

EFFECTIVE DATE [to be inserted]

(1) EUROCOM CI LTD

(2) CLIENT NAME

DBS CHECKS AND EMPLOYEE
SCREENING CONTRACT FOR THE
PROVISION OF SOFTWARE AS A
SERVICE SOLUTION

TABLE OF CONTENTS

1. DEFINITIONS AND INTERPRETATION	4
2. ACTS BY THE SUPPLIER	7
3. WAIVER.....	8
4. SEVERABILITY.....	8
5. SERVICE PROVIDER.....	8
6. COPYRIGHT.....	8
7. SUPPLIER'S REPRESENTATIVE	8
8. CLIENT'S REPRESENTATIVE	8
9. COMMENCEMENT AND TERM	8
10. SERVICES PROVISION AND SYSTEM	9
11. CLIENT'S RESPONSIBILITY	11
12. CONFIDENTIALITY	13
13. DATA PROTECTION	13
14. INDEMNITY AND INSURANCE	15
15. INSTRUCTIONS	16
16. INVOICES, PAYMENT AND ACCOUNTS.....	16
17. VALUE ADDED TAX.....	17
18. REPORTS.....	17
19. SUSPENSION OF IDENTITY AUTHENTICATION CHECKS ...	Error! Bookmark not defined.
20. TERMINATION	17
21. RECOVERY AND HANDOVER ON END OF CONTRACT	17
22. INTELLECTUAL PROPERTY RIGHTS	18
23. ASSIGNMENT AND SUB-CONTRATING	18
24. NOTICES	18
25. DISPUTES AND ARBITRATION	19

26. FORCE MAJEURE19

27. NO AGENCY/EMPLOYMENT/PARTNERSHIP19

28. EXCLUSION OF THIRD PARTY RIGHTS.....19

29. COMMUNITY, CULTURAL AND RELIGIOUS CONSIDERATIONS20

SCHEDULE 1 – SPECIFICATION21

SCHEDULE 2 –SERVICE LEVEL AGREEMENT.....22

SCHEDULE 3 – EXPERIAN DATA SERVICES END USER TERMS**Error! Bookmark not defined.**

THIS CONTRACT is made the [to be inserted].

BETWEEN:

- (1) **EUROCOM CI LTD** of Wesley House, Bull Hill, Leatherhead, Surrey, KT22 7AH (“the Supplier”) and
- (2) **XXXXXXXXXXXXXXXXXXXXXX** a private limited company registered under number XXXXXXXX and whose registered address is (“the Client”)

RECITALS:

The Client wishes to enter into this Contract for the Contract Period and to be provided with Services on the terms and conditions appearing below.

1. DEFINITIONS AND INTERPRETATION

- 1.1 In these conditions, except where the context otherwise requires, the following expressions shall have the following meanings:

“Agreed Purpose”	Means for the purpose of the Parties performing their obligations under this Contract.
“Client Data”	Means all information, text, diagrams, images or sounds which are embodied in any electronic or tangible medium and which are supplied or in respect of which access is granted by the Client under this Contract or which the Supplier is required to generate under this Contract.
“Conditions”	Means these conditions of Contract.
“Contract”	Means this contract entered into between the Supplier and the Client consisting of these Conditions and the Schedules and Annexesto them (if any).
“Contract Period”	Means the day from which the Client accepts the Supplier’s terms and conditions until terminated in accordance with this Contract.
“Contract Price”	Means the price exclusive of any applicable value added tax payable to the Supplier under this Contract in accordance with the Service Level Agreement Schedule 2 for the full and proper performance by the Supplier ofits obligations under this Contract.
“Commencement Date”	Means the date of the final signature applied to this Contract.
“Data Protection Legislation”	Means all applicable data protection

	legislation, including the GDPR and the UK GDPR.
“DBS”	Means the Disclosure and Barring Service as established under the Protection of Freedoms Act 2012 which merged the functions of the Criminal Records Bureau and the Independent Safeguarding Authority.
“Default”	Means any breach of the obligations of either Party (included but not limited to fundamental breach or breach of a fundamental term) or any default, act, omission, negligence or statement of either Party, its employees or agents in connection with or in relation to the subject matter of this Contract and in respect of which such Party is liable to the other.
“E-Bulk”	Means the system enabling an E-Registered Body to submit DBS checks electronically.
“E-Registered Body	Means the Supplier.
“Force Majeure Event”	Means any act of God, natural flood, fire (save where such fire is due to the negligence or fault of the Client), lightning or earthquake, war, military operations, act of terrorism, riot or any strike action by DBS staff employed and the Identity Authentication Check organisation’s staff employed (if any) and having an effect on the provision of the Service under the Contract.
“GDPR”	Means the General Data Protection Regulation (EU) 2016/679).
“Identity Authentication Checks Services”	Means the Yoti Service called “IDVT” also referred to as ‘Authorised Third Party Services’ .
“Intellectual Property Rights”	Means patents, inventions, trademarks, service marks, logos, design rights (whether registrable or otherwise) applications for any of the foregoing, copyright, semiconductor topography rights, database rights, domain names, trade or business names, moral rights and other similar rights or obligations whether registrable or not in any country (including the United Kingdom) and the right to sue for passing off but excluding any copyright, database rights and all other intellectual property rights covered under and in relation to the End User Terms.
“Party”	Means a party to this Contract.

“Registered Body”	Means an organisation approved and registered with the DBS as being authorised to apply for standard and enhanced DBS Disclosures on behalf of staff, volunteers or associates, or where the Registered Body is also a registered Umbrella Body with the DBS, also authorised to apply for Disclosures on behalf of 3 rd party customer organizations in respect of their staff, volunteers, or associates.
“Services”	Means the services and obligations of the Supplier provided under this Contract, including the provision of the full ‘Software as a Service’ solution, namely managed services with admin access, and may include any employee screening services
“Service Level Agreement”	Means the Service Level Agreement for Managed Services with Admin access more particularly described in Schedule 2.
“Shared Personal Data”	Means the personal data (including names, address, date of birth and information relating to criminal convictions) shared between the parties under this Contract in respect of applicants.
“Specification”	Means the specification as set out in Schedule 1
“System”	Means the system Xavier more particularly described in the Specification Schedule 1 and referenced in the Conditions to the Services shall include the System where the context admits.
“Total Value”	Means the total value of this Contract.
“UK GDPR”	Means the GDPR as transposed into the laws of the United Kingdom by operation of section 2 of the European Union (Withdrawal) Act 2018, as amended by the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019.
“Umbrella Body”	Means an organisation approved and registered with the DBS; as being authorised to apply for standard and enhanced DBS disclosures on behalf of third party customer organisations in respect of their staff, volunteers or associates.

“Upgrades”	Means upgrades and/or later versions of any System provided under this Contract.
“VAT”	Means value added tax chargeable under English law for the time being
“Working Day”	Means Monday to Friday inclusive other than bank holidays or any other public holidays in England.

In this Contract except where the context otherwise requires:

- 1.2 Condition, Schedules and paragraph headings shall not affect the interpretation of this Contract.
- 1.3 A person includes a natural person, corporation or unincorporated body (whether or not having separate legal personality) and that person’s legal and personal representatives, successors and permitted assignees.
- 1.4 Words in the singular shall include the plural and vice versa.
- 1.5 A reference to a statute or statutory provision is a reference to it as it is in force for the time being, taking account of any amendment, extension, or re-enactment and includes any subordinate legislation for the time being in force or made under it.
- 1.6 A reference to writing or written includes e-mail.
- 1.7 Where the words include(s), including or in particular are used in this Contract, they are deemed to have the words without limitation following them. Where the context permits, the words and otherwise are illustrative and shall not limit the sense of the words preceding them.
- 1.8 Any obligation in this Contract on a person not to do something includes an obligation not to agree, allow, permit or acquiesce to that thing being done.
- 1.9 Reference to employees of the Client shall be deemed to include the Client’s agent and sub-providers, or anyone acting on the Client’s behalf, including but not limited to, volunteers, temporary staff and workers who are engaged by the Client but who may not be deemed to be an “employee” of the Services User under the Employment Rights Act 1996, unless the context otherwise requires.
- 1.10 The Contract constitutes the entire agreement and understanding between the Parties and supersedes all prior written and oral representations, agreements or understandings between them relating to the subject matter of the Contract provided that neither Party excludes liability for fraudulent misrepresentations upon which the other Party has relied.
- 1.11 References to **appropriate safeguards, appropriate technical and organisational measures, controller, data subject, joint controller, personal data, personal data breach, processor, process(ing)** and **supervisory authority** shall have the meanings given to them in the Data Protection Legislation and cognate terms shall be construed accordingly.

2. ACTS BY THE SUPPLIER

Any decision, act of thing which the Supplier is required or authorised to take or do under the Contract may be taken or done by any person authorised, either expressly or implied, by the Supplier to take or do that decision, act or thing.

3. WAIVER

- 3.1 The failure by either Party to exercise any right or remedy shall not constitute a waiver of that right or remedy.
- 3.2 No waiver shall be effective unless it is communicated to the other Party in writing.
- 3.3 A waiver of any right or remedy arising from a breach of the Contract shall not constitute a waiver of any right or remedy arising from any other breach of the Contract.

4. SEVERABILITY

If any Condition or provision of the Contract not being of a fundamental nature, is held to be unlawful, invalid or unenforceable by the court of tribunal in any proceedings relating to the Contract, the validity or enforceability of the remainder of the Contract shall not be affected. If the court finds invalid a provision so fundamental as to prevent the accomplishment of the purpose of the Contract, the Parties shall immediately commence negotiations in good faith to remedy the invalidity.

5. SERVICE PROVIDER

The provision of the Services by Supplier is not exclusive and will not prevent the Client from receiving the same or similar services from any third party.

6. COPYRIGHT

Copyright in the Contract Documents shall vest in the Supplier but the Client may obtain or make at its own expense any further copies of the Contract Documents required for use by the Client in relation to the Service.

7. SUPPLIER'S REPRESENTATIVE

The Supplier's representative shall be our helpline phone number and helpline email address.

8. CLIENT'S REPRESENTATIVE

The Client's representative shall be the Head of HR Delivery or such representative appointed by the Client to act in the name of the Client for the purposes of the Contract. The Client's representative will be taken to be the person signing up to be the authorised person/manager on the Account account application.

9. COMMENCEMENT AND TERM

Subject to the earlier termination of this Contract in accordance with its provisions, this Contract

shall commence on the Commencement Date and shall continue until: (i) the Supplier has been given one month notice of termination; or (ii) otherwise terminated under this Contract.

10. SERVICES PROVISION AND SYSTEM

10.1 PROVISION OF SERVICES

10.1.1 The Supplier acknowledges and it is agreed that in respect of the Services, it shall:

- (b) ensure secure administrative access to the System for staff members of the Client as set out in the relevant Service Level Agreement;
- (c) ensure training is provided for staff members of the Client as set out in the relevant Service Level Agreement;
- (e) be responsible for the maintenance and necessary upgrading of the System as required to meet statutory requirements or those levied by the DBS;
- (f) use all reasonable endeavours to ensure that they are only submitting disclosure applications for exempt positions as provided for in the Rehabilitation of Offenders Act 1974 (Exceptions) Order 1975 (as amended);
- (g) use all reasonable endeavours to ensure that they are only submitting disclosure applications of the appropriate level (as determined in accordance with the relevant legislation and guidance) for relevant positions of employment or engagement;
- (h) take reasonable steps to ensure that applications for free of charge disclosures fall within the definition of a volunteer as described in the Police Act 1997 (Criminal Records) (Registration) Regulations 2006;
- (i) take reasonable measures to ensure that the Client verifies and validates (where necessary) the identity of the applicant by complying with conditions that will be set administratively by the DBS and that it will exercise all due diligence when completing disclosure application forms, in particular to ensure all mandatory data fields are completed correctly and in the correct format;
- (j) be responsible for countersigning of the application form on behalf of the Client confirming that there is a legal entitlement to the check, the information provided is true and accurate and that the Supplier has not knowingly made a false declaration;
- (k) ensure that any electronic systems, used to countersign applications comply with such specifications as may be set by the DBS;
- (l) ensure that all applications are submitted to the DBS via e-bulk within one working day of submission of a valid and correctly completed application by the ID verifier or to archive or delete at the Supplier's sole discretion such applications that are

incomplete or invalid or awaiting information from the Client and such information remains outstanding after two (2) working days ;

- (p) takes reasonable measures that it and the Client comply with the DBS' Code of Practice including, but not limited to the policy on the usage, storage and retention of disclosure information;
- (q) promptly inform the Client about the outcome of any investigation of the DBS into the disputed DBS check from the applicant and/or the Client;
- (r) ensure that the certificate information is kept securely in lockable non-portable storage containers with access strictly controlled and limited to those who are entitled to see it as part of their duties in line with the Supplier's written security policy;
- (s) ensure that it does not authorise the reproduction of any of the disclosure or its content, including photocopies or scanned images, unless with the prior agreement of the DBS or as a result of a stipulated requirement relating to three-channel service;
- (t) ensure that, in accordance with section 124 of the Police Act 1997 (as amended), Certificate Information is only passed onto those who are authorised to receive it in the course of their duties. The Supplier shall maintain a record of all those to whom Certificates or Certificate Information has been revealed and shall provide such record to the client for approval upon reasonable request by the Client;
- (u) ensure that, once a recruitment (or other relevant) decision has been made by the Client as the case may be, it shall not keep Certificate Information for any longer than is necessary, namely for a period of up to six (6) months to allow for the consideration and resolution of any disputes or complaints and, in very exceptional circumstances, for longer than six (6) months after having consulted with the DBS and in full consideration to the Data Protection and Human Rights of the Applicant before doing so;
- (v) ensure that, once the retention period set out in clause 11.1.1(u) has elapsed, the Supplier will ensure that any Certificate Information is immediately destroyed by secure means such as shredding, pulping, burning or purging from the system. While awaiting destruction, Certificate Information shall not be kept in any insecure receptacle. The Supplier will not keep any photocopy or other image of the Certificate or any copy or representation of the contents of a Certificate.
- (w) ensure that the Supplier and its Client has a policy on the recruitment of ex-offenders;
- (x) ensure that the Supplier complies with any reasonable request from the DBS for information that will enable it to make a decision on the suitability or continued suitability of registered persons;
- (y) ensure that the Supplier informs the DBS of any changes to details held on the register including but not limited to changes to personal/organisational details;

- (z) provide all necessary assistance and co-operation to the Client in line with the Service Level Agreement;
- (aa) for the avoidance of doubt, not be responsible for the Client's recruitment decisions;
- (bb) be entitled to contact the DBS if it is not satisfied that the Client is entitled to ask an exempted question and/or believe that the Client may be acting illegally provided it first consults with the Client regarding such concerns;
- (cc) if required by the Client, provide the Client with the function for various other employee screening checks, e.g. IDVT, right to work checks, employment references, credit or AML checks.

10.2 SERVICE STANDARD

- 10.2.1 The Supplier will provide the Services and perform its obligations under the Contract with all due skill, care and diligence in accordance with this Contract, good industry practice and all relevant professional and technical standards.
- 10.2.2 Without prejudice to Condition 11.2.1, the Supplier will use its reasonable endeavours to ensure that staff are appropriately experienced, qualified and trained to perform the Services and comply with the Supplier's obligations under this Contract.
- 10.2.3 For the avoidance of doubt, the Supplier expressly excludes all liability for the content or accuracy of the information which the System receives from the DBS and/or the outcome received from any of the references requested from third parties and under no circumstances will the Supplier be liable for any failure to verify the accuracy and completeness of the information provided by the DBS and any of the outcomes received by the database searches and references requested or any other failure by the Client to comply with its obligations detailed under this Contract.

11. THE SYSTEM

The Supplier will provide the Client with a System as detailed within the Specification.

12. CLIENT'S RESPONSIBILITY

12.1 The Client shall:

- (b) ensure that all applicants for relevant positions of employment or engagement are notified in advance of the requirement for a screening/disclosure and that the Client notify all applicants of the potential effect of a criminal record history on the recruitment and selection process and any recruitment decision;
- (c) ensure, that the Client, as the case may be, establishes the true identity of the applicant through the examination of a range of documents as set out by the DBS' or uses our IDVT system for British/Irish passport holders to establish ID and right to work in the UK

- (d) ensure that a suitably trained user will be responsible for verifying and validating of the identity of each applicant for which the Client requires the Services if the IDVT check fails;
- (e) be responsible for any submission of incorrect details of applicants;
- (f) be responsible for any payment due to the Supplier in relation to all DBS applications and screenings via Xavier including rejected or invalid submitted applications, made;
- (g) be responsible for raising any disputes arising from the information revealed by the DBS check, from the Client, and the applicant, to the Supplier and shall not contact the DBS directly;
- (h) in the event of such a dispute, not make a recruitment decision and ensure that the Client not make a recruitment decision until the investigation by the DBS is completed and until the Supplier has informed the Client about the outcome of the investigation;
- (i) be solely responsible for its recruitment decision following the Services provided by the Supplier;
- (j) ensure that DBS/Screening Certificate Information is only used by it for the specific purpose for which it was requested and for which the applicant's full consent has been given;
- (k) be responsible for the correct storage and security of the information revealed in the Screening and DBS check and that the information contained is only seen by those that have a right to see it in the course of their normal duties; The Client shall ensure that it complies with the DBS Code of Practice including but not limited to the usage, storage and retention of disclosure information;
- (l) ensure that no reproductions of the screening/disclosure or its content are made, including photocopies or scanned images, unless with the prior agreement of the Supplier as a result of a stipulated requirement relating to the e- channel service;
- (m) assist the Supplier with any reasonable request from the DBS for information that will enable it to make a decision on the suitability or continued suitability of registered persons;
- (n) assist the Supplier when auditing the Client's accounts in order to establish that the Client has complied with the conditions as to verification and validation of the identity of the applicant, as set administratively by the DBS;
- (o) comply with the DBS Code of Practice;
- (p) manage all queries and promptly respond to any query issued by the Supplier;
- (q) ensure access and logins are not shared, and promptly notify the Supplier in writing of any leavers within to enable the Supplier to deactivate the relevant account(s); and

- (r) ensure all new users undertake the required webinar training prior to granting access or logins;

13. CONFIDENTIALITY

13.1 Either Party agrees not to disclose any confidential information ("Confidential Information"), excluding any confidential information referred to within the End User Agreement which will need to be dealt with in accordance with the End User Agreement (if applicable), to any third party without the prior written consent of the other Party to the extent that it is necessary for the Party to disclose Confidential Information to its staff and agents. Each Party shall ensure that such staff and agents are subject to the same obligations as the Parties in respect of all Confidential Information.

13.2 Condition 13.1 shall not apply to information which:

- 13.2.1 Is or becomes public knowledge (otherwise than by breach of these Conditions or a breach of an obligation of confidentiality);
- 13.2.2 Is in the possession of the other Party, without restriction as to its disclosure, before receiving it from the other Party or any other department or office of His Majesty's Government;
- 13.2.3 Is required by law to be disclosed;
- 13.2.4 Was independently developed by one of the Parties without access to the Confidential Information;
- 13.2.5 The obligations contained in this Condition shall continue to apply after the expiry or termination of the Contract;
- 13.2.6 Either Party shall not handle or examine any document or thing bearing a government security classification of "Confidential", "Secret" or "Top Secret" other than in a Government establishment and the Parties shall not remove any such document or thing from such Government establishment without the prior written consent of the other Party;
- 13.2.7 Either Party shall not communicate with representatives of the general or technical press, radio, television or other communications media, with regard to the Contract, unless previously agreed in writing with the other Party;
- 13.2.8 Except with the prior consent in writing of the other party, neither party shall make use of the Contract or any Confidential Information otherwise than for the purposes of carrying out, and using, the Services.

14. DATA PROTECTION

14.1 This clause sets out the framework for the sharing of personal data between the parties as data controllers. Each party acknowledges that one party (the "**Data Discloser**") will regularly disclose to the other party (the "**Data Recipient**") Shared Personal Data collected by the Data Discloser for the Agreed Purposes.

- 14.2 Both Parties shall comply with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018. Each Party acts as an independent data controller in respect of Shared Personal Data.

Each Party shall:

- Maintain appropriate technical and organisational measures in line with ISO 27001:2022.
- Appoint a data protection contact for handling SARs and breaches.
- Notify the other Party of any data breach within 24 hours.
- Ensure any international data transfers comply with UK ICO-approved mechanisms.
- Handle personal data only for the Agreed Purpose.

- 14.3 The parties hereby acknowledge that the Data Discloser is a controller of the Shared Personal Data. The parties further acknowledge that the Data Recipient shall also be an independent controller (and not, for the avoidance of a doubt, a joint controller) in respect of the Shared Personal Data.

- 14.4 In respect of the Shared Personal Data, each party shall:

- 14.4.1 comply with Data Protection Legislation;
- 14.4.2 provide reasonable assistance to the other party in respect of the other party's obligations under Data Protection Legislation;
- 14.4.3 have in place appropriate technical and organisational measures to ensure the security of the Shared Personal Data processed in relation to this Contract, in particular having in place appropriate measures to prevent accidental or unlawful disclosure of, or access to the Shared Personal Data;
- 14.4.4 in the event it suffers a personal data breach, it shall notify the other party without undue delay (and in any event within 24 hours), and each party shall provide the other party with reasonable assistance to: (i) identify the cause and scope of the personal data breach; (ii) remedy and mitigate the personal data breach; and (iii) determine if any notification is required to be made either to a supervisory authority or a data subject pursuant to Data Protection Legislation;
- 14.4.5 in the event that it receives any complaint, notice or communication (including from a supervisory authority or a data subject) which relates directly or indirectly to the processing of Shared Personal Data under this Contract, it shall notify the other party without undue delay and in any event within 72 hours, and it shall provide the other party and any supervisory authority (if applicable) with full co-operation and assistance in relation to any such complaint, notice or communication;
- 14.4.6 ensure that appropriate safeguards are in place with respect to any transfer of the Shared Personal Data outside of the United Kingdom and/or the European Economic Area;
- 14.4.7 ensure access is granted only to those personnel who require access to the Shared Personal Data, and that such personnel have received adequate training in respect of data protection; and
- 14.4.8 notify the other in the event that it reasonably considers that any processing of the Shared Personal Data under this Contract is in breach of Data Protection Legislation.

- 14.5 The Data Discloser warrants and covenants that its collection and disclosure of the Shared Personal Data, and the Data Recipient's use of the Shared Personal Data, shall be permitted under Data Protection Legislation.
- 14.6 The Data Recipient shall:
- 14.6.1 only process the Shared Personal Data for the Agreed Purpose; and
 - 14.6.2 only retain the Shared Personal Data for so long as is necessary in order to achieve the Agreed Purpose.

15. INDEMNITY AND INSURANCE

- 15.1 Neither Party excludes or limits liability to the other Party in respect of:
- 15.1.1 death or personal injury caused by that party's negligence;
 - 15.1.2 breach of Clause 13 (Confidentiality);
 - 15.1.3 any indemnity provided pursuant to this Contract;
 - 15.1.4 fraud (including fraudulent misrepresentation);
 - 15.1.5 wilful misconduct or deliberate default; and
 - 15.1.6 any other liability that cannot be excluded or limited by law.
- 15.2 Subject always to Condition 15.1:
- 15.2.1 Neither party will be liable, whether in contract, tort (including negligence and breach of statutory duty) or otherwise, for any indirect or consequential loss;
 - 15.2.2 Supplier's total liability in contract, tort (including negligence and breach of statutory duty) or otherwise in connection with this Contract, will be limited to an amount equal to the greater of: (a) GBP £5,000,000; and (b) 200% of the total fees paid and payable to the Supplier under this Contract;
 - 15.2.3 Client's total liability in contract, tort (including negligence and breach of statutory duty) or otherwise in connection with this Contract, will be limited to an amount equal to 100% of the total fees paid and payable to Supplier under this Contract.
 - 15.2.4 Supplier will indemnify the Client and its respective employees, agents and officers from and against any and all claims, liabilities, losses, damages, penalties, fines, costs and expenses sustained or incurred by any of them arising out of or in connection with:
 - (a) any claim that the receipt and/or use of the Services and the System by the Client infringes the rights (including the Intellectual Property Rights) of any person;
 - (b) any breach by Supplier of Clause 14 or any Data Protection Legislation; and

- (c) any breach by Supplier of applicable laws.

16. INSTRUCTIONS

- 16.1 Instructions given to the Supplier by the Client's Representative shall be in writing.
- 16.2 Any oral instruction given to the Supplier shall be confirmed in writing by the Client's Representative as soon as possible thereafter. Provided that if the Supplier shall confirm in writing to the Client's Representative any such oral instructions and such oral instructions and written confirmation thereof by the Supplier is not contradicted in writing by the Client's Representative within fourteen (14) days of receipt thereof by the Client's Representative, the oral instructions shall be deemed to be an instruction in writing by the Client's Representative.

17. INVOICES, PAYMENT AND ACCOUNTS

- 17.1 The Supplier shall invoice the Client during the month in which the Client initiated the DBS check/screening by confirming the amount due from the Client.
- 17.2 Unless stated otherwise, the Client shall pay such an amount as is properly due Within fourteen (14) days of receipt of the invoice by the Supplier. Payment for undisputed invoices not received by the due date may result in the Supplier suspending the Services provided to the Client until all outstanding undisputed sums are settled in full.
- 17.3 The Supplier shall not be entitled to charge for the provision of any services that are not part of the Services agreed within the Contract, unless the Contract has been properly varied in advance in accordance with Condition 3.
- 17.4 The charges payable under this agreement are subject to receipt by the Supplier of the Minimum Throughput Amount in each rolling 12 month period of this agreement. If the minimum Throughput amount has not been achieved, the Supplier reserves the right to charge further administrative fees and/or only refund part/none of the balance held on account on behalf of the client. If an account has remained dormant for a period of 12 months or more, the supplier reserves the right to close the account and refund to the Client any balances held on account. If repeated repayment attempts (minimum five) are unsuccessful, balances may be applied toward administrative costs at the Supplier's discretion. DBS checks set up on the system that are inactive for more than 60 days will be archived and only the DBS fee will be added back to the account of the Customer.
- 17.5 For the purpose of calculating any statutory interest under the Late Payment of Commercial Debts (Interest) Act 2018, the relevant date for the payment of the debt shall be deemed to be the last day of a period of thirty (30) days commencing on the day when the Client receives notification from the Supplier that payment of undisputed fees remains outstanding.
- 17.6 The Supplier will keep full and proper accounts and records relating to all expenditure reimbursed by the Client and all payments made by the Client in respect of the Services and the System.
- 17.7 The Supplier will permit the Client acting by its officers, servants and agents or independent auditors on request and at all reasonable times to examine all accounts and records in relation to the provisions of the Services and the Supplier will provide the Client or its independent auditor with such explanations relating to that

expenditure as the Client may request.

- 17.8 The Supplier will ensure that the said accounts and records are available for a period of six years after termination of expiry of the Contract, whichever is the latest.

18. VALUE ADDED TAX

In addition to the sum specified in Condition 19 the Client shall pay to the Supplier such VAT as may be properly chargeable by the Supplier in connection with the provision of the Service. The Supplier shall issue a tax invoice in respect thereof.

19. REPORTS

- 19.1 In the event that the Client requires the Supplier to produce any reports, other than reports freely available from the System, the Client shall request the same from the Supplier with a full, written specification. Such reports will be subject to a reasonable additional charge as notified by the Supplier.
- 19.2 All data is archived 6 months after a DBS check result has been received or has been dormant for 6 months. The Supplier will not provide access to an account that has been closed and cannot provide data for checks that have been archived

20. TERMINATION

- 20.1 Either Party may terminate this Contract by providing one month's written notice after the initial 12-month term, or immediately in the event of material breach, insolvency, or breach of the DBS Code of Practice.
- 20.2 If either party commits a material breach of the Contract, other than a breach of the End User Agreement terms and conditions, which is either not capable of remedy, or if it is capable of remedy, the relevant party fails to remedy such a breach within twenty eight (28) days of being notified by the other party in writing to do so, that other party shall be entitled to terminate the Contract with immediate effect by notice in writing to the party that committed the material breach and without prejudice to any other right or remedies of either party in respect of the breach concerned or any other breach of the Contract.
- 20.3 The Supplier shall be entitled to terminate the Contract with immediate effect if the Client has breached the DBS Code of Practice and/or has not ensured that its client(s) adhere to the DBS Code of Practice
- 20.4 The Client shall be entitled to terminate the Contract with immediate effect upon providing one month's written notice.

21. RECOVERY AND HANDOVER ON END OF CONTRACT

- 21.1 On termination of the Contract howsoever arising, the Client shall, return to the Supplier all copies of the System or, if requested by the Supplier, shall destroy the same by erasing them from the magnetic media on which they are stored, including any stored on its client(s)'s magnetic media, and certify in writing to the Supplier that

they have been destroyed provided that the Client may extract and store any Client Data upon separate media for continuity purposes.

- 21.1.1 The Client will be responsible for collecting and removing all Client Data including its client(s)'s data from the System within sixty (60) days of the Contract end date. The System will be available to the administrator for this purpose. All other users of the System site will have their access disabled the day after the Contract end date. The user passwords shall be revoked, preventing connection and sixty one (61) days after the Contract end date all Client Data and its client(s)' data shall be deleted.
- 21.1.2 When this Contract terminates (for whatever reason), the Client may, for a period of six (6) months thereafter, require the Supplier to use all reasonable endeavours to assist the Client in the transfer of the provision of the Services to either the Client or a third party nominated by the Client and give the Client and/or such third party nominated by the Client such help as may be reasonably necessary to ensure such transfer to take place smoothly. The Supplier may charge for the Services the then current rates, as agreed between the Parties.

22. INTELLECTUAL PROPERTY RIGHTS

- 22.1 Subject to any pre-existing rights of third parties and of the Supplier, the Intellectual Property Rights (other than copyright) in all reports, documents and other materials which are generated or acquired by the Supplier (or any of its sub-contractors or agents) ("the Suppliers Materials") in the performance of the Services shall belong to and be vested automatically in the Supplier and/or the DBS. Supplier grants to the Client a non-exclusive, worldwide, irrevocable, sub-licensable, royalty-free, fully paid-up, perpetual licence to use the Suppliers Materials in connection with its use and exploitation of the Services.
- 22.2 Nothing in this Contract or done under the Contract shall be taken to diminish any Crown copyright, patent rights or any other Intellectual Property Rights which would, apart from this Contract, vest in the Crown or Supplier.

23. ASSIGNMENT AND SUB-CONTRACTING

- 23.1 The Supplier shall be entitled to assign the benefit of the Contract or any part thereof upon obtaining the Client's prior written consent.
- 23.2 The Supplier shall be entitled to sub-contract the provision of the Service or any part thereof to any person upon obtaining the Client's prior written consent.
- 23.3 The Client shall not assign the Contract or any part thereof or the benefit or advantage of the Contract or any part thereof without obtaining the Supplier's prior written consent.

24. NOTICES

Any demand, notice, or other communication required to be given under the Contract shall be sufficiently served if served personally on the addressee, or if sent by prepaid first class recorded delivery post to the registered office or last known address of the party to be served therewith or electronic communication and if so sent shall, subject to proof to the contrary, be deemed to have been received by the addressee on the second business day after the date of posting or on

successful transmission, as the case may be.

25. DISPUTES AND ARBITRATION

Any dispute arising out of or in connection with this Contract or the performance of the Service shall be notified by the aggrieved Party to the other and the Supplier's Representative and the Client's Representative shall endeavour to resolve any such dispute between them within twenty Working Days or receiving written notification of the same.

26. FORCE MAJEURE

- 26.1 If either Party is affected by a Force Majeure Event it shall immediately notify the other Party in writing of the matters constituting the Force Majeure Event and shall keep that Party fully informed of any relevant changes of circumstances whilst such Force Majeure Event constitutes. The Party affected by the Force Majeure Event shall take all reasonable steps available to it to minimise the effects of the Force Majeure Event on the performance of its obligations under the Contract.
- 26.2 Save as provided in Condition 30.5 and 30.6, a Force Majeure Event shall not entitle either Party to terminate the Contract and neither Party shall be in breach of the Contract, or otherwise liable to the other, by reason of any delay in performance, or non performance of any of its obligations due to a Force Majeure Event.
- 26.3 If the Party affected by a Force Majeure Event fails to comply with its obligations under Conditions 30.1 or 30.2 above then no relief for the Force Majeure Event, including the provisions of Condition 30.3 above, shall be available to it and the obligations of each Party shall continue in force.
- 26.4 If a Force Majeure Event results in the suspension of the Services, the Client shall not be obliged to pay the Contract Price until such time as such suspension has ceased. For the avoidance of doubt, this shall not effect any payment obligations in relation to the System.
- 26.5 If a Force Majeure Event continues for ninety (90) days or more, the Parties may terminate the Contract with immediate effect.

27. NO AGENCY/EMPLOYMENT/PARTNERSHIP

Nothing in this Contract shall be construed as creating a legal partnership or contract of employment or a relationship of principal and agent between the Supplier and the Client and the Client shall not at any time or in any circumstances take any action so as to bind (or purport to bind) the Supplier and nor shall the Client hold itself out as having authority to bind the Supplier and shall ensure that staff do not hold themselves out likewise. The Parties shall act in all respects as independent contractors.

28. EXCLUSION OF THIRD PARTY RIGHTS

- 28.1 Save for as expressly provided within this Contract, no person who is not a party to this Contract (including any employee, officer, agent, representative or sub-contractor of either party) shall have the right to enforce any term of this Contract which expressly or by implication confers a benefit on that person without the express prior agreement in writing of the parties which agreement must refer to this Condition 33.

28.2 Even if a person who is not a party to this Contract (including any employee, officer, agent, representative or sub-contractor of either party) has the right to enforce any term of this Contract by virtue of Section 1 of the Contracts (Rights of Third Parties) Act 1999, the Parties may, notwithstanding Section 2 of the Contracts (Rights of Third Parties) Act, vary or cancel this Contract by agreement between them without requiring the consent of such third party.

29. COMMUNITY, CULTURAL AND RELIGIOUS CONSIDERATIONS

The Parties shall be aware of the need to observe any community, cultural and religious considerations during the Contract Period.

SCHEDULE 1 – SPECIFICATION

The Xavier Employee Screening and DBS Checks Solution will enable you process many variation of screenings as well as basic, standard and enhanced DBS applications through a fully online system.

The Solution has the following facilities:

- Applicant personal details form
- Setting up applicants' access to online forms for completion of Screenings/DBS checks.
- Setting up ID verifiers to validate the ID of applicants for DBS checks if relevant.
- Recording of applicants ID documentation as required by the DBS
- Login details are sent to applicant and ID verifiers via e-mail.
- ID verifiers can change their password when logged into the system.
- The system is set up to automatically prompt, via e-mail, both applicants, ID verifiers and previous references at relevant stages of the process.
- System can be sorted to identify individuals whose checks are outstanding at various stages
- Screenings can be 'terminated' which stops the chase e-mails if required
- The system is integrated with various databases to be able to get electronic results in real time e.g. ID, credit and AML
- The system is made secure by installing a SSL certificate and setting up https.

Limitations exist on choices, options and access depending on the level of service agreed

This specification provides high level specification and does not include all details or restrictions of the system. It is designed as guidance to indicate the main functionality of the system.

SCHEDULE 2 –SERVICE LEVEL AGREEMENT
Xavier Screening/ DBS Check Service Level Agreement

For the purposes of this Schedule 2, references to “We”/”we” are to the Supplier and references to “You”/”you” are to the Client.

1. About Xavier Screening/ DBS Checks Solution - Managed Service with Administrative Access

- You set up administrative access for your staff to set-up checks on the system
 - (a) You set up and manage ID Verifiers and candidate user accounts and access
 - (b) Initiate screenings which have been added to your account in real time
 - (c) You track and manage the screening process
 - (d) The Supplier will countersign and submit completed checks to the DBS under Eurocom CI Ltd’s Registered Body number via secure e-Bulk
 - (e) You receive electronic notification of disclosure results with no content

2. Benefits of using Xavier Screening/DBS Checks Managed Service with Administrative Access

- (f) Sophisticated online system to carry out your candidate screenings and DBS checks
- (g) Reduced data error as the online form auto-validates information
- (h) No paper application forms to complete and no postage required
- (i) Easily accessible via the web on a PC, laptop or an i-Phone
- (j) Secure logons and clear instructions
- (k) FAQ section
- (l) Automated e-mail reminders for non-completion of forms by applicants and of ID validation by the designated verifier
- (m) E-bulk facility allowing the electronic transfer of your data to the national DBS
- (n) Faster receipt of disclosures
- (o) Experience of working with both public sector and commercial organisations
- (p) Professional, friendly and experienced staff

3. Support – your contacts

Operational support eg eligibility queries, new screening types to add to your account and application process

Contact Eurocom CI Team

Telephone 01372 886920

Email info@eurocomci.co.uk

Office hours: 9:00am – 5:00pm (Mon–Fri).

4. Effective Dates

The effective date of this agreement is in your contract

5. Technical Support Service Levels

The following service levels apply during our standard office hours which are 9am – 5.00pm

Full Service Unavailability

Response times – If full service of Xavier Screening/DBS check system is unavailable we will respond to you, the Client, following notification of a fault, within 2 working hours

Fix time – If full service of Xavier is unavailable we will fix the fault following notification, from you the Client, within 10 working hours

Major Functionality Unavailability

Response times – If major functionality of Xavier is unavailable we will respond to you the Client, following notification of a fault, within 5 working hours

Fix time – If major functionality of Xavier is unavailable we will fix the fault, following notification from you the Client, within 20 working hours

Minor Functionality Unavailability

Response times – If minor functionality of Xavier is unavailable, we will respond to you the Client, following notification of a fault, within 10 working hours.

Fix time – If minor functionality of Xavier is unavailable we will fix the fault, following notification from you the Client, within 10 working days.

Please note that full service unavailability and major functionality unavailability must be reported via telephone in order for us to meet the SLA timelines. Reporting these via e-mail may result in a delay.

Minor functionality unavailability can be reported either via telephone or via e-mail.

6. Other Guarantees

- (q) To provide an Screening/DBS solution that is accredited by the DBS and MOJ.
- (r) Enable secure administrative access to Screening/ DBS Checks for your staff members allowing you to manage your Screening/DBS checks online.
- (s) To electronically submit completed and submitted forms within 1 working day of submission by the ID verifier.
- (t) Secure hosting for the system via an ISO27001 accredited hosting organisation
- (u) To adhere to the DBS Code of Practice at all times.
- (v) To maintain complete confidentiality at all times and adhere to the Data Protection Act 2018
- (w) Allow DBS and MOJ site visits as required.
- (x) Provide an Account Manager to deal with any aspects of the agreement – see contacts section

Your responsibilities

We request that you commit to the following:

- To adhere to the DBS Code of Practice at all times
- To maintain complete confidentiality at all times

7. Pricing

The pricing is as agreed between the Parties in the quotation prior to the set up of the system and acceptance of the terms in the welcome email. Volume discounts are only applicable if the Minimum Throughput volumes are being met on each 12 month rolling basis.

8. Complaints Procedure

The Supplier endeavours to make its service the best that it can be at all times. We also know that sometimes you will want to let us know that you are not happy about something that we have done – or not done. We hope that we can sort these problems out with you to your satisfaction but accept that on occasions this will not be possible.

For this reason, there is a complaints procedure which gives you the chance to tell us when you think something has gone wrong and offers you the assurances that your complaint will be taken seriously. Often you will be able to resolve problems face to face, or by telephone but if you feel that this is not possible then you can put your complaint in writing and send it to:

Telephone 01372 886920
Email info@eurocomci.co.uk

If you are writing, it would be appreciated if you could cover the following points:

- What your complaint is about
- The brief history of the complaint from your point of view
- Your view on what should happen next
- The names of any staff involved

When a complaint is received your Account / Business Manager will:

- Try to put it right
- Respond to your correspondence within five working days

Where we are not able to meet that deadline, perhaps if a response requires further investigation, we will agree a completion date with you.

In all instances your complaint will be looked into by a senior member of staff and that person will contact you. We will also ensure that lessons are learned from what happened and work to prevent it happening again.