Service Level Agreement (SLA)

Umbrella Body Service Disclosure and Barring Service Check (including Digital ID and In Branch Verification)

EmploymentCheck is a trading style of **Commercial Services Kent Ltd** (Reg No. 5858177) a company wholly owned by Kent County Council. Registered in England and Wales.
Registered Office: 1 Abbey Wood Road, Kings Hill, West Malling, Kent ME19 4YT.

1. Agreement Overview

This Agreement represents a Service Level Agreement ("SLA" or "Agreement") between HR Connect EmploymentCheck and the Customer for the provisioning of the Umbrella Body Disclosure and Barring (DBS) 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: EmploymentCheck, 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 Standard, Enhanced and Basic DBS checks including Barred List checks (where applicable).

- Use of the EmploymentCheck solution is complete with an optional integration with a partnered, certified third-party Digital Verification Service Provider (DVSP) 'Yoti' to enable digital ID checks to be undertaken for the purpose of ID verifying applicants requiring a DBS check.

- Use of the EmploymentCheck solution is complete with an optional integration with Yoti and the Post Office to offer an In Branch Verification Service (IBV). This option allows for IBV checks to be conducted by DBS applicants in Post Office branches, offering an alternative means of ID verification.

Your Access Allows

- The Customers 'Admin' users can set up online applications via the EmploymentCheck system for an applicant requiring a Disclosure and Barring Service check. A bulk upload facility is available upon request.
- The Customers 'Applicant' users can complete and submit a DBS application form online through the EmploymentCheck system.
- The Customers 'ID Verifier' users can submit manual ID verification through the EmploymentCheck system.
- The Customer has access to integrated external ID Validation checks if any Standard or Enhanced level DBS check must go down Route Two, namely checking the ID via an external ID validation process. Additional charges will apply.
- The Supplier countersigns and submits completed checks to the DBS under our registered body number via secure e-Bulk. The Customer will be notified of any checks that cannot be processed due to application ineligibility.
- The EmploymentCheck system manages and tracks each application through the process once the form has been submitted through the e-Bulk system.
- The Customer will receive an electronic notification of disclosure results to the nominated manager.
- The Customer has access to grant ID Verifier access to the system for the purpose of undertaking manual documentation verification as part of the DBS application process.
- The Customer can process Update Service checks on a transactional basis via an optional integrated function. An additional charge for Update Service checks will be applicable.
- The Customer can configure DBS applications to be verified digitally, via an integrated solution provided by Yoti Ltd, an accredited DVS.
- The Customer can configure DBS applications to be verified via an In Branch Verification (IBV) process, provided by Yoti Ltd in partnership with the Post Office.
- The Customer has access to a standard reporting suite (as amended from time to time) for easy analysis of DBS checks. EmploymentCheck's standard report suite consists of the following reports:
    - Billing Report - DBS Checks
    - Billing Report - DBS Update Service
    - Billing Report - Digital ID Checks
    - Billing Report - Route 2 External ID Check Checks
    - Billing Report - IBV Checks
    - DBS Application Status - Awaiting Applicant
    - DBS Application Status - Awaiting Digital ID

- DBS Application Status - Awaiting IBV
- DBS Application Status - Awaiting ID Verifier
- DBS Application Status - Receipt Received
- DBS Application Status - Holding
- DBS Disclosure Results
- DBS Certificates Issued with Content

6. Customer Responsibilities

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

- Create and manage DBS applications via a secure online form.
- To comply with the Standard and Enhanced Check: DBS Code of Practice and the Basic Check: Processing Standards at all times.
- Maintain confidentiality and adhere to the Data Protection Act 2018 as well as any other relevant legislation and guidelines, at all times. EmploymentCheck reserves the right to carry out audits and/or visits to ensure the Customer is fully compliant with all terms of their contract and the DBS Code of Practice. Non-compliance may lead to suspension of services.
- Ensure there is a legal requirement to request a DBS check in line with DBS Checks guidance for employers before initiating a check.
- Ensure the role has been assessed for the right level of check, workforce and appropriate barring list information and will adhere to the Standard and Enhanced DBS eligibility guidance.
- Ensure eligibility has been checked and where relevant have ensured the role meets the DBS definition of a true volunteer.
- Ensure eligibility of the role has been checked against the DBS Home-based position definition.
- 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/
- Ensure all applicants for relevant positions or employment are notified in advance of the requirement for a Disclosure.
- Ensure that any applications are completed accurately and in full.
- Ensure applicant data is not amended on their behalf and instead, roll back the application to the applicant, for them to amend their own personal data.
- Notify all potential applicants of the potential effect of a criminal record history on the recruitment and selection process and any recruitment decision.
- Maintain a written policy on the suitability of ex-offenders for employment in relevant positions. This should be available upon request to potential applicants at the point of requesting them to complete a DBS application form or asking consent to use their information to access a DBS service. An example policy can be found in **Annex A**.
- Ensure that a result received as part of an application submitted electronically is not reproduced in such a way that it infers that it is a certificate issued by the DBS.
- Do not disclosure information contained within a DBS Certificate unless the recipient is entitled to receive this.
- Discuss the content of the disclosure with the applicant before withdrawing any offer of employment.
- If further information is required from the police due to disclosure information being limited, it is the responsibility of the Customer to pursue this with Police Legal, requesting support from the counter signatory as required.
- Not knowingly make a false statement for the purpose of obtaining or enabling another person to obtain a Certificate.

- As a DBS Umbrella Body, EmploymentCheck must ensure that all users of the EmploymentCheck system undertake appropriate training. Training is required to provide assurance that DBS applications are completed accurately, ensuring that all data fields determined by the DBS as mandatory are completed in full. We are also obliged under the DBS Code of Practice to ensure that where evidence checkers complete any part of the administration of the application process, sufficient training has been provided to enable the same degree of accuracy required by DBS of the counter signatory. In order to comply with this requirement, new ID Verifier's must view EmploymentCheck's ID Verification training video before access is granted by the Customer. This is also outlined in the Terms and Conditions within EmploymentCheck.
- Ensure that access to the system is limited to those who require it as part of the recruitment and vetting process.
- Each log-in identifier is specific to the individual trained person. The Customer must have systems in place to ensure identifiers are not made available to any other persons.
- Inform HR Connect immediately should an Admin user account no longer be required.
- To comply with EmploymentCheck's Umbrella Body DBS Procedures and System User Guides as amended from time to time.
- Access to the DBS service requires the Customer to accept the Yoti Ltd Terms and Conditions where the Route 2 External ID Check is required.
- If utilising the optional Update Service functionality, then all checks must be completed in line with the DBS Update Service: employer guide - GOV.UK.
- Pay all relevant fees within 30 days of receipt of invoice. If fees are not paid within 30 days, EmploymentCheck reserves the right to withdraw access to the service.

7. Service Provider Responsibilities

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

- Provide an online DBS solution with e-Bulk that is accredited by the DBS and Ministry of Justice (MOJ).
- Provide an online DBS solution that is accredited by the DBS to conduct Digital ID checks via a certified Digital Verification Service Provider - Yoti.
- Provide an In Branch Verification (IBV) service via Yoti Ltd and the Post Office, to offer an alternative option for ID verification.
- Provide an external ID Validation check solution for checks required to go down Route Two. An additional charge for external ID verification checks will be applicable.
- Provide an optional integrated functionality to conduct Update Service checks. An additional charge for Update Service checks will be applicable.
- Ensure secure hosting for the system in an ISO27001 accredited environment.
- Enable secure access to EmploymentCheck for up to 3 designated Super Admin. users. Training deemed necessary by the Service Provider will be mandatory. Any additional training requirements are available at an additional cost.
- To electronically submit completed DBS application forms no later than the end of business on the next working day following submission by the ID Verifier (this is based on the EmploymentCheck team being in full receipt of the disclosure information including confirmation of eligibility). A working day is defined as between 8.30am – 5.00pm excluding public holidays and concessionary days observed by HR Connect.
- Where errors are identified or further information is required at e-Bulk stage EmploymentCheck will return the application to the designated 'manager' as identified by the Customer on the DBS application. If no response is received from the Customer within 10 working days the application will be archived.
- Liaise directly with the designated 'manager' when the DBS request additional information from us regarding a submitted DBS check.
- Notify the designated 'manager' of clear disclosures via email including the level of check requested.
- Notify the designated 'manager' of disclosures with additional information via email. Any challenges to the content supplied within a returned DBS check must be taken up directly with the DBS by the applicant.

- Ensure compliance with the DBS Code of Practice at all times.
- Provide the Customer with an example written policy on the suitability of ex-offenders for employment in relevant positions. An example policy can be found in **Annex A**.
- Provide a written policy on the secure handling of information provided by DBS, electronically or otherwise, and make it available to applicants at the point of requesting them to complete a DBS application form or asking consent to use their information to access any service DBS provides. This is contained within the Privacy Notice on EmploymentCheck.
- Ensure applicants for a DBS check are made aware of the Standard and Enhanced Check: DBS Code of Practice and the Basic Check: Processing Standards and provided with a copy on request.
- Handle all information provided by DBS, as a consequence of applying for a DBS product, in line with the obligations under Data protection Act 1998.
- Handle all DBS related information provided by the applicant in line with the obligations under Data Protection Act 1998.
- Deactivate all user accounts which have not been active for over 6 months. Should Admin accounts need to be reactivated, the Customer will do so upon request from the user if suitable.
- Maintain an ongoing relationship with Yoti to ensure the continued provision of Yoti services.
- Raise support queries with Yoti directly where required.
- Maintain all standard email templates and reports. The Customer will be assigned the standard email templates for correspondence of all stages of the application lifecycle along with standard suite of reports.
- Provide system training videos and user guides to the Customer.
- Respond to all Service Support queries within 3 working days (as outlined below).
- Meet response times associated with Service-Related incidents (as outlined below).
- Appropriate notification to Customer for all scheduled maintenance.
- 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 or enhancements will be documented and communicated to the customer.
- Notice will be provided in advance of planned system 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 Support 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 B** 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 to in **Annex B**.

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

Example Policy on Suitability of Ex-offenders for Employment (Annex A)

Commercial Services Kent Policy Statement on the Recruitment of Ex-Offenders

As an organisation using the Disclosure and Barring Service (DBS) to assess applicants' suitability for positions of trust, Commercial Service Kent (CSK) complies fully with the DBS Code of Practice and undertakes to treat all applicants for positions fairly. It undertakes not to discriminate unfairly against any subject of a Disclosure on the basis of conviction or other information revealed.

CSK is committed to the fair treatment of its staff, potential staff or users of its services, regardless of race, gender, religion, sexual orientation, responsibilities for dependants, age, physical/mental disability or offending background.

We actively promote equality of opportunity for all with the right mix of talent, skills and potential and welcome applications from a wide range of candidates, including those with criminal records. We select all candidates for interview based on their skills, qualifications and experience.

A Disclosure is only requested after a thorough risk assessment has indicated that one is both proportionate and relevant to the position concerned. For those positions where a Disclosure is required, job adverts and recruitment briefs will contain a statement that a Disclosure will be requested in the event of the individual being offered the position.

For roles requiring an enhanced or standard disclosure (exempt from Rehabilitation of Offenders Act) you will be asked questions at application stage with regards to any cautions or convictions (including spent convictions) and you will be asked to provide details of these (including offence dates, dates of conviction/caution, offence types and sentences received).

Where a Disclosure is to form part of the recruitment process, we encourage all applicants called for interview to provide details of their criminal record at an early stage in the application process. We guarantee that this information is only to be seen by those who need to see it as part of the recruitment process.

For roles requiring a Basic check and for roles where no DBS check is required (roles covered by the Rehabilitation of Offenders Act) you will only be asked questions once you have accepted a conditional offer of employment and as part of the pre-employment process. We will only ask about ‘unspent’ convictions as defined in the Rehabilitation of Offenders Act 1974. Any information provided will be fully considered in consultation with the applicant before a decision is made.

We ensure that all those in CSK who are involved in the recruitment process are fully supported to identify and assess the relevance and circumstances of offences by members of staff who have received appropriate guidance and training in the relevant legislation relating to the employment of ex-offenders, e.g. the Rehabilitation of Offenders Act 1974.

At interview, or in a separate discussion, we ensure that an open and measured discussion takes place on the subject of any offences or other matter that might be relevant to the position. Failure to reveal information that is directly relevant to the position sought could lead to withdrawal of an offer of employment.

We make every subject of a DBS Disclosure aware of the existence of the DBS Code of Practice and make a copy available on request.

We undertake to discuss any matter revealed in a Disclosure with the person seeking the

position before withdrawing a conditional offer of employment.

CSG reserves the right to judge each case on its merits within the following parameters:

- Nature of offence(s) listed and / or police information disclosed
- Relevance to the post applied for
- Length of time elapsed since incident
- Whether the matters disclosed form any pattern
- The circumstances under which the offence was committed
- Changes in the applicant's personal circumstance
- Openness of declaration during the recruitment process
- Country of conviction
- Decriminalisation
- Remorse

Matters revealed in a Disclosure will be risk assessed as outlined in the CSK Disclosure and Barring Service (DBS) Procedure.

Having a criminal record will not necessarily bar you from working with us. This will depend on the nature of the position and the circumstances and background of your offences.

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

1. The contact details of the Controller's Data Protection Officer (or representative) are on the Customer 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, 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. Where the digital identity or in branch verification services are in use, data will be input via the Yoti integration. 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. • Secure transfer of data to the DBS (as required), including for conducting Update Service checks if utilised. • 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 data to and receipt of data from identity authentication check service provider for the purposes of ID authentication (where ID authentication check service used) – information required for ID authentication only. • 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. • Transfer of ID documentation data as part of an in branch verification service provided by Yoti and the Post Office. 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 or In Branch Verification checks. Data will be transferred from Yoti's system to the EmploymentCheck system upon completion of the digital identity or in branch verification check. Yoti's identity verification service allows one time verification of a living person's identity. For DBS verifications, there are 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"). In branch verifications are covered by Yoti's standard terms and conditions: Yoti Identity Verification Privacy Notice

	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>EmploymentCheck Security and Data Location</u> The EmploymentCheck solution is hosted by ANS Group Limited, ANS datacentres are located in Manchester, UK. Application backups are also stored in ANS' Manchester based data centres. EmploymentCheck backups are managed by ANS Group Limited via their Secure Backup Gateway product which is powered by Commvault. <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 DBS check applicants, ID verifiers and system administrative users including: • Name, gender, address, address history and contact details • Date and place of birth • Employment and/or educational details • Licences or permits held • ID document details • Criminal record For the Yoti digital verification or in branch verification checks, biometric face scans may also be collected.
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>Yoti's Data Retention</u> 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 <u>Yoti Deletion Rights</u> 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. <u>Yoti Objection Rights</u> 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 Ltd – IT Provider
- ANS Group Limited – Server Hosting and Infrastructure Support
- Yoti Limited – Route 2 External ID Check for Standard/Enhanced DBS checks
- Yoti Limited – Digital Verification Service and In Branch Verification Service
- Ideal Postcodes – Postcode Lookup Integration

Technical and organisational security measures

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

The EmploymentCheck solution uses an 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. The solution is protected by encryption of data at rest and in transit and MFA is mandated for all privileged accounts which are controlled by strict Role Based Access Contols (RBAC).

The system is fully hosted on a dedicated server with an ISO27001 certified datacentre who were procured in line with the requirements set out by the DBS and specific security data related to system access is encrypted at rest via MD5 encryption. Our hosting provider is ISO 9001, 2000 and 27001 certified and are audited on an annual basic by both external independent quality assessors and by Vendor partners and undergo regular penetration testing in line with ISO 27001 compliance.

Access to data on the system is tightly controlled and only authorised personnel have access to the minimum data/information required to perform their designated tasks. The database itself is password protected to prevent any unauthorised access. When data is processed and transmitted to the DBS the EmploymentCheck system complies with and where possible exceeds all DBS approved cryptographic requirements to ensure secure transmission of data between itself and the authorities. All data is transferred over the FTPS protocol and an element of the transmission is encrypted using an AES-256 algorithm to ensure message integrity.

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.