains current or whether a change has occurred since the certificate was issued.

The service operates using the official DBS Update Service and is designed to complement, rather than replace, the DBS application process. It supports safeguarding-critical environments by enabling proportionate, ongoing assurance without requiring unnecessary repeat DBS applications, where lawful and appropriate.

The Update Service is delivered by a specialist DBS provider with extensive experience supporting public sector, education, healthcare, voluntary, and regulated organisations. The service is used in environments where safeguarding oversight, auditability, and timely identification of changes to DBS status are essential.

This service description applies to the **Update Service**, which may be purchased as a standalone G-Cloud service or as an optional module alongside other DBS-related services. The specific service configuration and delivery model applicable to a customer are determined by the selected Digital Platform item.

2. Service Scope

The Update Service provides software-enabled and, where applicable, managed service capabilities to support DBS Update Service status checking in line with DBS guidance and eligibility requirements.

Included

The Update Service includes:

- Management of individual consent for DBS Update Service status checking
- Capture and validation of DBS certificate details required for status checks
- Execution of DBS Update Service status checks using official DBS Update Service interfaces
- Monitoring of Update Service registration and certificate eligibility
- Identification of changes, lapses, or loss of Update Service eligibility
- Exception-based reporting to support safeguarding oversight
- Management information and audit reporting

The service supports use alongside DBS certificates obtained through Atlantic Data services or other lawful DBS application routes.

Exclusions

Unless explicitly stated in the selected Digital Platform item, the Update Service does not include:

- Submission of new DBS applications
- Identity verification or DBS eligibility determination
- Safeguarding or employment decision-making on behalf of customers

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

The Update Service supports a structured end-to-end journey for managing ongoing DBS status assurance.

3.1 Service Setup and Configuration

The service is configured in line with the selected Digital Platform item, including organisational structure, user access, safeguarding requirements, and reporting preferences.

3.2 Consent and Eligibility Management

The individual's explicit consent is obtained and recorded to support DBS Update Service status checking. Certificate eligibility and Update Service registration status are verified prior to status checks.

3.3 Status Checking

DBS Update Service status checks are performed using official DBS Update Service channels in accordance with DBS guidance. Status checks confirm whether the DBS certificate remains current or whether a change has occurred.

3.4 Exception Identification

Where a status check indicates a change, lapse, or loss of eligibility, this is identified and recorded within the service.

3.5 Reporting and Safeguarding Oversight

Status check outcomes and exceptions are reported to the customer to support safeguarding oversight and appropriate follow-up actions.

4. Service Features and Capabilities

The Update Service provides features designed to support ongoing DBS status assurance.

Core Features

- Cloud-based management of DBS Update Service status checking
- Secure capture and management of consent records

- Validation of DBS certificate details and Update Service eligibility
- Execution of DBS Update Service status checks
- Exception-based reporting and alerting
- Management information and audit reporting
- Role-based access controls

5. Service Delivery Model

The Update Service is delivered using a secure, cloud-based software platform. Atlantic Data is responsible for the operation, maintenance, and support of the platform.

Where included, managed service components may support consent management, monitoring, and exception handling in line with the selected service configuration.

6. Support and Service Management

Support and service management for the Update Service are provided in a structured manner to ensure continuity, reliability, and effective resolution of issues.

Support Channels

Support is provided through service desk, email, and telephone channels during published support hours. Contact details and access arrangements are provided during onboarding.

Incident Escalation

Incidents and service issues are assessed, prioritised, and progressed based on their impact and urgency, with escalation routes in place for safeguarding-critical issues.

Service Monitoring and Management

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

7. Service Availability and Performance

The Update Service is designed to provide reliable and consistent availability to support safeguarding-critical assurance activities. Availability and performance are managed to ensure customers can access the service when required and that DBS Update Service status checking activities are not disrupted unnecessarily.

Service Availability

The service is delivered via a secure, cloud-hosted platform that is available to authorised users through standard web browsers.

The platform is designed to support continuous access for operational use, subject to:

- Planned maintenance activities
- Unplanned incidents or events outside Atlantic Data's control
- Availability of external third-party systems

Where maintenance is planned, customers are notified in advance where reasonably practicable.

Performance and Reliability

The platform is designed to support the expected volumes and usage patterns associated with DBS Update Service status checking and safeguarding oversight. Performance is monitored to ensure that:

- Status checks can be initiated and processed efficiently
- Reporting and management information remain accessible
- Exception identification and notification can be performed without undue delay

Performance management focuses on service stability, accuracy, and operational effectiveness rather than transaction speed alone.

Resilience and Continuity

Measures are in place to support service resilience and continuity, including:

- Redundancy within the hosting environment
- Data backup and recovery processes
- Business continuity and incident response planning

These measures are designed to reduce the risk of service interruption and support timely recovery where incidents occur.

Dependencies and External Services

Certain aspects of the Update Service depend on external systems and services, including the Disclosure and Barring Service Update Service. Availability and response times for these external services are outside Atlantic Data's direct control and may affect end-to-end service operation.

8. Security and Compliance

The Update Service is designed and operated with security, data protection, and regulatory compliance as core principles. Controls are in place to protect personal data, support safeguarding obligations, and meet the expectations of public sector and regulated organisations.

Information Security

Atlantic Data maintains an information security management framework designed to protect the confidentiality, integrity, and availability of service data.

Security controls include:

- Role-based access controls
- Secure authentication and authorisation mechanisms
- Segregation of environments and duties
- Monitoring and logging of system access and activity
- Regular review and continuous improvement of security controls

Data Protection and Privacy

The Update Service is operated in compliance with applicable data protection legislation, including the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

Personal data is processed solely for the purposes of delivering DBS Update Service status checking and safeguarding assurance on behalf of customers. Data handling practices are designed to support:

- Lawful, fair, and transparent processing
- Data minimisation and purpose limitation
- Appropriate retention and secure disposal
- Support for data subject rights

DBS Compliance

The service is delivered in accordance with DBS Update Service requirements and guidance. This includes:

- Adherence to DBS consent and eligibility rules
- Secure handling of DBS certificate information and status data
- Controls to support auditability and safeguarding oversight

Certifications and Assurance

Atlantic Data holds and maintains relevant certifications and assurance measures to support service security and reliability, including:

- ISO/IEC 27001 certification for information security management
- Regular independent penetration testing conducted by accredited providers
- Appropriate assurance measures aligned with public sector expectations

Evidence of certifications and assurance measures can be provided on request.

9. Hosting and Data Residency

The Update Service is delivered using a secure, cloud-hosted infrastructure designed to support availability, resilience, and compliance with UK data protection and public sector expectations.

Hosting Environment

The service is hosted within a managed cloud environment that supports the secure operation of the software platform.

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

Data Residency

Personal data processed as part of the Update Service is hosted within the United Kingdom.

Data residency arrangements are designed to support compliance with UK data protection legislation and safeguarding requirements.

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 Update Service manages personal and operational data in a controlled and transparent manner to support safeguarding oversight and compliance with legal and regulatory obligations.

Data Categories

The service may process the following categories of data:

- DBS certificate reference information
- Update Service registration and eligibility information
- Consent records
- Status check outcomes and exception data

- Service usage, reporting, and audit information

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

Data Processing Roles

Atlantic Data acts as a data processor on behalf of customers for the purposes of delivering the Update Service. Customers act as data controllers and determine the lawful basis and purposes for processing personal data.

Data Retention

Personal data is retained in accordance with:

- DBS Update Service guidance and audit requirements
- Applicable legal and regulatory obligations
- Customer-defined retention periods, where permitted

Retention periods and data handling arrangements are agreed during onboarding and may be reviewed periodically. Data that is no longer required is securely deleted or anonymised in line with defined procedures.

Data Access and Control

Access to personal data is restricted to authorised users and personnel based on defined roles and responsibilities. Controls are in place to prevent unauthorised access, alteration, or disclosure of data.

Data Subject Rights

The service supports customers in meeting their obligations in relation to data subject rights, including access, rectification, and erasure, in line with applicable data protection legislation.

11. Onboarding and Implementation

Onboarding Approach

Onboarding for the Update Service is designed to be structured, efficient, and proportionate to the selected service configuration.

Onboarding typically includes:

- Confirmation of the selected Digital Platform item
- Set-up of organisational details, user roles, and access controls
- Configuration of safeguarding requirements and reporting preferences
- Agreement of consent capture and operational processes

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

Implementation Activities

Implementation activities may include:

- System configuration and environment setup
- User account creation and role assignment
- Testing of status checking and reporting workflows

The scope and duration of implementation activities depend on the selected service and organisational complexity.

User Enablement

Users are supported during onboarding through:

- Guidance on system use and DBS Update Service processes
- Access to user documentation and supporting materials
- Initial support to ensure users can operate the service effectively

Go-Live and Early Support

Following onboarding, the service moves into live operation. Additional support may be provided during the early stages of use to address queries and confirm correct configuration.

12. Offboarding and Exit Planning

Offboarding from the Update Service is managed in a controlled and transparent manner to support continuity, data protection, and safeguarding obligations.

Offboarding Approach

Offboarding is initiated in line with contractual arrangements and agreed timelines. The approach is proportionate to the nature of the customer's use of the Update Service.

Offboarding activities may include:

- Confirmation of offboarding scope and timetable
- Controlled closure of user access
- Agreement of data handling and transfer requirements

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, retained where legally required, or 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 using the Update Service have defined responsibilities to ensure the service is used appropriately, lawfully, and in line with safeguarding requirements.

Organisational Responsibilities

Customers are responsible for:

- Ensuring lawful use of DBS Update Service status checking
- Obtaining and maintaining valid individual consent
- Maintaining accurate certificate and eligibility information
- Ensuring authorised users are trained to use the service appropriately

Safeguarding and Decision-Making

Customers remain responsible for:

- Reviewing status check outcomes and exceptions
- Determining appropriate safeguarding or employment actions

The service supports safeguarding oversight but does not replace customer responsibility or judgement.

14. Optional Modules

The Update Service supports a modular approach. Optional modules or integrations may be added where explicitly included in the selected Digital Platform item and service configuration.

Optional modules may include integration with other DBS-related services or reporting enhancements, where applicable.