The Blade
Abbey Street
Reading RG1 3BA
0118 466 0822
www.trustid.co.uk

Proposal to: NHS South, Central and West CSU

Date: 04 March 2025

Proposal Summary

TrustID is pleased to provide this proposal to supply our Cloud identity checking services which includes:

- Commercial details
- Details about the services provided
- TrustID terms and conditions
- Third party licence terms and conditions

Customer Information

Customer name: NHS South, Central and West CSU

Customer contact: [redacted]

Proposal reference: 25-21977

Omega House
Eastleigh
SO50 5PB

Commercial Details

Services are supplied on a per-document basis. Each document or share code checked uses one credit. Credits are purchased in pre-paid bundles and have two-year validity from date of purchase, after which unused credits will expire. Access is to be provided to the following services.

Services (Scope of Work contains a full description of services)

Digital Scheme Identity Verification (RTW and DBS)
Document Verification
eCloud
Electronic identity verification (IDV) - Address checking
Face Biometrics

Billing Terms: In advance
Payment Terms: 30 days from invoice date

Volume of Credits [redacted]
Price per Credit [redacted]
Total [redacted]

All prices are exclusive of VAT

TrustID Scope of Work

Digital Scheme Identity Verification (RTW and DBS)

Digital Scheme Identity Verification (supporting Digital DBS and Right to Work schemes in accordance with UKDIATF and GPG45)

TrustID is a certified Identity Service Provider. For checks performed under a Digital Scheme, TrustID will provide a "Level of Confidence" (as defined by GPG45) in the applicant's identity, allowing the Relying Party to proceed with a DBS or RTW check.

Where a Basic DBS or RTW check is required, TrustID will attempt to establish at least a Medium Level of Confidence in the identity. Where a Standard or Enhanced DBS check is required, TrustID will attempt to establish at least a High Level of Confidence in the identity. Where the minimum requirement of confidence is not reached, TrustID will return a result indicating the Level of Confidence has not been met.

Checks requiring a High Level of Confidence will also require either eCloud or Address Checking.

Profiles supported under Medium Levels of Confidence are M1A, M1C and M2C. Profiles supported under High Levels of Confidence are H1A and H2B.

Document Verification

TrustID supports the verification of over 16,000 global government-issued identity documents, including:
- International Passports
- Government-issue ID cards
- Visas and Biometric Residence cards
- International Driving licences

TrustID's Document Verification service performs automated machine-based checks and document fraud analysis on identity document images. Documents which do not pass these checks are automatically escalated to the TrustID document analysts for manual assessment.
Checks performed on identity documents submitted by any route include:
- Machine Readable Zone (MRZ) formatting and algorithms
- UK Driver number format and cross check
- Expiry date
- UK Fraudulent document database
- TrustID document watchlist

For images submitted by TrustID GuestLink, the following additional checks are performed:
- Genuine document presence to detect copies or screen grabs
- Photo check to look for signs that the face has been overlaid or changed
- Detail checks matching alignment, colour, symbols and other details present on a genuine version
- Integrity check to identify if the image file has been edited

For each supported document submitted for verification, TrustID will provide one of the following assessment outcomes:
- Accepted – no suspicious characteristics identified
- Failed – suspicious characteristics identified (e.g. fake document, chip inconsistencies)
- Rejected – poor image quality
- No validation – validation not available, or unsupported document type

eCloud

eCloud enables document holders in possession of a biometric document to open the RFID chip embedded in their document. The country signing certificate on the chip will be checked, and the data contained on the chip will then be cross-referenced against the image and the Machine Readable Zone displayed on the biodata page of the document.

eCloud requires the installation of an app on the applicant's device (Android and iOS are supported). Applicants are guided to the appropriate app store during the GuestLink upload process.

Electronic identity verification (IDV) - Address checking

The name of the person on the document and their claimed address will be checked against various external data sources, for example, credit file, electoral roll and CCJ register. A check will also be made to identify if the person is marked as deceased against any of these sources.

Where the IDV check is used as part of a Digital Scheme check, one of the following results will be returned:
- Match – at least one record indicating the data subject lives at the claimed address
- No IDV Match – no records indicating the data subject lives at the claimed address
- Deceased – records indicate that data subject at the claimed address is deceased

Where the IDV check is not part of a Digital Scheme check, one of the following results will be returned:
- 2 Match – at least two records indicating the data subject lives at the claimed address
- 1 Match – one record indicating the data subject lives at the claimed address
- No IDV Match – no records indicating the data subject lives at the claimed address
- Deceased – records indicate that data subject at the claimed address is deceased

By accepting this Proposal, you authorise TrustID to engage LexisNexis Risk Solutions (LNRS) as a Third-Party Processor of Data for the provision of this service. Refer to paragraph 5.5 below for link to LNRS terms. To comply with LNRS's requirements, TrustID will contact the customer within 45 days of the contract start date to confirm that address checks undertaken during the initial period were performed in accordance with LNRS's acceptable use cases. TrustID may also contact customers at any point during the contract to confirm the continued compliance.

Face Biometrics

Performs liveness and facial recognition checks on a live selfie captured by the applicant to confirm they are present at the point of capture, and that the selfie is the same person as the photograph in the document being submitted for verification.

Face biometrics uses automated machine-based checks for both liveness and face matching, with manual re-assessment on face matching checks should automated checks fail.

Accessing the service

Users access the service and initiate checks using the TrustID web portal or the Application Programming Interface (API). Users may upload images of documents directly to TrustID or use TrustID to invite their applicants to submit their own images and other data directly.

With prior agreement Customers may use a 3rd Party platform to submit checks and retrieve results on the Customer's behalf. The 3rd Party is responsible for ensuring the availability of this connection and for the safeguarding of data in transit between the Customer and TrustID.

Results will be available to download for 7 days, after which all personally identifiable information will be deleted by default, unless a longer availability period has been agreed.

Customer Acceptance Form

Proposal reference for: NHS South, Central and West CSU**:** 25-21977

The customer named above (the "Customer") agrees to purchase the products set out in this Proposal on behalf of itself and its customer. Once the Customer's Offer is accepted by TrustID Ltd, it will constitute a legal agreement between the parties subject to, and governed by,the Terms and Conditions which shall take precedence over any conflicting terms or conditions in any other document in relation to the products set out in the Proposal.

Future orders may be accepted but will be subject to these Terms and Conditions subject to:
1) additional and where applicable variable prices set out in the acceptance of the Customers order by the Supplier; and
2) any variation, amendment or extension of those Terms and Conditions as set out in the acceptance of the Customer Order by the Supplier.

The Contract shall commence on the Commencement Date and shall be for a minimum term of 24 months and thereafter subject to the above provisions relating to future orders shall continue until such time as either party gives the other party not less than 7 days prior written notice. Where TrustID terminates the contract under this provision Customer shall be entitled to a refund of any credits remaining on the date of termination. Where Customer terminates the contract under this provision Customer shall not be entitled to a refund of any credits remaining upon the date of termination.

Signed: [redacted]

Print name: [redacted]

Position: [redacted]

Date: 04-Mar-2025

PO Number:

TrustID Terms & Conditions

1. INTERPRETATION

1.1 Definitions. In these Conditions, the following definitions apply:

Business Day: a day other than a Saturday, Sunday or public holiday in England, when the banks in London are open for business.

Commencement Date: the date on which the Order, signed by the Customer is accepted in writing by the Supplier.

Compromised Documents: means any document that the Service identifies as suspicious.

Conditions: these terms and conditions as amended from time to time in accordance with clause 13.

Contract: the contract between the Supplier and the Customer for the Licence and Services and for the supply of the Services in accordance with these Conditions.

Customer: the person, organisation or firm whose order the Supplier has accepted and agrees to provide the Service under the terms of these Conditions.

Fee: as defined at clause 4.1

Force Majeure Event: has the meaning given to it in clause 9.

Login Details: as defined at clause 3.2

Order: the Customer's order for the supply of the Services to itself or its customers, being the Scope of Work once signed by the Customer and any subsequent Order issued by the Customer which shall also be subject to these Terms and Conditions.

Personal Data: has the meaning given in the GDPR;

Scope of Work: means the Scope of Work set out above setting out the details of the Services to be provided by the Supplier to the Customer and its customers subject to these Conditions.

Services: means the electronic validation by the Suppliers Software when accessed by the Customer or its customers of identified documents and other data against certain criteria set out in the Order.

Supplier Software: The Software which supports the Services.

Supplier: TrustID Limited registered in England and Wales with company number 05953015.

2. BASIS OF CONTRACT

2.1 These conditions apply to the Contract to the exclusion of any other terms that the Customer seeks to impose or incorporate before or after the Commencement Date, or which are implied by trade, customer, practice or course of dealing.

2.2 The Order constitutes an offer by the Customer to purchase the Services in accordance with these Conditions.

2.3 The Order shall only be deemed to be accepted on the Commencement Date on which date the Contract shall come into existence.

2.4 The Contract and these Conditions constitute the entire agreement between the parties. The Customer acknowledges that it has not relied on any statement, promise, representation, assurance or warranty made or given by or on behalf of the Supplier which is not set out in the Contract.

2.5 Any Scope of Work given by the Supplier shall not constitute an offer, and is only valid for a period of 90 Business Days from its date of issue.

3. LICENCE AND ACCESS

3.1 In consideration of the Fee paid by the Customer to the Supplier the Supplier grants to the Customer and its customers a non-exclusive, time-limited, worldwide, non-transferable licence to access and use the Supplier Software solely for the purposes of the Services as set out in the Order ("The Licence").

3.2 As soon as reasonably practical after the Commencement Date, the Supplier shall provide the Customer with the Service login details specified in the Order (the Login Details). The Login Details are confidential and personal to the Customer

3.3 Customer will be responsible for maintaining the security of any Login Details and passwords and ensuring that its customers maintain that level of security of the login details and passwords.

4. FEES

4.1 The price for the Services shall be the price set out in the Order, and such prices are stated exclusive of VAT (the Fee).

4.2 The Supplier may invoice the Customer the Fee plus applicable VAT for Services as specified in the Order.

4.3 The Customer shall pay the invoice in full, including any VAT, and in cleared funds within the time frame quoted in the Commercial Details section of this document. Payment shall be made to the bank account nominated in writing by the Supplier.

4.4 If the Customer fails to make any payment due to the Supplier under the Contract by the due date for payment, then, without limiting the Supplier's remedies under clause 8:

a) the Customer shall pay interest on the overdue amount at the rate of 4% per annum above Lloyds Bank plc's base rate from time to time. Such interest shall accrue on a daily basis from the due date until actual payment of the overdue amount, whether before or after judgment. The Customer shall pay the interest together with the overdue amount; and

b) the Supplier may suspend the Licence and the use of the Service while any sum remains outstanding.

4.5 The Customer shall pay all amounts due under the Contract in full without any set-off, counterclaim, deduction or withholding (except for any deduction or withholding required by law). The Supplier may at any time, without limiting any other rights or remedies it may have, set off any amount owing to it by the Customer against any amount payable by the Supplier to the Customer.

5. CUSTOMER'S OBLIGATIONS

5.1 The Customer shall and will ensure that its customers shall:

a) ensure that the terms of the Order and the information provided by the Customer when using the Services is complete and accurate;

b) co-operate with the Supplier in all matters relating to the Services as the Supplier may reasonably require;
c) obtain, maintain and execute all necessary equipment, third party licences or agreements and consents and any other licences, permissions and consents which may be required for the Services before the date on which the Services are to start;
d) Grant the Supplier the right to share any data, including Personal Data, contained in a scanned document with relevant third parties but only to the extent that it is necessary to do so to provide any third party validation checks requested by the Customer;
e) Grant the Supplier the right to retain and share with third parties including the Metropolitan Police (or other UK police authority) and regulatory bodies, any data in relation to Compromised Documents and Metadata, such right to continue after termination of this Contract;
f) use for the Services only within the normal business purposes of the Customer (which shall not include allowing the use of the Service by, or for the benefit of, any person other than the Customer);
g) notify the Supplier as soon as it becomes aware of any unauthorised use of the Service by any person;
h) keep the Login Details provided by the Supplier confidential;
i) not permit any third parties to become aware of the Login Details;
j) be responsible for all charges including Fees incurred for the use of the Service when access to the Service is obtained through the use of the Customer's Login Details;
k) take responsibility for and maintain the platform used by it to connect to the Services and the Supplier will have no liability for any failure to receive the services or diminishment in the Services caused by that platform;
l) accept responsibility for the selection of the Services and the extent of the Services as set out in the Order to achieve its intended results and acknowledges that the Services have not been developed to meet the individual requirements of the Customer;
m) accept responsibility for Service failures which arise as a result of any third party equipment, software or hardware owned or licenced by the Customer.

5.2 The Customer warrants that it and its customers are fully and lawfully entitled to transfer Personal Data, to Supplier for the purposes of the Services and undertakes to ensure that the processing of Personal Data complies with all other applicable laws.

5.3 If the Supplier's performance of any of its obligations in respect of the Services is prevented or delayed by any act or omission by the Customer or its customers or failure by the Customer or its customers to perform any relevant obligation (**Customer Default**):
a) the Supplier shall without limiting its other rights or remedies have the right to suspend performance of the Services until the Customer remedies the Customer Default, and to rely on the Customer Default to relieve it from the performance of any of its obligations to the extent the Customer Default prevents or delays the Supplier's performance of any of its obligations;
b) the Supplier shall not be liable for any costs or losses sustained or incurred by the Customer arising directly or indirectly from the Supplier's failure or delay to perform any of its obligations as set out in this clause 5; and
c) the Customer shall reimburse the Supplier on written demand for any costs or losses sustained or incurred by the Supplier arising directly or indirectly from the Customer Default. As such the maximum value of Customer liability should be the value of the order.

5.4 The Customer acknowledges that the Services and Scope of Works as delivered by the Supplier incorporate data, materials and functionality made and delivered by third-party suppliers to the Supplier on the basis of their Terms and Conditions which are incorporated into these Suppliers Terms and Conditions and accept those Third Party Terms and Conditions as part of the delivery of the Services and Scope of Work by the Supplier including but not limited to that:
a) any third-party suppliers own and retain all proprietary right, title and interest in their products and any technical information or other materials relating to their products including without limitation any and all copyrights, patents, trademarks, tradenames and other intellectual property rights embodied in or used in connection with their product documentation and materials and including without limitation any modifications, enhancements, translations, localisations or other derivative works thereof made by the third-party's suppliers.
b) they may not use all or any of the Products, Services, Data or any other Data or Results provided by the third-party suppliers to train or test directly or indirectly or either by itself or through a third-party any machine learning or artificial intelligence technology or process.
c) subject to any contracted exceptions they may only use the product for the identity verification of its own customers, consumer or business customers and not sell or transfer any results to any other third-party except for regulators who have made a lawful request to obtain results.
d) they acknowledge that the third-party suppliers and TrustID may use non personally identifiable data from the end user for its own internal purposes.

5.5 Where PEP & Sanction screening and or address checks are performed, the Customer acknowledges that to undertake these checks the Customer is bound by and required to adhere to the terms of the Customer's Obligations in the LexisNexis Risk Solutions Customer Licence Terms which can be viewed here https://www.trustid.co.uk/lnrscustomer-licence-terms/

5.6 Where the DBS Service is used, the Customer acknowledges that to undertake these checks the Customer is bound by and required to adhere to the terms of the Customer's Obligations in the Matrix Security Watchdog Ltd (MSW) Customer Licence Terms which can be viewed here: Terms of Service | Matrix Security Watchdog

6. SUPPLIER OBLIGATIONS

6.1 The Supplier warrants that the use of Services will be as set out in the Scope of Work but accepts no liability for the performance of any third party platform used by the Customer to connect to the Services.

6.2 The Supplier warrants that; a) it has obtained and will maintain for the duration of this contract all permissions, licences and consents necessary to perform the Services, b) the Services shall be performed with all due care, skill and diligence and in accordance with good industry practice, c) the Services and the supply in the performance of its obligations under this contract shall comply with all applicable laws, regulatory requirements, mandatory standards and codes of practice of any competent authority for the time being in force.

6.3 The Supplier will deliver and fulfil its obligations as set out in the Scope of Work.

6.4 All other conditions, warranties or other terms which might have effect between the parties or be implied or incorporated into this licence or any collateral contract, whether by statute, common law or otherwise, are hereby excluded, including the implied conditions, warranties or other terms as to satisfactory quality, fitness for purpose or the use of reasonable skill and care.

7. LIMITS OF LIABILITY

7.1 Nothing in this Agreement shall exclude or restrict liability for death or personal injury resulting from the negligence of the Supplier or its employees while acting in course of their employment or for fraud.

7.2 The Supplier's liability in contract, tort or otherwise arising out of or in connection with the performance or observance of its obligations under these Conditions shall be limited to A total amount of £20,000

7.3 In any event the Supplier shall not be liable in contract, tort or otherwise for any loss of business, contracts, profits or anticipated savings or for any indirect or consequential loss whatsoever.

7.4 In no circumstances shall the Supplier be liable to the Customer for any loss or damage arising from any interruption or cessation of Service.

7.5 the Supplier hereby expressly excludes all liabilities in respect of inaccurate or incomplete information obtained via the Service howsoever arising including (without limitation) those arising as a result of inaccuracies in the information provided to the Supplier.

7.6 All dates and times supplied by the Supplier for the delivery of the Login Details or the provision of Services are an estimate and may be subject to reasonable delay.

7.7 All references to "the Supplier" in this clause 7 shall, for the purposes of this clause, be treated as including all employees, subcontractors and suppliers of the Supplier, all of whom shall have the benefit of the exclusions and limitations of liability set out in this clause.

7.8 The parties acknowledge and agree that any terms and conditions implied by law, trade, custom, practice or course of dealing, are excluded to the fullest extent permitted by law.

8. TERMINATION

8.1 Without affecting any other right or remedy available to it, either party may terminate the Contract with immediate effect by giving written notice to the other party if:

a) the other party fails to pay any amount due under the Contract on the due date for payment and remains in default not less than 15 days after being notified in writing to make such payment;

b) the other party commits a material breach of any other term of the Contract which breach is irremediable or (if such breach is remediable) fails to remedy that breach within a period of 20 Business Days after being notified in writing to do so;

c) the other party suspends, or threatens to suspend, payment of its debts or is unable to pay its debts as they fall due or admits inability to pay its debts or (being a company or limited liability partnership) is deemed unable to pay its debts within the meaning of section 123 of the Insolvency Act 1986 or commences negotiations with all of any class of its creditors with a view to rescheduling any of its debts or to make a proposal for or enters into any compromise or arrangement with its creditors;

d) the other party suspends or ceases, or threatens to suspend or cease, carrying on all or a substantial part of its business.

8.2 Any provision of the Contract that expressly or by implication is intended to come into or continue in force on or after termination or expiry of the Contract shall remain in full force and effect.

8.3 Termination or expiry of the Contract shall not affect any rights, remedies, obligations or liabilities of the parties that have accrued up to the date of termination or expiry, including the right to claim damages in respect of any breach of the agreement which existed at or before the date of termination or expiry.

8.4 On termination for any reason:

a) all rights granted to the Customer and its customers under the Contract shall cease;

b) the Customer and its customers shall cease all activities authorised by the Contract; and

c) the Customer shall immediately pay to the Supplier any sums due to the Supplier under the Contract.

9. FORCE MAJEURE

9.1 For the purposes of this Contract, **Force Majeure Event** means an event beyond the reasonable control of either party including but not limited to strikes, lock-outs or other industrial disputes (whether involving the workforce of the Supplier or any other party), failure of a utility service or transport network, act of God, war, riot, civil commotion, malicious damage, compliance with any law or governmental order, rule, regulation or direction, accident, breakdown of plant or machinery, fire, flood, storm or default of suppliers or subcontractors.

9.2 Neither party shall be liable to the other or its customers as a result of any delay or failure to perform its obligations under this Contract as a result of a Force Majeure Event.

9.3 If the Force Majeure Event prevents either party from providing any of the Services and/or Goods for more than 4 weeks, the affected party shall, without limiting its other rights or remedies, have the right to terminate this Contract immediately by giving written notice to the other.

10. SEVERANCE

10.1 If any provision or part-provision of the Contract is or becomes invalid, illegal or unenforceable, it shall be deemed modified to the minimum extent necessary to make it valid, legal and enforceable. If such modification is not possible, the relevant provision or part-provision shall be deemed deleted. Any modification to or deletion of a provision or part-provision under this clause shall not affect the validity and enforceability of the rest of the Contract.

11. WAIVER

11.1 A waiver of any right under the Contract or law is only effective if it is in writing and shall not be deemed to be a waiver of any subsequent breach or default. No failure or delay by a party in exercising any right or remedy under the Contract or by law shall

constitute a waiver of that or any other right or remedy, nor prevent or restrict its further exercise of that or any other right or remedy. No single or partial exercise of such right or remedy shall prevent or restrict the further exercise of that or any other right or remedy.

12. THIRD PARTIES

12.1 A person who is not a party to the Contract shall not have any rights to enforce its terms.

13. VARIATION

13.1 Except as set out in these Conditions, no variation of the Contract, including the introduction of any additional terms and conditions shall be effective unless it is agreed in writing and signed by both Parties.

14. DATA PROTECTION

14.1 Definitions in this clause:

Affiliate: an entity that owns or controls, is owned or controlled by or is under common control or ownership with another, where control is defined as the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of an entity, whether through ownership of voting securities, by contract or otherwise;
Applicable Laws: any law including (without limitation) GDPR to which the Customer or Supplier is subject;
Contract Personal Data: any Personal Data Processed by the Supplier on behalf of the Customer pursuant to or in connection with the Contract including (without limitation) the categories of data listed in the Processing Appendix of these Terms and Conditions together with any additional Personal Data to which the Processor may have access to from time to time in performing the Services under the Contract;
Data Protection Laws: the Data Protection Act 2018 and as amended, replaced or superseded from time to time, the UK GDPR, the GDPR and any laws implementing or supplementing the UK GDPR in the UK and the GDPR in Ireland and, to the extent applicable, the data protection or privacy laws of any other country;
GDPR: the General Data Protection Regulation (Regulation (EU) 2016/679;
UK GDPR: the UK General Data Protection Regulation, as defined in Section 3(10) of the Data Protection Act 2018
The terms **Data Controller, Data Processor, Data Subject, Personal Data Breach, Process/Processing, Special Categories of Personal Data, Biometric Data, Member State** and **Supervisory Authority** shall have the same meaning as in the GDPR and shall be construed accordingly.

14.2 Processing of Personal Data:

a) Both the Supplier and the Customer agree to comply at all times with all of their respective obligations under Data Protection Laws.
b) The parties have agreed that it is necessary for the Supplier as a Processor to Process the Contract Personal Data on behalf of the Customer as Controller.
c) The Supplier is appointed by the Customer as a processor to Process such Personal Data on behalf of the Customer as is necessary to provide the Services in accordance with the terms of the Contract.
d) The Supplier shall not Process Personal Data other than to the extent such processing is necessary in accordance with the provision of the Services under the Contract or on the Customer's documented instructions unless Processing is required by Applicable Laws to which the Supplier is subject, in which case the Supplier shall to the extent permitted by Applicable Laws inform the Customer of that legal requirement before the relevant Processing of that Personal Data. In particular, the Supplier as processor shall not itself exercise control, nor shall it transfer, or purport to transfer, control of such Personal Data to a third party, except as it may be specifically instructed, in documented form, to do so by the Customer.
e) In the event a party breaches its data protection obligations by act, error or omission, the breaching party shall indemnify the other party against any losses, costs, damages, or claims that are suffered, sustained or incurred by the other party as a result of the breach. Where permitted by the law, regulatory fines shall also be indemnified
f) The Customer as the Controller authorises the Supplier to engage another Processor ('Third Party Processor') of Data on the condition that the Supplier as the Processor enters into a written contract with such Third Party Processor which reflects and will continue to reflect the requirements of the Data Protection Legislation. As between the Customer and the Supplier the Supplier shall remain fully liable for the acts and omissions of any Third Party Processor appointed by it pursuant to this Agreement. The Supplier shall provide the Customer with a list of the existing Third Party Processors, as set out here. The Supplier shall give Customer prior notice of any intended addition to or replacement of those existing Third Party Processors. If Customer objects to that change, the Supplier make good-faith efforts to resolve any reasonable concerns raised by Customer and shall keep Customer informed of those efforts.
g) TrustID will maintain and complete accurate records and information to demonstrate its compliance with the Article 28 of the UK GDPR and Article 28 of the GDPR and allow for audits by the customer or the customers designated auditor and immediately inform the customer if in the opinion of TrustID an instruction infringes the data protection legislation.

14.3 Transfer of Data Outside of the United Kingdom and the EEA:
The Supplier may transfer any Personal Data outside of the UK and the European Economic Area ("EEA") as long as the following conditions are fulfilled:

a) the Supplier complies with its obligations under the Data Protection Laws by providing an adequate level of protection to any Personal Data that is transferred; and
b) the Supplier complies with reasonable instructions notified to it in advance by the Customer with respect to the processing of the Personal Data.

14.4 Security:

a) The Supplier shall take reasonable steps to ensure the reliability of any employee, agent or contractor who may have access to the Personal Data or process the personal data, ensuring that all such individuals are subject to confidentiality undertakings or professional or statutory obligations of confidentiality.

b) The Supplier shall ensure that it has in place appropriate technical and organisational measures to protect against unauthorised or unlawful processing of Personal Data and against accidental loss or destruction of, or damage to, Personal Data, appropriate to the harm that might result from the unauthorised or unlawful processing or accidental loss, destruction or damage and the nature of the data to be protected, having regard to the state of technological development and the cost of implementing any measures (those measures may include, where appropriate, pseudonymising and encrypting Personal Data, ensuring confidentiality, integrity, availability and resilience of its systems and services, ensuring that availability of and access to the Personal Data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of the technical and organisational measures adopted by it).

c) Notwithstanding the generality of Clause 14.4.(b) above, the Supplier may implement additional measures from time to time (at the Supplier's discretion).

d) The Supplier represents and warrants that the Supplier's technical and organisational measures meet the requirements set out in Article 32 UK GDPR and the GDPR, with respect to the Personal Data to be Processed by the Supplier on behalf of the Customer;

e) Personal Data processed by the Supplier has been and shall be collected and processed by the Customer in accordance with all applicable laws and without limitation to the foregoing, the Customer shall take all steps necessary including without limitation providing appropriate privacy notices and ensuring that there is a lawful basis or bases as specified in the Processing Appendix for both the Customer and the Supplier to process Personal Data (including, without limitation, by obtaining valid explicit consent from the Data Subjects) to ensure that the processing of the Personal Data by the Supplier in accordance with the Contract is in accordance with all Applicable Laws.

14.5 Personal Data Breach:

a) Each party shall notify the other without undue delay of becoming aware of a Personal Data Breach affecting the Contract Personal Data, including providing information (as and when available) to assist the other to meet any obligations to report a Personal Data Breach under the Data Protection Laws.

b) Each party shall co-operate with the other and take such reasonable commercial steps as are agreed in good faith by the parties to assist in the investigation, mitigation and remediation of each Personal Data Breach and to the extent that a Personal Data Breach results from a breach by one party of its obligations in this Contract that party shall reimburse the other for those costs reasonably and properly incurred in performing its obligations under this Clause.

14.6 Data Subject Rights:

a) The Supplier shall promptly notify the Customer if it receives a request from a Data Subject under any Data Protection Laws in respect of Contract Personal Data.

b) Taking into account the nature of the Processing, the Supplier shall provide reasonable assistance to the Customer in the fulfilment of the Customer's obligation to respond to requests for exercising Data Subject rights under the Data Protection Laws.

14.7 Data Protection Impact Assessment and Prior Consultation:

The Supplier shall, where requested to do so by the Customer, provide to the Customer reasonable assistance with any data protection impact assessments which are required under Article 35 UKGDPR or Article 35 of the GDPR or any equivalent provisions of any Data Protection Law, and with any prior consultations to any supervisory authority of the Customer which are required under Article 36 GDPR or Article 36 of the UK GDPR or any equivalent provisions of any Data Protection Law, and shall work with the Customer to implement agreed mitigation actions to address privacy risks so identified.

14.8 Audit rights:

a) Subject to Clause 14.8.(b)**,** the Supplier shall make available to the Customer on request all information reasonably necessary to demonstrate compliance with this Contract, and shall allow for and contribute to audits, including inspections, by an auditor mandated by the Customer in relation to the Processing of the Personal Data.

b) The Customer shall give the Supplier reasonable notice of any audit or inspection to be conducted under Clause 14.8.(a) and shall make (and ensure that each of its mandated auditors makes) reasonable endeavours to avoid causing any damage, injury or disruption to the Supplier's premises, equipment, personnel and business while its personnel are on those premises in the course of such an audit or inspection.

14.9 Deletion or return of Personal Data on termination:

Subject to the requirements of any applicable exit plan, the Supplier shall cease Processing the Personal Data within thirty (30) days upon the termination or expiry of the Contract or, if sooner, the service to which it relates and, as soon as possible thereafter at the choice of the Customer, either return, or delete from its systems, the Personal Data. If the Customer does not inform the Supplier of its choice to require the return or deletion of such Personal Data within thirty (30) days of the termination or expiry of the Contract, or if sooner, the service to which it relates, then the Customer shall be deemed to have chosen the deletion of the Personal Data.

15. CONFIDENTIALITY

15.1 Each party shall, during the term of the Contract and thereafter, keep confidential all, and shall not use for its own purposes (other than implementation of this licence) nor without the prior written consent of the other disclose to any third party (except its professional advisors or as may be required by any law or any legal or regulatory authority) any, information of a confidential nature (including trade secrets, technical or commercial know-how, specifications, inventions, processes or initiatives which are of a confidential nature and information of commercial value) which may become known to such party from the other party and which relates to the other party or any of its Affiliates, unless that information is public knowledge or already known to such party at the time of disclosure, or subsequently becomes public knowledge other than by breach of the Contract, or subsequently comes lawfully into the possession of such party from a third party. Each party shall use its reasonable endeavours to prevent the unauthorised disclosure of any such information.

15.2 No party shall make, or permit any person to make, any public announcement concerning the Contract without the prior consent of the other parties (such consent not to be unreasonably withheld or delayed), except as required by law, any governmental or

regulatory authority. Save that the parties hereby agree that the Supplier may refer to the Customer as a customer for promotional and marketing activity.

16. GOVERNING LAW AND JURISDICTION

16.1 The Contract and any dispute or claim arising out of or in connection with it or its subject matter or formation (including non-contractual disputes or claims) shall be governed by and construed in accordance with the law of England and Wales; and each party irrevocably submits to the exclusive jurisdiction of the courts of England and Wales.

Processing Appendix

The parties acknowledge that for the purposes of the Data Protection Legislation the Customer is the Controller and the Supplier is the Processor and the following sets out the scope, nature and purpose of processing by the Supplier, the duration of the processing and the types of Personal Data and the categories of Data Subject:

Scope	The Services
Nature	The Services as further specified in Scope of Work
Purpose of Processing	The delivery of the Services; and internal staff training
Duration of Processing	The processing period is 7 days from the completion of checks, or as otherwise agreed with the Customer. Where LexisNexis Risk Solutions (LNRS) is engaged to perform address checking and PEP & Sanction screening, this data is retained by LNRS for 6 years, in line with the maximum time period for bringing contract legal actions, to allow LNRS to defend any such claims. Where a DBS application has been submitted, the following retention schedule applies within the Matrix Security Watchdog platform: 6 months after completion date – application is moved to the eBulk archive. PII used to support the application is retained but DBS results are removed. 1 year after completion date – application is purged with all PII removed except for full name, DOB, employer name and position applied for. 3 years after completion date – application is fully and securely deleted from eBulk.
Types of Personal Data	Data subject's photograph (selfie) Data items on ID documents incl: full name; DOB; nationality; photograph; gender; issuing country; document number; validity period; signature; driving qualifications; address; birth certificate details; marriage certificate details; national insurance or other national identity number; email address; postal address Data obtained by other means: Location or IP address (from 'selfie'), postal address (entered by data subject), presence (or not) of criminal record, PEP & Sanction match data, address history N.B. Where face biometrics form part of the Services, the photograph from ID documents and selfie will be processed biometrically which is one of the Special Categories of Personal Data.
Categories of Data Subject	Applicants to be employees/ customers/ student/ tenants of controller which has requested them to submit their data; or some other proposed relationship with controller
Lawful basis/bases for Processing[1]	**UK Customers**: For non-Special Categories of Personal Data, the lawful basis is that contained in Article 6.1.b of the UK GDPR – processing necessary for the performance of a contract, to which the Data Subject is party or in order to take steps at the request of the Data Subject prior to entering in to a contract; or Article 6.1.f of the UK GDPR – processing necessary for the performance of legitimate interests pursued by the Controller or by a third party[2]. For criminal data the Schedule 1 of Data Protection Act 2018 condition which applies is the Data Subject has given explicit consent to the Processing. For Special Categories of Personal Data, the Schedule 1 of Data Protection Act 2018 condition which applies is normally Article 9.2.a – the Data Subject has given explicit consent to the Processing. Alternatively, some Customers may be able to use the Article 9.2.b[3] exception which permits the processing of special category data for "employment, social security and social protection (if authorised by law)". **EU Customers**: For non-Special Categories of Personal Data, the lawful basis is that contained in article 6.1(b) of the GDPR – processing necessary for the performance of a contract, to which the Data Subject is party or in order to take steps at the request of the Data Subject prior to entering in to a contract; or Article 6.1.f of the GDPR– processing necessary for the performance of legitimate

[1] For law enforcement bodies which are subject to Part 3 of the Data Protection Act 2018 the customer is required to specify the correct lawful basis.
[2] Where a Customer relies on 6.1.f Legitimate Interests, they must provide a Legitimate Interests Assessment
[3] Where a Customer relies on the 9.2.b exception, they must also keep an appropriate policy document

	interests pursued by the Controller or by a third party[4]. For processing of Special Categories of Personal Data, the Article 9(2)(a) exception (the Data Subject has given explicit consent to the Processing), and/or Article 9(2)(b) exception (employment, social security and social protection if authorised by law) applies.

See the link below for a current list of organisations appointed as Third-Party Processors, the purpose of processing and their location of processing.

https://www.trustid.co.uk/processors

[4] Where a Customer relies on 6.1.f Legitimate Interests, they must provide a Legitimate Interests Assessment