Service Level Agreement (SLA)

Umbrella Body Service Right to Work (RtW) Checks

1. Agreement Overview

This Agreement represents a Service Level Agreement ("SLA" or "Agreement") between HR Connect EmploymentCheck and Customer for the provisioning of the Umbrella Body Service – Right to Work (RtW) check solution required to support and sustain the product or service throughout the duration of the contract.

This Agreement will continue unless revised by HR Connect to ensure compliance with legal and commercial developments throughout the duration of the contract.

This Agreement outlines the parameters of all services covered, as understood by all parties and are accepted in accordance with HR Connect General Terms of Sale (which can be found at www.hrconnect.org.uk).

Together with the Order and the General Terms of Sale this document provides a binding agreement between both parties.

If it is found that there is an inconsistency between this Agreement and the General Terms of Sale, then detail as defined within this document will take precedence.

2. Purpose

The purpose of this Agreement is to ensure that all elements and commitments are in place to provide a consistent service, support and delivery to the Customer by HR Connect.

The objectives of this Agreement are to:

- Define the service / product that the Customer is purchasing
- Provide clear reference to service ownership, accountability, roles and/or responsibilities.
- Present a clear, concise and measurable description of service provision to the customer.

3. Stakeholders

The following Service Provider and Customer will be used as the basis of the Agreement and represent the primary stakeholders associated with this Agreement:

Service Provider: Employment Check, part of HR Connect

Customer: Customer ("Customer")

HR Connect reserve the right to support this contract through third party sources where appropriate. System operators employed by HR Connect may be changed by from time to time at its discretion.

4. Periodic Review

This Agreement is valid for the term of the contract as outlined in the Order Form and is valid until further notice. This Agreement may be reviewed at a minimum once per financial year; however, in lieu of a review during any period specified, the current Agreement will remain in effect.

Contents of this Agreement may be amended by HR Connect as required and communicated to all affected parties through publishing on our website.

5. Service Agreement

The following detailed service parameters are the responsibility of the Service Provider in the ongoing support of this Agreement.

Service to be provided

The following Services are covered by this Agreement:

Provision of an online solution for conducting Right to Work checks. The solution supports three methods for completing Right to Work checks in line with Home Office guidance:

1) Using a Digital Identity Service Provider (IDSP) to undertake a Digital ID check to digitally verify Applicant documents which can be used to establish a statutory excuse. EmploymentCheck is partnered with a market-leading, certified third-party IDSP – Yoti. This integration enables Digital ID checks to be undertaken for the purpose of completing Right to Work checks. The passport images and face scan images used for the Digital ID check are returned to the EmploymentCheck system where they can be downloaded and stored locally. The Customer needs to retain this evidence for the duration of employment + 2 years.

2) Through a check of the Applicant's Right to Work status online via the Home Office Share Code route. The 'Profile' page can be uploaded to the EmploymentCheck system, and an expiry date entered if required. This document can be downloaded and stored locally. The Customer needs to retain this evidence for the duration of employment + 2 years.

3) By performing a manual check of the Applicant's original documents. The copies of the original documentation can be uploaded to the EmploymentCheck solution, and an expiry date entered if required. These documents can be downloaded and stored locally. The Customer needs to retain this evidence for the duration of employment + 2 years.

All three methods will provide an employer with a Statutory Excuse.

The Right to Work evidence and if applicable, the face scan image will only be stored on the EmploymentCheck system for 6 months after the Right to Work check has entered the 'Application Archived' status. After which point, the document evidence and face scan will be permanently purged from the EmploymentCheck solution.

6. Customer Responsibilities

Customer responsibilities and/or requirements in support of this Agreement include:

- Conduct Right to Work Checks on employees in line with Home Office guidelines. The Customer retains responsibility for ensuring that Right to Work checks have been conducted correctly and that a statutory excuse has been obtained prior to individuals commencing work. Employers could be liable for financial penalties should the Home Office guidance not be correctly applied when Right to Work checks are undertaken. Cantium Business Solutions accepts no responsibility for Right to Work checks not being completed by the customer in line with statutory guidance.
- The Customer is responsible for downloading Right to Work evidence and saving this against an Employee's HR record for the duration of employment + 2 years. Right to Work evidence can be downloaded from the EmploymentCheck system but this evidence will be purged 6 months after an application enters the 'Application Archived' status therefore the EmploymentCheck system should not be considered a storage repository for Right to Work evidence to meet statutory guidance.
- Create and manage Right to Work applications via a secure online form.
- Understand the role of the relying party and comply with all requirements relating to the use of Digital ID checks for carrying out Right to Work Checks.
- To maintain complete confidentiality at all times and adhere to the Data Protection Act 2018, as amended.

7. Service Provider Responsibilities

Service Provider responsibilities and/or requirements in support of this Agreement include:

- To provide a compliant, online Right to Work solution to conduct RtW checks via one of three routes: via a certified Digital Identity Service Provider (IDSP) – Yoti, via the manual route using List A and List B Document Lists or via Home Office Share Code route.
- Enable secure administrative access to the EmploymentCheck system allowing the management of Right to Work checks being undertaken.
- Secure hosting for the EmploymentCheck system via an ISO27001 accredited hosting organisation.
- Provide technical support where calls will be logged and dealt with as per the Service Performance section below.
- Maintain an ongoing relationship with YOTI to ensure the continued provision of YOTI services.
- Raise support queries with YOTI directly where required.
- To adhere to the DBS Code of Practice at all times.
- To maintain complete confidentiality at all times and adhere to the Data Protection Act 2018, as amended.
- Account Management support to deal with any aspects of the agreement.

8. Service Assumptions

Assumptions related to in-scope services and/or components include:

- Functionality enhancements will be communicated and documented to the customer.
- Ongoing Digital ID support will be provided by Yoti in partnership with HR Conenct and Yoti themselves will be responsible for maintaining their own infrastructure and certifications.
- Notice will be provided in advance of planned system maintenance.

9. Service Performance

Coverage parameters specific to the service(s) covered in this Agreement are as follows:

Effective support of in-scope services is a result of maintaining consistent service levels. The following sections provide relevant details on service availability, monitoring of in-scope services and related components.

10. Service Availability

Coverage parameters specific to the service(s) covered in this Agreement are as follows:

Telephone support: 8:30 A.M. to 5:00 P.M. Monday – Friday, Excluding bank holidays and HR Connect concessionary days

Email support: Monitored 8:30 A.M. to 5:00 P.M. Monday – Friday, Excluding bank holidays and HR Connect concessionary days

Emails received outside of office hours will be collected and responded to as per the SLA above.

11. Service Requests

In support of services outlined in this Agreement, the Service Provider will respond to service-related incidents and/or requests submitted by the Customer within the following time frames:

Within 8 hours (during business hours) for issues classified as High priority.

Within 48 hours for issues classified as Medium priority.

Within 5 working days for issues classified as Low priority.

Remote assistance will be provided in-line with the above timescales dependent on the priority of the support request.

12. Service Feedback

HR Connect endeavours to make its service the best that it can be at all times.

We therefore encourage and appreciate all FEEDBACK you may wish to present us with, both POSITIVE or Negative.

Where possible, would aim to rectify any problems you incur to a level that meets both our high expectations, although we do recognise that on occasion may not be possible. Please be assured that your feedback will be taken seriously. Often, we will be able to resolve problems face to face or by telephone. If you feel that this is not possible then you can put your feedback in writing by e-mail to: info@hrconnect.org.uk

Please cover the following points:

- Your reason for feedback.
- An overview of the feedback and its handling to date.
- Your view on what should happen next.
- The names of any staff involved

When your feedback is received, we will:

- Endeavour to rectify any problems caused within 20 working days.
- Acknowledge your correspondence within 5 working days.

Where we are unable to meet the proposed 20 working day deadline, if for example further investigation is required, we will contact you to inform you of progress of your complaint and agree a completion date with you.

In all instances your feedback will be investigated by a senior member of staff and that person will contact you. We will also ensure that if required additional training and development will be provided to our staff and that lessons are learned from what has happened, to prevent it happening again.

13. General Data Protection Rules

Please refer to Annex A attached for data management rules applicable to this contractual agreement.

For the purposes of this agreement the following party will be responsible for adherence to the legislation referred in Annex A

1. **Data Controller: Customer**
2. **Data Processor: HR Connect**
3. **Sub Processor: N/A**

Schedule of Processing, Personal Data and Data Subjects (Annex A)

The contact details of the Controller's Data Protection Officer (or representative) are on the Customer Order Form.

The contact details of the Processor's Data Protection Officer (or representative) are:

Email: DPO@csltd.org.uk
Post: Data Protection Officer, Commercial Services Group, 1 Abbey Wood Road, Kings Hill, West Malling, ME19 4YT

The Processor shall comply with any further written instructions with respect to processing by the Controller.

Any such further instructions shall be incorporated into this Schedule.

Data processing details

Processing of the Protected Data by the Processor under the Contract shall be for the subject-matter, duration, nature and purposes and involve the types of personal data and categories of Data Subjects set out in this Schedule.

Description	**Details**
Identity of the Controller and Processor	The Parties acknowledge that for the purposes of the Data Protection Legislation, the Customer is the Controller and that HR Connect is the Processor as defined in the Contract.
Subject matter of the processing	The processing is needed in order to ensure that the Processor can effectively provide the service(s) as outlined in the Contract and Service Level Agreement.
Duration of the processing	Processing will take place as for the period defined in the contract.
Nature and purposes of the processing	The purpose of processing is to fulfil HR Connect's obligations in delivering the service(s) outlined in the Contract and Service Level Agreement. Data will be input by the Customer's administrators, ID Verifiers and Applicants onto the EmploymentCheck system and via the YOTI integration using the YOTI smartphone app or embedded IDV route. Data will be transferred from YOTI's system to Cantium's EmploymentCheck system upon completion of the Digital Identity check if this route is used. No personal data will be transferred directly from the EmploymentCheck system to the Yoti systems. Instead personal information will be entered directly into the Yoti system. YOTI's Identity Verification service allows one time verification of a living person's identity. This verification is conducted under the rules set out in the Department for Culture, Media and Sport's UK digital identity and attributes trust framework (known as the "UKDIAFT").

	HR Connect will provide data processing services including: • Hosting the EmploymentCheck application. • Application maintenance and development. • Secure user redirection to Yoti's online solution for the Digital ID process. • Evidence document storage to allow for Right to Work evidence to be downloaded from the EmploymentCheck system for a maximum of 6 months after a RtW check has entered the 'Application Archived' status. It's agreed that the customer is responsible for storing this Right to Work evidence for the duration of employment + 2 years on their own HR system, separate from the EmploymentCheck system. • Purging of personal and sensitive data, including Right to Work evidence, 6 months after a check has been archived by the Customer's admin users or the systems automated archive function (the Customer can determine how long a RtW check remains in the Result Received status before being auto-archived). • Reporting for the purposes of billing for services provided. • Reporting for the purposes of providing Key Performance Indicator reports for the customer. <u>Cantium Data Security and Data Centre Location</u> In order to facilitate the maintenance, development and investigation of system issues, identified Cantium technical staff may access data stored within the system database to perform tasks in the interests of the Customer for the purposes of: • Data analysis and report generation • Insertion and alteration of data to facilitate Customer requests • Correction of system issues • Extraction of data to facilitate Customer requests • Research facilitating improvements and enhancements to the system In all cases, only the minimum of data required will be accessed and no data will be altered, inserted, or removed without the express written permission from the Data Controller. All staff accessing the data are trained and vetted in line with HR Connect policy. The EmploymentCheck solution uses a SSL certificate for secure transmission of data between client terminals and the dedicated servers which are utilised for no other purpose than for the EmploymentCheck system. Cantium data hosting is provided by ANS group – all EmploymentCheck datacentres are located in Manchester, UK. Both Cantium and ANS Group are ISO 27001 accredited – further

	info relating to data centre security can be found here. YOTI Information Collection and Use YOTI collect information from those using YOTI's Identity Verification service to send clients an assertion of identity so that they can conduct digital DBS, Right to Work or Right to Rent checks on you. YOTI collect some device information as part of their analytics. If YOTI suspect your document is fraudulent YOTI may keep it in an internal database to ensure that (a) this document is never accepted by YOTI and (b) is used to improve their anti-fraud techniques. If YOTI find a suspected fraudulent document, they may share this with relevant law enforcement and anti-fraud bodies. YOTI do not process your data: (i) for any marketing purposes; (ii) to create aggregate data sets which can identify you; or (iii) in any way that you have not agreed to or is not explained in this privacy policy. YOTI Limited will provide data processing services including: - *Identity Document date extraction.* YOTI extracts data from your identity documents to establish your identity. YOTI extracts your names, date of birth, document number, type of document, document expiry date and photo. - *Selfie.* YOTI captures images of your face to conduct liveness tests to check that you are a real person and not someone trying to impersonate you. YOTI takes a scan of your face to create a biometric template of your face, which YOTI stores securely. A biometric template is a digital map of your face. YOTI perform face matches to compare your selfie with the photo on your identity document. When you add a document YOTI compares its photo with the face template to make sure users only upload their own documents. As YOTI are capturing your biometrics, YOTI will ask you to consent to this. If you do not want to consent then you will not be able to complete the digital identification process and you can speak to the HR vetting company or employer / volunteer organisation you are working with about other routes you can use for verification. - *Third Party data sources.* YOTI may send information to trusted third parties, such as Credit Reference Agencies, to look for other information about the individual that helps Yoti verify the identity.

	- *Information on how YOTI verified your identity.* This information creates an audit trail stating how YOTI verified your identity. It is sent to their client as part of their digital service for or about the user. This information includes your IP address when using YOTI's Identity Verification service. - *Feedback and Email.* If your user sends feedback to Customer Support YOTI will use that information to get in touch with the user to resolve the issue or to acknowledge the feedback. <u>YOTI Security and Data Location</u> Yoti keeps the Identity Verification data encrypted in their UK datacentres and occasionally the data could be sent to their security centre in India for further checks. In this instance, Yoti transfer personal data (via remote access) used for identity checks under UKDIATF to our Yoti India security centre. The relevant personal data is that which is uploaded by the individual end user (ID document, selfie image) and it is used to perform the identity checks. This is an international transfer of data and subject to the protections of Chapter V of the UK GDPR. As data exporter, Yoti has SCCs (+ UK Addendum) in place as well as a transfer impact assessment to ensure any data transferred is subject to adequate safeguards. This transfer is temporary and the data is deleted within 28 days from Yoti systems - any ongoing storage of data for the client's benefit is within Yoti's UK data centres (and is subject to client managed retention). Yoti rely on the new EU SCCs issued on 4 June 2021 for transfers to India. Yoti are audited annually by KPMG against the SOC2 Type 2 Security control standards and Yoti also maintain their ISO 27001 certification. Yoti has the decryption keys for encrypted data, but Yoti have access controls in place to limit which staff have access to the server. Yoti staff may need access data to troubleshoot problems and manage the server in emergency events. If Yoti decide or are obliged to send or store personal information in another country, Yoti will update this section to describe the protections Yoti has put in place.
Type of Personal Data being Processed	Personal data relating to applicant users including: • Name • Date of birth • Contact details • Employment details

	• ID document details including images • Immigration status • Biometric Face Scan (if Digital ID used)
Categories of Data Subject	These will include: • Prospective and current employees (and those undertaking work for, or on behalf of the Customer), service users and clients of the Customer
Plan for return and destruction of the data once the processing is complete UNLESS requirement under union or member state law to preserve that type of data	In line with the contract, at the written direction of the Controller, unless a copy is specifically required to be retained by the Processor for audit or compliance purposes in performance of its obligations for up to six (6) years, the Processor will delete or return Personal Data (and any copies of it) to the Controller on termination of the Contract unless the Processor is required by Law to retain the Personal Data. <u>HR Connect's Data Retention</u> An automated purging process will identify records which have reached the end of their retention schedule. Purging of personal and sensitive data will be conducted 6 months after a check has been archived by the Customer's admin users or the systems automated archive function. It's agreed that the customer is responsible for storing this evidence for the duration of employment + 2 years separately from the EmploymentCheck system. Once personal and sensitive data has been removed from the application, a record of the Right to Work check will be kept on the EmploymentCheck system until the end of the contract term. <u>Yoti's Data Retention</u> The maximum amount of time that Yoti will have access to data is 28 days; after which Yoti either: • delete data completely or. • delete data in line with the requesting company's privacy notice. Yoti will hold data for 28 days following the completion of the Identification Verification session and do not have access to view the data after this time. Yoti may in some instances keep data for longer than 28 days where there are legal, regulatory or anti-fraud reasons to keep data for a longer period of time. Under these circumstances, users would not be able to exercise your right to erasure. Users can contact us to delete data by emailing privacy@Yoti.com. <u>Yoti Deletion Rights</u> In certain circumstances the users are entitled to ask us to delete the personal information Yoti holds about them. Yoti may keep data

	for longer than 28 days where there are legal or regulatory reasons to do so. <u>Yoti Objection Rights</u> In certain circumstances the users are entitled to object to Yoti processing personal information. There are unlikely to be any circumstances when this right applies to Yoti Identity Verification service personal information. If the user wants to contact us about their objection rights, please email: privacy@Yoti.com. <u>Yoti Restriction Rights</u> In certain circumstances the users are entitled to ask Yoti to restrict Yoti's processing of your personal information. Users can ask us to do this if: • they dispute the accuracy of personal information; • their processing is unlawful but they prefer restriction to deletion; • Yoti no longer need the information but the users need it for legal reasons; or • The user has objected to their processing and Yoti are still dealing with this objection. If users want to contact Yoti about their restriction rights, please email: privacy@Yoti.com

Sub-processors authorised

HR Connect utilise the following Sub-Processor(s):

- ANS Group Limited – Server Hosting and Infrastructure Support
- YOTI Limited - Digital Identity Service Provider
- Cantium Business Solutions – IT Support

Technical and organisational security measures

The Supplier shall implement and maintain the following technical and organisational security measures to protect the Protected Data:

In accordance with the Data Protection Laws, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the processing of the Protected Data to be carried out under or in connection with the Contract, as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons and the risks that are presented by the processing, especially from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to the Protected Data transmitted, stored or otherwise processed, the Supplier shall implement appropriate technical and organisational security measures appropriate to the risk, including as appropriate those matters mentioned in Articles 32(1)(a) to 32(1)(d) (inclusive) of the GDPR.