Service Level Agreement (SLA)

Umbrella Body Service Digital ID for DBS 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, 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:

Use of the EmploymentCheck integration with a partnered, certified third-party DVS - YOTI to enable Digital ID checks to be undertaken for the purpose of ID Verifying Applicants requiring DBS Standard, Enhanced or Basic applications.

The YOTI integration provides two routes for conducting Digital ID checks through the EmploymentCheck system: via an embedded web solution and via a smartphone app method. Both methods are covered by this SLA as standard.

For DBS Standard and DBS Enhanced applications, the Level of Confidence requested to be obtained through YOTI will be HIGH.

For DBS Basic applications, the Level of Confidence requested to be obtained through YOTI will be AT LEAST MEDIUM.

6. Customer Responsibilities

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

- Create DBS Standard, Enhanced and Basic applications and select whether a Digital ID check completed through YOTI is required for the application.
- Ensure maintained adherence to the DBS Code of Practice and/or Basic Check Processing Standard at all times including whilst using the Digital ID check integration with YOTI.
- To maintain complete confidentiality at all times and adhere to the Data Protection Act 2018, as amended.
- Understand the role of the relying party and comply with all requirements relating to the use of Digital ID checks for carrying our DBS Standard, Enhanced and Basic applications: Digital ID Guidelines
- Use of the Digital Identity functionality on EmploymentCheck utilises an integration with a third-party Digital Verification Service (DVS) - YOTI. Use of the functionality ensures compliance with YOTI's terms and conditions which can be found below:

  https://www.yoti.com/privacy/

  https://www.yoti.com/privacy/identity-verification-ukdiatf/

7. Service Provider Responsibilities

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

- To provide an online DBS solution that is accredited by the DBS to conduct Digital ID checks via a certified Digital Verification Service (DVS) - YOTI.
- Enable secure administrative access to the EmploymentCheck system allowing the management of DBS checks being undertaken via the Digital ID route.
- 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 changes will be documented and communicated to the customer.
- Notice will be provided on planned maintenance.
- Ongoing support will be provided by YOTI and YOTI themselves will be responsible for maintaining their own infrastructure and certifications.

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-Related Incidents and 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)

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

   [See Order Form]

2. 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

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

4. 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 and their clients onto the EmploymentCheck system and via the YOTI integration using the white-labelled 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. 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 (via a third-party provider) • Application maintenance and development • Secure user redirection to YOTI's online process. • Purging of personal and sensitive data 24 months after a check has been archived by the Customer's admin users or the systems automated archive function in line with the DBS compliance requirements. • Purging of the CRB01 file which stores a record of all data submitted to the DBS during countersigning 12 months after submission in line with DBS compliance requirements. • Reporting for the purposes of billing for services provided • Reporting for the purposes of providing Key Performance Indicator reports for the customer • Transfer of the user session to YOTI's SDK and receipt of data from YOTI which has been used to conduct a Digital Identity check on the Applicant. <u>YOTI Information Collection and Use</u> 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's Identity Verification service is a one off verification journey, so YOTI do not create an account for Applicants. YOTI also 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 name, date of birth, address (if present), 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. - *Address.* You may assert your address to YOTI, and YOTI may check it against the records held by a Credit Reference Agency. The check will be in the name of YOTI Limited. Or YOTI may take your address from an identity document that you have submitted to us. - *Third Party data sources.* YOTI may send your information to trusted third parties, such as Credit Reference Agencies, to look for other information about you that helps us verify your 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 you. This information includes your IP address when using YOTI's Identity Verification service. - *Feedback and Email.* If you send feedback to their Customer Support YOTI will use that information to get in touch with you to resolve your issue or to acknowledge your feedback. In order to facilitate the maintenance, development and investigation of system issues, identified HR Connect 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. <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. 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 your 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 your 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. • Gender. • Address. • Date of birth. • ID document details.
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. YOTI's Data Retention YOTI delete your data in line with the requesting companies (the company asking you to perform the checks) retention period. The maximum amount of time that YOTI will have access to your data is 28 days; after which YOTI either: 1. delete your data completely or. 2. delete your data in line with the requesting company's privacy notice. YOTI will hold your 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 your data for longer than 28 days where there are legal, regulatory or anti-fraud reasons to keep your data for a longer period of time. Under these circumstances you would not be able to exercise your right to erasure. You can contact us to delete your data by emailing privacy@yoti.com YOTI Deletion Rights In certain circumstances you are entitled to ask us to delete the personal information YOTI holds about you. YOTI may keep your data for longer than 28 days where there are legal or regulatory reasons to do so. YOTI Objection Rights In certain circumstances you are entitled to object to YOTI processing your personal information. There are unlikely to be any circumstances when this right applies to YOTI Identity Verification service personal information. If you want to contact us about your objection rights, please email: privacy@yoti.com YOTI Restriction Rights In certain circumstances you are entitled to ask us to restrict YOTI's processing of your personal information. You can ask us to do this if: • you dispute the accuracy of your personal information;

	• their processing is unlawful but you prefer restriction to deletion; • YOTI no longer need the information but you need it for legal reasons; or • you have objected to their processing and YOTI are still dealing with this objection. If you want to contact us about your restriction rights, please email: privacy@yoti.com

Sub-processors authorised

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

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

Technical and organisational security measures

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

1.1 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.