

Atlantic Data – Right to Work Service

1. Service Overview

The Right to Work Service provides a cloud-based compliance and assurance service that supports organisations in verifying and recording an individual's legal right to work in the United Kingdom. The service enables organisations to carry out Right to Work checks in accordance with Home Office guidance and statutory requirements, supporting compliant workforce onboarding and ongoing assurance.

The service is designed to support regulated and safeguarding-critical environments, including public sector, healthcare, education, and other organisations with formal compliance obligations. It provides a structured, auditable approach to Right to Work checking while supporting proportionality, accuracy, and governance.

The Right to Work Service is delivered by a specialist provider with extensive experience in identity verification and workforce compliance services. The service supports lawful checking processes and does not replace customer responsibility for employment decision-making.

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

2. Service Scope

The Right to Work Service provides software-enabled and, where applicable, managed service capabilities to support compliant Right to Work checking in line with Home Office requirements.

Included

The Right to Work Service includes:

- Management of Right to Work checking workflows
- Support for compliant Right to Work checking methods based on individual nationality and eligibility
- Capture and validation of evidence required for Right to Work checks
- Secure handling and storage of Right to Work check records
- Management information and audit reporting
- Support for ongoing compliance and assurance

The service supports Right to Work checks carried out using official Home Office-approved methods, including digital and manual routes, where applicable.

Exclusions

Unless explicitly stated in the selected Digital Platform item, the Right to Work Service does not include:

- Employment decision-making on behalf of customers
- HR, payroll, or workforce management systems
- Immigration advice or legal determination of immigration status

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

The Right to Work Service supports a structured end-to-end journey for carrying out compliant Right to Work checks.

3.1 Service Setup and Configuration

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

3.2 Check Initiation

A Right to Work check is initiated by an authorised user as part of a recruitment or onboarding process. The individual is provided with information explaining the purpose of the check and how their information will be used.

3.3 Evidence Capture

Evidence required to complete the Right to Work check is captured using approved methods. Depending on the individual's nationality and eligibility, this may include:

- Digital ID Checks for UK Nationals
- Digital checks using official Home Office online services, such as View and Prove

3.4 Verification and Validation

Captured evidence is verified and validated to ensure completeness and compliance with Home Office requirements. Validation checks are applied to reduce errors and support auditability.

3.5 Outcome Recording

The outcome of the Right to Work check is recorded within the service, including the date of the check, method used, and any follow-up requirements.

3.6 Reporting and Compliance Oversight

Right to Work check records and outcomes are made available through the service to support compliance monitoring, audit, and governance.

4. Service Features and Capabilities

The Right to Work Service provides features designed to support compliant and auditable Right to Work checking.

Core Features

- Cloud-based Right to Work checking and case management
- Support for Home Office-approved digital and manual checking routes
- Secure capture and storage of Right to Work evidence
- Validation checks to support compliance and accuracy
- Management information and audit reporting
- Role-based access controls and segregation of duties

5. Service Delivery Model

The Right to Work Service is delivered using a secure, cloud-based software platform. Atlantic Data is responsible for the availability, maintenance, and support of the platform.

Where included, managed service components may support evidence validation and compliance oversight in line with the selected service configuration.

6. Support and Service Management

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

Support Channels

Support is provided through the following channels:

- Service Desk Support – for operational queries and system usage assistance
- Email Support – for non-urgent requests and reporting queries
- Telephone Support – for time-sensitive or compliance-related issues

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

Incident Escalation

Service issues are assessed, prioritised, and progressed based on their impact and urgency. Escalation routes are in place for compliance-critical issues.

Service Monitoring and Management

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

7. Service Availability and Performance

The Right to Work Service is designed to provide reliable and consistent availability to support compliance-critical workforce onboarding and assurance activities. Availability and performance are managed to ensure customers can access the service when required and that Right to Work checking activities are not disrupted unnecessarily.

Service Availability

The service is delivered via a 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 external dependencies outside Atlantic Data's control
- Availability of external third-party systems used to complete checks

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 Right to Work checking and compliance oversight. Performance is monitored to ensure that:

- Checks can be initiated and completed efficiently
- Evidence capture and record creation can be performed without undue delay
- Reporting and management information remain accessible

Performance management focuses on service stability 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 service depend on external systems and services, including Home Office online checking services (for example, online Right to Work checking routes) and third-party components used as part of identity and evidence verification. 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 Right to Work Service is designed and operated with security, data protection, and regulatory compliance as core principles. Controls are in place to protect personal data, support lawful processing, 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:

- Access controls based on defined user roles
- Secure authentication and authorisation mechanisms
- Segregation of environments and duties
- Monitoring and logging of system access and activity
- Regular review and improvement of security controls

Data Protection and Privacy

The 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 Right to Work checking 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

Home Office Compliance

The service is designed to support compliance with Home Office Right to Work guidance and statutory requirements, including:

- Use of appropriate checking routes based on nationality and eligibility

- Capture of evidence required to establish a statutory excuse, where applicable
- Creation and retention of compliant Right to Work check records
- Support for auditability and governance 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

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

9. Hosting and Data Residency

The Right to Work 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 Right to Work Service is hosted within the United Kingdom.

Data residency arrangements are designed to support compliance with UK data protection legislation and public sector 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 Right to Work Service manages personal and operational data in a controlled and transparent manner to support compliance oversight and legal and regulatory obligations.

Data Categories

The service may process the following categories of data:

- Individual identity and contact information required to complete Right to Work checks
- Evidence and record data captured as part of Right to Work checking (for example, document details or online check references)
- Check outcomes and follow-up requirements
- Consent and acknowledgement records, where applicable
- Service usage, reporting, and audit information

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

Data Processing Roles

Atlantic Data acts as a data processor on behalf of customers for the purposes of delivering the Right to Work 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:

- Home Office Right to Work guidance and record-keeping 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 Right to Work 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 Right to Work checking workflows and compliance settings
- Agreement of evidence capture methods and operational processes
- Configuration of reporting and audit outputs

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 checking workflows and reporting

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 Right to Work checking processes
- Access to user documentation and supporting materials
- Initial support to ensure users can operate the service effectively

User enablement is designed to support consistent and compliant use of the service.

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 Right to Work Service is managed in a controlled and transparent manner to support continuity, data protection, and orderly transition at the end of service use.

Offboarding Approach

Offboarding is initiated in line with contractual arrangements and agreed timelines. The approach is proportionate to the nature of the customer's Right to Work checking 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
- Home Office 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 using the Right to Work Service have defined responsibilities to ensure the service is used appropriately, lawfully, and in line with Home Office requirements.

Organisational Responsibilities

Customers are responsible for:

- Ensuring lawful Right to Work checking and adherence to Home Office guidance
- Selecting and applying the correct checking route based on nationality and eligibility
- Ensuring evidence captured and records created meet statutory requirements

- Maintaining accurate organisational and user information within the service
- Ensuring users are authorised and trained to use the service appropriately

Employment Decision-Making

Customers remain responsible for:

- Reviewing Right to Work check outcomes
- Making employment decisions and taking follow-up actions where required

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

Compliance Responsibilities

Customers are responsible for complying with applicable laws, guidance, and policies relevant to their use of Right to Work services, including data protection obligations.