EBC GLOBAL
Employment Background Checks

EBC GLOBAL CONTRACT - Reference: XXXXXXX

PARTIES

1. **EBC Global Ltd**, a company incorporated in England and Wales (registration number **10115814**) having its registered office at **Abacus House Caxton Place Cardiff CF23 8HA** the "**Provider**"); and

2. **XXXXXXX Limited**, a company incorporated in England and Wales (registration number **1234567**) having its registered office at **ADDRESS.** (the **"Customer"**)

TERMS AND CONDITIONS

(a) Minimum Term: 24 months minimum commitment
(b) Billing frequency for Employment check Pro, payable annually in advance or monthly by Direct Debit.
(c) Configuration: payable in advance
(d) Service commences when the client has signed this agreement
(e) Billing frequency for Transactions: As per the Transactional Products Table below
(f) New Development Services are invoiced 50% on order and the remaining 50% on delivery.
(g) NO services will be completed without written Client approval to proceed at the quoted chargeable rate
(h) Product billing commences 7 days after the agreement even if client actions to allow service delivery are not completed.
(i) The Provider reserves the right to increase prices by 15% if a direct debit is not set up by the company
(j) Any additional bespoke development work will be quoted by EBC Global and the client will accept this by confirmation email. Development is charged at **£850** a day. Billing for these services are bound by this agreement
(k) Additional training after initial set up will be billed at **£100** per hour.
(l) Additional Employment Check Pro licences that are requested after this initial contract agreement must be requested by email and are subject to 24 months Minimum Term from the date of installation
(m) The Supplier acknowledges that Checks may be funded by the candidate using Paypal. Any candidate Checks via Paypal will be allocated against the Customer minimum monthly commitment
(n) Any payments completed via a third party such as PayPal will incur additional 3rd party transaction charges at the rate of 3%
(o) The Supplier reserves the right to invoice any 'checks' exceeding the minimum monthly commitment on either (i) a quarterly basis, or (ii) on the 12 months anniversary of the Effective date or (iii) at the end of a Calendar year, 31st December
(p) All costs are subject to 20% VAT
(q) Any Checks in addition to the Committed Checks initially purchased will be offered to the client at the standard EBC Checks charge rate. The client is not obligated to accept these new check services, but in doing so agrees that the new check charge will be added to the current agreement on the current Contractual Term

SERVICE

(a) Employment Check Pro Licence + Transactional Checks

Summary of Charges

Product	Unit Cost	No. Units	One-Off Cost	Monthly Cost	Annual cost	Due
Bespoke Configuration	£850.00 per day	0	£00,000.00	£00,000.00	£000,000.00	On Contract signature
Training	£850.00 per day	0	£00,000.00	£00,000.00	£000,000.00	On Contract signature
Development	£1000.00 per day	0	£00,000.00	£00,000.00	£000,000.00	50% on Contract Signature 50% on delivery
On-Site post live support	£850.00 per day	0	£00,000.00	£00,000.00	£000,000.00	On Contract signature
Employment Check Pro	£270 per licence	0	£00,000.00	£00,000.00	£000,000.00	Annual in Advance or Monthly by direct Debit
Employment Check Lite	£80 per licence	0	£00,000.00	£00,000.00	£000,000.00	Annual in Advance or Monthly by direct Debit
Shared Data	£30 per licence	0	£00,000.00	£00,000.00	£000,000.00	Annual in Advance or Monthly by direct Debit
Annual minimum checks charged as per the Transactional products table below		500	£00,000.00	£00,000.00	£000,000.00	Annual in Advance or Monthly by direct Debit
Total		**0000**	**£00,000.00**	**£00,000.00**	**£000,000.00**	**£000,000.00**

Transactional Products Table

Product (Checks)	Cost per Check	Check Volumes	Committed Checks per annum
DBS Basic	£ 32.00	0	£0.00
DBS Standard	£ 32.00	0	£0.00
DBS Enhanced	£ 64.50	0	£0.00
RTW	£ 4.50	0	£0.00
Credit	£ 9.00	0	£0.00
Sanctions	£ 9.00	0	£0.00
DVLA	£ 9.00	0	£0.00
Social Media	£ 35.00	0	£0.00
EHV (Employment History verification)	£ 10.00	0	£0.00
Disclosure Scotland	£ 40.00	0	£0.00
Electronic References	£ 0.50	0	£0.00
GSAT	£ 7.50	0	£0.00
APP – My Status Update – Single charge	£ 0.20	0	£0.00
International Criminal Checks	By Country	0	£0.00
Total Checks Annual Commitment	**£XXXXXX**	**£XXXXXX**	**£XXXXXX**

AGREEMENT

1. Definitions

1.1 Except to the extent expressly provided otherwise, in this Agreement:

"**Account**" means an account enabling a person to access and use the Hosted Services, including both administrator accounts and user accounts;

"**Agreement**" means this agreement including any Schedules, and any amendments to this Agreement from time to time;

"**Business Day**" means any weekday other than a bank or public holiday in England;

"**Business Hours**" means the hours of 09:00 to 17:00 GMT/BST on a Business Day;

"**Charges**" means the amounts specified in Service Order Form (Pricing);
"**Control**" means the legal power to control (directly or indirectly) the management of an entity (and "**Controlled**" should be construed accordingly);
"**Customer Confidential Information**" means:

(a) any information disclosed by or on behalf of the Customer to the Provider during the Term (whether disclosed in writing, orally or otherwise) that at the time of disclosure:
(i) was marked or described as "confidential"; or
(ii) should have been reasonably understood by the Provider to be confidential; and
(b) the Customer Data;

"**Customer Data**" means all data, works and materials: uploaded to or stored on the Platform by the Customer; transmitted by the Platform at the instigation of the Customer; supplied by the Customer to the Provider for uploading to, transmission by or storage on the Platform; or generated by the Platform as a result of the use of the Hosted Services by the Customer;
"**Customer Personal Data**" means any Personal Data that is processed by the Provider on behalf of the Customer in relation to this Agreement;
"**Data Protection Laws**" means all applicable laws relating to the processing of Personal Data including, while it is in force and applicable to Customer Personal Data, the General Data Protection Regulation (Regulation (EU) 2016/679);
"**Effective Date**" means the date of first login attempt into Customer's Account;
"**Force Majeure Event**" means an event, or a series of related events, that is outside the reasonable control of the party affected (including failures of the internet or any public telecommunications network, hacker attacks, denial of service attacks, virus or other malicious software attacks or infections, power failures, industrial disputes affecting any third party, changes to the law, disasters, explosions, fires, floods, riots, terrorist attacks and wars);
"**Hosted Services**" means services specified in Service Order Form (Services);
"**Intellectual Property Rights**" means all intellectual property rights wherever in the world, whether registrable or unregistrable, registered or unregistered, including any application or right of application for such rights (and these "intellectual property rights" include copyright and related rights, database rights, confidential information, trade secrets, know-how, business names, trade names, trademarks, service marks, passing off rights, unfair competition rights, patents, petty patents, utility models, semi-conductor topography rights and rights in designs);
"**Minimum Term**" means, in respect of this Agreement, the period specified in Service Order Form (Terms and Conditions) beginning on the Effective Date;
"**Personal Data**" has the meaning given to it in the General Data Protection Regulation (Regulation (EU) 2016/679);
"**Platform**" means the platform managed by the Provider and used by the Provider to provide the Hosted Services, including the application and database software for the Hosted Services, the system and server software used to provide the Hosted Services, and the computer hardware on which that application, database, system and server software is installed;
"**RTW credit"** means RTW checks are charged per credit per document used .passports = 1 credit, Sharecode = 1 credit.
"**Schedule**" means any schedule attached to the main body of this Agreement;
"**Services**" means any services that the Provider provides to the Customer, or has an obligation to provide to the Customer, under this Agreement;
"**Support Services**" means support in relation to the use of, and the identification and resolution of errors in, the Hosted Services, but shall not include the provision of training services;"**Supported Web Browser**" means the current release from time to time of Microsoft Edge, Mozilla Firefox, Google Chrome or Apple Safari;
"**Term**" means the term of this Agreement, commencing in accordance with Clause 2.1 and ending in accordance with Clause 2.2;

2. Term

2.1 This Agreement shall come into force upon the Effective Date for each Customer's Account.
2.2 This Agreement shall continue in force, subject to termination in accordance with Clause 13 or any other provision of this Agreement.

2.3 By making a payment or having access to the Services the Customer agrees to this Agreement being operational and accepts all Terms and Conditions of this agreement.

3. Hosted Services

3.1 The Provider shall create an Account for the Customer and shall provide to the Customer login details for that Account.
3.2 The Provider hereby grants to the Customer a licence to use the Hosted Services by means of a Supported Web Browser for the internal business purposes of the Customer during the Term.
3.3 The licence granted by the Provider to the Customer under Clause 3.2 for the Hosted Services may only be used by the employees of the Customer;
3.4 Except to the extent expressly permitted in this Agreement or required by law on a non-excludable basis, the licence granted by the Provider to the Customer under Clause 3.2 is subject to the following prohibitions:

(a) the Customer must not sub-license its right to access and use the Hosted Services;
(b) the Customer must not permit any unauthorised person to access or use the Hosted Services; and
(c) the Customer must not republish or redistribute any content or material from the Hosted Services;

3.5 The Customer shall use reasonable endeavours, including reasonable security measures relating to Account access details, to ensure that no unauthorised person may gain access to the Hosted Services using an Account.
3.6 The parties acknowledge and agree that Schedule 2 (Availability SLA) shall govern the availability of the Hosted Services.
3.7 The Customer must comply with Schedule 1 (Acceptable Use Policy) and must ensure that all persons using the Hosted Services with the authority of the Customer or by means of an Account comply with Schedule 1 (Acceptable Use Policy).
3.8 The Customer must not use the Hosted Services in any way that causes, or may cause, damage to the Hosted Services or Platform or impairment of the availability or accessibility of the Hosted Services.
3.9 The Customer must not use the Hosted Services:
(a) in any way that is unlawful, illegal, fraudulent or harmful; or
(b) in connection with any unlawful, illegal, fraudulent or harmful purpose or activity.
3.10 For the avoidance of doubt, the Customer has no right to access the software code (including object code, intermediate code and source code) of the Platform, either during or after the Term.
3.11 The Provider may suspend the provision of the Hosted Services if any amount due to be paid by the Customer to the Provider under this Agreement is overdue, and the Provider has given to the Customer at least 7 days written notice, following the amount becoming overdue, of its intention to suspend the Hosted Services on this basis.

4. Support Services

4.1 The Provider shall provide the Support Services to the Customer during the Term.
4.2 The Provider shall provide the Support Services in accordance with the standards of skill and care reasonably expected from a leading service provider in the Provider's industry.
4.3 The Provider shall provide the Support Services in accordance with Schedule 3 (Support SLA).
4.4 The Provider may suspend the provision of the Support Services if any amount due to be paid by the Customer to the Provider under this Agreement is overdue, and the Provider has given to the Customer at least 7 days written notice, following the amount becoming overdue, of its intention to suspend the Support Services on this basis.

5. Customer Data

5.1 The Customer hereby grants to the Provider a non-exclusive licence to the Customer Data to the extent reasonably required for the performance of the Provider's obligations and the exercise of the Provider's rights under this Agreement.
5.2 The Customer warrants to the Provider that the Customer Data when used by the Provider in accordance with this Agreement will not infringe the Intellectual Property Rights or other legal rights of any person, and will not breach the provisions of any law, statute or regulation, in any jurisdiction and under any applicable law.
5.3 The Provider shall create a back-up copy of the Customer Data at least daily, shall ensure that each such copy is sufficient to enable the Provider to restore the Hosted Services to the state they were in at the time the back-up was taken, and shall retain and securely store each such copy for a minimum period of 7 days.

6. No assignment of Intellectual Property Rights

6.1 Nothing in this Agreement shall operate to assign or transfer any Intellectual Property Rights from the Provider to the Customer.

7. Charges and Payments

7.1 The Customer shall pay the Charges to the Provider in accordance with this Agreement and as per the summary Terms and Conditions

7.2 All amounts stated in or in relation to this Agreement are, unless the context requires otherwise, stated exclusive of any applicable value added taxes, which will be added to those amounts and payable by the Customer to the Provider.

7.3 The Provider may elect to vary any element of the Provider Charges by giving to the Customer not less than 30 days written notice of the variation expiring on any anniversary of the date of execution of this Agreement, providing that no such variation shall result in an aggregate percentage increase in the relevant element of the Charges during the Term that exceeds 10% over the percentage increase, during the same period, unless such charge increases are directly as a result of a 3rd Party provider increase, over which Provider has no commercial control. Any such 3rd party increase will be advised as soon as the Provider is formally notified

7.4 The Provider shall issue invoices for the Charges to the Customer on or after the invoicing dates specified in Service Order Form (Terms and Conditions).

7.5 The Customer must pay the Charges to the Provider within the period of 7 days following the issue of an invoice in accordance with this Clause 7.

7.6 The Customer must pay the Charges by direct debit.

7.7 If the Customer does not pay any amount properly due to the Provider under this Agreement, the Provider may:

(a) charge the Customer interest on the overdue amount at the rate of 8% per annum above the Bank of England base rate from time to time (which interest will accrue daily until the date of actual payment and be compounded at the end of each calendar month); or

(b) claim interest and statutory compensation from the Customer pursuant to the Late Payment of Commercial Debts (Interest) Act 1998.

7.8 Any new checks created or delivered by the Supplier in addition to the Committed Checks initially purchased or noted in the products table, will be offered to the client at the standard EBC Checks charge rate. The client is not obligated to accept these new check services, but in doing so agrees that the new check charge will be added to the current agreement on the current Contractual Term

8. Provider's confidentiality obligations

8.1 The Provider must:

(a) keep the Customer Confidential Information strictly confidential;

(b) not disclose the Customer Confidential Information to any person without the Customer's prior written consent, and then only under conditions of confidentiality approved in writing by the Customer;

(c) use the same degree of care to protect the confidentiality of the Customer Confidential Information as the Provider uses to protect the Provider's own confidential information of a similar nature, being at least a reasonable degree of care; and

(d) act in good faith at all times in relation to the Customer Confidential Information.

8.2 Notwithstanding Clause 8.1, the Provider may disclose the Customer Confidential Information to the Provider's officers, employees, professional advisers, insurers, agents and subcontractors who have a need to access the Customer Confidential Information for the performance of their work with respect to this Agreement and who are bound by a written agreement or professional obligation to protect the confidentiality of the Customer Confidential Information.

8.3 This Clause 8 imposes no obligations upon the Provider with respect to Customer Confidential Information that:

(a) is known to the Provider before disclosure under this Agreement and is not subject to any other obligation of confidentiality;

(b) is or becomes publicly known through no act or default of the Provider; or

(c) is obtained by the Provider from a third party in circumstances where the Provider has no reason to believe that there has been a breach of an obligation of confidentiality.

8.4 The restrictions in this Clause 8 do not apply to the extent that any Customer Confidential Information is required to be disclosed by any law or regulation, by any judicial or governmental order or request, or pursuant to disclosure requirements relating to the listing of the stock of the Provider on any recognised stock exchange.
8.5 The provisions of this Clause 8 shall continue in force for a period of 1 year following the termination of this Agreement, at the end of which period they will cease to have effect.

9. Data protection
9.1 Each party shall comply with the Data Protection Laws with respect to the processing of the Customer Personal Data.
9.2 The Customer warrants to the Provider that it has the legal right to disclose all Personal Data that it does in fact disclose to the Provider under or in connection with this Agreement.
9.3 The Customer shall only supply to the Provider, and the Provider shall only process, in each case under or in relation to this Agreement, the Personal Data of data subjects falling within the categories specified in Part 1 of Schedule 4 (Data processing information) and of the types specified in Part 2 of Schedule 4 (Data processing information); and the Provider shall only process the Customer Personal Data for the purposes specified in Part 3 of Schedule 4 (Data processing information).
9.4 The Provider shall only process the Customer Personal Data during the Term and for not more than 30 days following the end of the Term, subject to the other provisions of this Clause 9.
9.5 The Provider shall only process the Customer Personal Data on the documented instructions of the Customer (including with regard to transfers of the Customer Personal Data to any place outside the European Economic Area), within the EEA (European Economic Area) as set out in this Agreement or any other document agreed by the parties in writing.
9.6 Notwithstanding any other provision of this Agreement, the Provider may process the Customer Personal Data if and to the extent that the Provider is required to do so by applicable law. In such a case, the Provider shall inform the Customer of the legal requirement before processing, unless that law prohibits such information on important grounds of public interest.
9.7 The Provider shall ensure that persons authorised to process the Customer Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.
9.8 The Provider and the Customer shall each implement appropriate technical and organisational measures to ensure an appropriate level of security for the Customer Personal Data, including those measures specified in Part 4 of Schedule 4 (Data processing information).
9.9 The Provider must not engage any third party to process the Customer Personal Data without the prior specific or general written authorisation of the Customer. The Provider is hereby authorised by the Customer, as at the Effective Date, to engage those third parties identified in, or falling within the processor categories specified in, Part 5 of Schedule 4 (Data processing information) to process the Customer Personal Data. In the case of a general written authorisation, the Provider shall inform the Customer at least 14 days in advance of any intended changes concerning the addition or replacement of any third party processor, and if the Customer objects to any such changes before their implementation, then the Provider must not implement the changes.The Provider shall ensure that each third party processor is subject to the same legal obligations as those imposed on the Provider by this Clause 9.
9.10 The Provider shall, insofar as possible and taking into account the nature of the processing, take appropriate technical and organisational measures to assist the Customer with the fulfilment of the Customer's obligation to respond to requests exercising a data subject's rights under the Data Protection Laws.
9.11 The Provider shall assist the Customer in ensuring compliance with the obligations relating to the security of processing of personal data, the notification of personal data breaches to the supervisory authority, the communication of personal data breaches to the data subject, data protection impact assessments and prior consultation in relation to high-risk processing under the Data Protection Laws.
9.12 The Provider shall make available to the Customer all information necessary to demonstrate the compliance of the Provider with its obligations under this Clause 9 and the Data Protection Laws.
9.13 The Provider shall, at the choice of the Customer, delete or return all of the Customer Personal Data to the Customer after the provision of services relating to the processing, and shall delete existing copies save to the extent that applicable law requires storage of the relevant Personal Data.
9.14 The Provider shall allow for and contribute to audits, including inspections, conducted by the Customer or another auditor mandated by the Customer in respect of the compliance of the Provider's processing of Customer Personal Data with the Data Protection Laws and this Clause 9. The Provider may charge the Customer at its

standard time-based charging rates for any work performed by the Provider at the request of the Customer pursuant to this Clause 9.14.
9.15 If any changes or prospective changes to the Data Protection Laws result or will result in one or both parties not complying with the Data Protection Laws in relation to processing of Personal Data carried out under this Agreement, then the parties shall use their best endeavours promptly to agree such variations to this Agreement as may be necessary to remedy such non-compliance.

10. Acknowledgements
10.1 The Customer acknowledges that complex software is never wholly free from defects, errors and bugs; and subject to the other provisions of this Agreement, the Provider gives no warranty or representation that the Hosted Services will be wholly free from defects, errors and bugs.
10.2 The Customer acknowledges that complex software is never entirely free from security vulnerabilities; and subject to the other provisions of this Agreement, the Provider gives no warranty or representation that the Hosted Services will be entirely secure.
10.3 The Customer acknowledges that the Hosted Services are designed to be compatible only with that software and those systems; and the Provider does not warrant or represent that the Hosted Services will be compatible with any other software or systems.
10.4 The Customer acknowledges that the Provider will not provide any legal, financial, accountancy or taxation advice under this Agreement or in relation to the Hosted Services; and, except to the extent expressly provided otherwise in this Agreement, the Provider does not warrant or represent that the Hosted Services or the use of the Hosted Services by the Customer will not give rise to any legal liability on the part of the Customer or any other person.
10.5 The Customer acknowledges responsibility for mistakes on applications to the Provider for criminal checks, credit checks and any of its other submissions. The Customer also accepts that there is no liability on the Provider for applications processed with incorrect data or documents supplied by the Customer.

11. Limitations and exclusions of liability
11.1 Nothing in this Agreement will:
(a) limit or exclude any liability for death or personal injury resulting from negligence;
(b) limit or exclude any liability for fraud or fraudulent misrepresentation;
(c) limit any liabilities in any way that is not permitted under applicable law; or
(d) exclude any liabilities that may not be excluded under applicable law.
11.2 The limitations and exclusions of liability set out in this Clause 11 and elsewhere in this Agreement:
(a) are subject to Clause 11.1; and
(b) govern all liabilities arising under this Agreement or relating to the subject matter of this Agreement, including liabilities arising in contract, in tort (including negligence) and for breach of statutory duty, except to the extent expressly provided otherwise in this Agreement.
11.3 Neither party shall be liable to the other party in respect of any losses arising out of a Force Majeure Event.
11.4 Neither party shall be liable to the other party in respect of any loss of profits or anticipated savings.
11.5 Neither party shall be liable to the other party in respect of any loss of revenue or income.
11.6 Neither party shall be liable to the other party in respect of any loss of use or production.
11.7 Neither party shall be liable to the other party in respect of any loss of business, contracts or opportunities.
11.8 Neither party shall be liable to the other party in respect of any loss or corruption of any data, database or software.
11.9 Neither party shall be liable to the other party in respect of any special, indirect or consequential loss or damage.
11.10 The liability of each party to the other party under this Agreement in respect of any event or series of related events shall not exceed the greater of £5,000 sterling.
11.11 The aggregate liability of each party to the other party under this Agreement shall not exceed the greater of £5,000 sterling.

12. Force Majeure Event
12.1 If a Force Majeure Event gives rise to a failure or delay in either party performing any obligation under this Agreement (other than any obligation to make a payment), that obligation will be suspended for the duration of the Force Majeure Event.

12.2 A party that becomes aware of a Force Majeure Event which gives rise to, or which is likely to give rise to, any failure or delay in that party performing any obligation under this Agreement, must:
(a) promptly notify the other; and
(b) inform the other of the period for which it is estimated that such failure or delay will continue.
12.3 A party whose performance of its obligations under this Agreement is affected by a Force Majeure Event must take reasonable steps to mitigate the effects of the Force Majeure Event.

13. Renewal and Termination
13.1 This Agreement commences on the Effective date and continues for the Minimum Term and is not subject to early termination by the Customer.
13.2 All sums due become immediately payable on termination.
13.3 The Provider may terminate this Agreement by giving to the Customer not less than 90 days written notice of termination. The Customer may terminate this Agreement by giving to the Provider not less than 90 days written notice of termination before the end of the Minimum Term.
13.4 This Agreement will automatically renew on the anniversary of the renewal date Such renewal will trigger a new minimum term of 24 months.
13.5 Either party may terminate this Agreement immediately by giving written notice of termination to the other party if:

(a) the other party commits any breach of this Agreement, and the breach is not remediable;
(b) the other party commits a breach of this Agreement, and the breach is remediable, but the other party fails to remedy the breach within the period of 30 days following the giving of a written notice to the other party requiring the breach to be remedied; or
(c) the other party persistently breaches this Agreement (irrespective of whether such breaches collectively constitute a material breach).

14. Effects of termination
14.1 Upon the termination of this Agreement, all of the provisions of this Agreement shall cease to have effect, save that the following provisions of this Agreement shall survive and continue to have effect (in accordance with their express terms or otherwise indefinitely).
14.2 Except to the extent that this Agreement expressly provides otherwise, the termination of this Agreement shall not affect the accrued rights of either party.
14.3 Within 30 days following the termination of this Agreement for any reason:

(a) the Customer must pay to the Provider any Charges in respect of Services provided to the Customer before the termination of this Agreement; and
(b) the Provider must refund to the Customer any Charges paid by the Customer to the Provider in respect of Services that were to be provided to the Customer after the termination of this Agreement, without prejudice to the parties' other legal rights.

15. Notices
15.1 Any notice from one party to the other party under this Agreement must be given by one of the following methods (using the relevant contact details set out in Clause 15.2):

(a) delivered personally or sent by courier, in which case the notice shall be deemed to be received upon delivery;
(b) sent by recorded signed-for post, in which case the notice shall be deemed to be received 2 Business Days following posting; or
(c) delivered by email, in which case the notice shall be deemed to be received upon delivery,

providing that, if the stated time of deemed receipt is not within Business Hours, then the time of deemed receipt shall be when Business Hours next begin after the stated time.
15.2 The Provider's contact details for notices under this Clause 15 are as follows: EBC Global Ltd, Abacus House, Caxton Place, Cardiff, CF23 8HA, United Kingdom contact@ebcglobal.co.uk.
15.3 The addressee and contact details set out in Clause 15.2 may be updated from time to time by a party giving written notice of the update to the other party in accordance with this Clause 15.

16. Assignment
16.1 The Customer hereby agrees that the Provider may assign, transfer or otherwise deal with the Provider's contractual rights and obligations under this Agreement.
16.2 The Customer must not assign, transfer or otherwise deal with the Customer's contractual rights and/or obligations under this Agreement without the prior written consent of the Provider.

17. No waivers
17.1 No breach of any provision of this agreement will be waived except with the express written consent of a Director of EBC Global.
17.2 No waiver of any breach of any provision of this Agreement shall be construed as a further or continuing waiver of any other breach of that provision or any breach of any other provision of this Agreement.

18. Severability
18.1 If a provision of this Agreement is determined by any court or other competent authority to be unlawful and/or unenforceable, the other provisions will continue in effect.
18.2 If any unlawful and/or unenforceable provision of this Agreement would be lawful or enforceable if part of it were deleted, that part will be deemed to be deleted, and the rest of the provision will continue in effect.

19. Law and jurisdiction
19.1 This Agreement shall be governed by and construed in accordance with English law.
19.2 Any disputes relating to this Agreement shall be subject to the exclusive jurisdiction of the courts of England.

20 **Publicity**.
20.1 The Provider can use the Customer Company's name for press release, advertising or other publicly disseminated material in connection with this agreement.

SCHEDULE 1 (ACCEPTABLE USE POLICY)

1. Introduction

1.1 This acceptable use policy (the "**Policy**") sets out the rules governing:

(a) the use of the website at www.ebcglobal.co.uk, any successor website, and the services available on that website or any successor website (the "**Services**"); and

(b) the transmission, storage and processing of content by you, or by any person on your behalf, using the Services ("**Content**").

1.2 References in this Policy to "you" are to any customer for the Services and any individual user of the Services (and "your" should be construed accordingly); and references in this Policy to "us" are to EBC Global Ltd (and "we" and "our" should be construed accordingly).

1.3 By using the Services, you agree to the rules set out in this Policy.

1.4 We will ask for your express agreement to the terms of this Policy before you upload or submit any Content or otherwise use the Services.

1.5 You must be at least 18 years of age to use the Services; and by using the Services, you warrant and represent to us that you are at least 18 years of age.

2. General usage rules

2.1 You must not use the Services in any way that causes, or may cause, damage to the Services or impairment of the availability or accessibility of the Services.

2.2 You must not use the Services:

(a) in any way that is unlawful, illegal, fraudulent or harmful; or

(b) in connection with any unlawful, illegal, fraudulent or harmful purpose or activity.

2.3 You must ensure that all Content complies with the provisions of this Policy.

3. Unlawful Content

3.1 Content must not be illegal or unlawful, must not infringe any person's legal rights, and must not be capable of giving rise to legal action against any person (in each case in any jurisdiction and under any applicable law).

3.2 Content, and the use of Content by us in any manner licensed or otherwise authorised by you, must not:

(a) be libellous or maliciously false;

(b) be obscene or indecent;

(c) infringe any copyright, moral right, database right, trade mark right, design right, right in passing off, or other intellectual property right;

(d) infringe any right of confidence, right of privacy or right under data protection legislation;

(e) constitute negligent advice or contain any negligent statement;

(f) constitute an incitement to commit a crime, instructions for the commission of a crime or the promotion of criminal activity;

(g) be in contempt of any court, or in breach of any court order;

(h) constitute a breach of racial or religious hatred or discrimination legislation;

(i) be blasphemous;

(j) constitute a breach of official secrets legislation; or

(k) constitute a breach of any contractual obligation owed to any person.

3.3 You must ensure that Content is not and has never been the subject of any threatened or actual legal proceedings or other similar complaint.

4. Factual accuracy

4.1 Content must not be untrue, false, inaccurate or misleading.

4.2 Statements of fact contained in Content and relating to persons (legal or natural) must be true; and statements of opinion contained in Content and relating to persons (legal or natural) must be reasonable, be honestly held and indicate the basis of the opinion.

5. Monitoring

5.1 You acknowledge that we may actively monitor the Content and the use of the Services.

6. Harmful software

6.1 The Content must not contain or consist of, and you must not promote or distribute by means of the Services, any viruses, worms, spyware, adware or other harmful or malicious software, programs, routines, applications or technologies.
6.2 The Content must not contain or consist of, and you must not promote or distribute by means of the Services, any software, programs, routines, applications or technologies that will or may have a material negative effect upon the performance of a computer or introduce material security risks to a computer.

SCHEDULE 2 (SUPPORT SLA)

1. Introduction
1.1 This Schedule 3 sets out the service levels applicable to the Support Services.

2. Helpdesk
2.1 The Provider shall make available to the Customer a helpdesk in accordance with the provisions of this Schedule 3.
2.2 The Customer may use the helpdesk for the purposes of requesting and, where applicable, receiving the Support Services; and the Customer must not use the helpdesk for any other purpose.
2.3 The Provider shall ensure that the helpdesk is accessible by email and using the Provider's web-based ticketing system.
2.4 The Provider shall ensure that the helpdesk is operational during Business Hours during the Term.
2.5 The Customer shall ensure that all requests for Support Services that it may make from time to time shall be made through the helpdesk.

3.Response and resolution
3.1 Issues raised through the Support Services shall be categorised as follows:
(a) critical: the Hosted Services are inoperable or a core function of the Hosted Services is unavailable;
(b) serious: a core function of the Hosted Services is significantly impaired;
(c) moderate: a core function of the Hosted Services is impaired, where the impairment does not constitute a serious issue; or a non-core function of the Hosted Services is significantly impaired; and
(d) minor: any impairment of the Hosted Services not falling into the above categories; and any cosmetic issue affecting the Hosted Services.
3.2 The Customer shall determine, acting reasonably, into which severity category an issue falls.
3.3 The Provider shall use reasonable endeavours to respond to requests for Support Services promptly, and in any case in accordance with the following time periods:
(a) P1 - critical: 4 Business Hours;
(b) P2 - serious: 1 Business Day;
(c) P3 - minor: 5 Business Days; and
3.4 The Provider shall use reasonable endeavours to resolve issues raised through the Support Services promptly, and in any case in accordance with the following time periods:
(a) P1 - critical: 8 Business Hours;
(b) P2 - serious: 2 Business Days;
(c) P3 - minor: 5 Business Days; and

4. Provision of Support Services
4.1 The Support Services shall be provided remotely, save to the extent that the parties agree otherwise in writing.

5. Limitations on Support Services
5.1 The Provider shall have no obligation to provide Support Services in respect of any issue caused by:
(a) the improper use of the Hosted Services by the Customer; or
(b) any alteration to the Hosted Services made without the prior consent of the Provider.

SCHEDULE 3 (DATA PROCESSING INFORMATION)

1. Categories of data subject
1.1 The Provider may process data for Employees stored on the Hosted Services by the Customer.

2. Types of Personal Data

2.1 The Provider may process any data provided to, stored on or collected by the Hosted Services by the Customer of the following

1.Application form - Employee profile

A. Personal details
    a. Title
    b. Full name
    c. Previous name used
        i. Date from
        ii. Date to
    d. Date of Birth
    e. Town of Birth
    f. Country of Birth
    g. Nationality
    h. 2nd Nationality
    i. Passport/ID number
    j. Passport/ID country of issue
    k. Visa/Work permit number
    l. UK Driving Licence number
    m. NI Number
    n. Mobile number
    o. Landline number
    p. Email address
    q. Mother's maiden name

B. Current/Previous address
    a. Address line 1
    b. Address line 2
    c. Town
    d. County
    e. Postcode
    f. Country
    g. Resident from date
    h. Resident to date (previous address only)

C. Documentation upload
    a. Proof of ID
    b. Proof of Address
    c. Proof of NI Number
    d. Driving Licence
    e. Consent form
    f. Other supporting documentation

2. References

a. Employment reference
    a. Third party back up reference
    b. Educational reference
    c. Employment reference
    d. Employment in family business reference
    e. Gap reference
    f. HMRC reference
    g. Job Centre Plus reference
    h. Personal reference
    i. Self-employment reference
    j. Sponsoring company reference
    k. Voluntary sector reference

2. Referee full name
3. Referee first name
4. Company name

5. Address line 1
6. Address line 2
7. Town
8. County
9. Postcode
10. Country
11. Primary contact number
12. Secondary contact number
13. Primary email address
14. Secondary email address
15. Position
16. Type of work
17. Location
18. Hours per week
19. Reason for leaving
20. Other details
21. Dates not available (Y/N)
22. Dismissed(Y/N)
23. Would you re-employ (Y/N)

3. Purposes of processing

3.1 The Provider may process data to generate application forms, documents and references.
3.2 The Provider may process data to generate printable version or email reference requests.
3.3 The Provider may process data to apply for Basic, Standard or Enhanced DBS, Disclosure Scotland, Acces Northern Ireland, for Adverse credit checks, sanction list checks, driving licence checks or any other legitimate check that is required for employment screening puposes.

4. Security measures for Personal Data

4.1 The Provider will take appropriate technical and organisational precautions to secure Customer's personal data and to prevent the loss, misuse or alteration of Customer's personal data.
4.2 The Provider will store all Customer's personal data on secure servers, personal computers and mobile devices, and in secure manual record-keeping systems.
4.3 Customer's personal data stored on secured servers will be stored by the Provider in encrypted form.
4.4 The Customer acknowledge that the transmission of unencrypted (or inadequately encrypted) data over the internet is inherently insecure, and the Provider cannot guarantee the security of data sent over the internet.
4.5 The Customer should ensure that passwords used to access the Hosted Services and are not susceptible to being guessed, whether by a person or a computer program. The Customer is responsible for keeping the passwords confidential and the Provider will not ask the Customer for passwords except when the Customer log in to the Hosted Services.

5. Sub-processors of Personal Data

5.1 Personal data may be processed by one of the following organisations for which EBC Global has an obligation to ensure service continuation from providers and assumes the liability for such service: The Disclosure and Barring Service, Disclosure Scotland, The DVLA, Trans Union, Equifax, CreditSafe, Verifile and other organisations.

PERSONAL DATA BREACH NOTIFICATION POLICY

1. Introduction

1.1 This policy sets out the policies and procedures of EBC Global Ltd (the "**company**") with respect to detection of personal data breaches, responding to personal data breaches and notification of personal data breaches to supervisory authorities, data controllers and data subjects.
1.2 When dealing with personal data breaches, the company and all company personnel must focus on protecting individuals and their personal data, as well as protecting the interests of the company.

2. Definitions

2.1 In this policy:

(a) "**Appointed Person**" means the individual primarily responsible for dealing with personal data breaches affecting the company, being the data protection officer of the company;
(b) "**Data Controller**" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data;
(c) "**Data Processor**" means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;
(d) "**Data Subject**" means an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;
(e) "**Personal Data"** means any information relating to a data subject;
(f) "**Personal Data Breach**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed by the company (including any temporary or permanent loss of control of, or inability to access, personal data); and
(g) "**Supervisory Authority**" means the Information Commissioner's Office of the United Kingdom.

3. Detection of personal data breaches

3.1 The company has put in place technological measures to detect incidents which may result in personal data breaches.
3.2 The company has put in place organisational measures to detect incidents which may result in personal data breaches.
3.3 The company shall regularly review the technical and organisational measures it uses to detect incidents which may result in a personal data breach. Such reviews shall be carried out at least quarterly.

4. Responding to personal data breaches

4.1 All personnel of the company must notify the appointed person immediately if they become aware of any actual or possible personal data breach.
4.2 The appointed person is primarily responsible for investigating possible and actual personal data breaches and for determining whether any notification obligations apply. Where notification obligations apply, the appointed person is responsible for notifying the relevant third parties in accordance with this policy.
4.3 All personnel of the company must cooperate with the appointed person in relation to the investigation and notification of personal data breaches.
4.4 The appointed person must determine whether the company is acting as a data controller and/or a data processor with respect to each category of personal data that is subject to a personal data breach.
4.5 The steps to be taken by the appointed person when responding to a personal data breach may include:

(a) ensuring that the personal data breach is contained as soon as possible;
(b) assessing the level of risk to data subjects as soon as possible;
(c) gathering and collating information from all relevant sources;
(d) considering relevant data protection impact assessments;
(e) informing all interested persons within the company of the personal data breach and the investigation;
(f) assessing the level of risk to the company; and
(g) notifying supervisory authorities, data controllers, data subjects and others of the breach in accordance with this policy.

4.6 The appointed person shall keep a full record of the response of the company to a personal data breach, including the facts relating to the personal data breach, its effects and the remedial action taken. This record shall form part of the personal data breach register of the company.

5. Notification to supervisory authority

5.1 This section 5 applies to personal data breaches affecting personal data with respect to which the company is acting as a data controller.
5.2 The company must notify the supervisory authority of any personal data breach to which this section 5 applies without undue delay and, where feasible, not later than 72 hours after the company becomes aware of the breach, save as set out in subsection 5.4.
5.3 Personal data breach notifications to the supervisory authority must be made by the appointed person using the form set out in Form 1 (Notification of personal data breach to supervisory authority). The completed form must be sent to the supervisory authority by secure and confidential means. The appointed person must keep a record of all notifications, and all other communications with the supervisory authority relating to the breach, as part of the personal data breach register of the company.
5.4 The company will not notify the supervisory authority of a personal data breach where it is unlikely to result in a risk to the rights and freedoms of natural persons. The appointed person shall be responsible for determining whether this subsection 5.4 applies, and the appointed person must create a record of any decision not to notify the supervisory authority. This record should include the appointed person's reasons for believing that the breach is unlikely to result in a risk to the rights and freedoms of natural person. This record shall be stored as part of the personal data breach register of the company.
5.5 To the extent that the company is not able to provide to the supervisory authority all the information specified in Form 1 (Notification of personal data breach to supervisory authority) at the time of the initial notification to the supervisory authority, the company must make all reasonable efforts to ascertain the missing information. That information must be provided to the supervisory authority, by the appointed person, as and when it becomes available. The appointed person must create a record of the reasons for any delayed notification under this subsection 5.5. This record shall be stored as part of the personal data breach register of the company.
5.6 The company must keep the supervisory authority informed of changes in the facts ascertained by the company which affect any notification made under this section 5.

6. Notification to Data Controller

6.1 This section 6 applies to personal data breaches affecting personal data with respect to which the company is acting as a data processor.
6.2 The company must notify the affected data controller(s) of any personal data breach to which this section 6 applies without undue delay.
6.3 Personal data breach notifications to the affected data controller(s) must be made by the appointed person using the form set out in Form 2 (Notification of personal data breach to data controller). The completed form must be sent to the affected data controller(s) by secure and confidential means. The appointed person must keep a record of all notifications, and all other communications with the affected data controller(s) relating to the breach, as part of the personal data breach register of the company.
6.4 To the extent that the company is not able to provide to the affected data controller(s) all the information specified in Form 2 (Notification of personal data breach to data controller) at the time of the initial notification to the affected data controller(s), the company must make all reasonable efforts to ascertain the missing information. That information must be provided to the affected data controller(s), by the appointed person, as and when it becomes available.

7. Notification to data subjects

7.1 This section 7 applies to personal data breaches affecting personal data with respect to which the company is acting as a data controller.
7.2 Notifications to data subject under this section 7 should, where appropriate, be made in consultation with the supervisory authority and in accordance with any guidance given by the supervisory authority with respect to such notifications.
7.3 The company must notify the affected data subjects of any personal data breach to which this section 7 applies if the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, save as set out in subsection 7.5.

7.4 Personal data breach notifications to the affected data subjects must be made by the appointed person in clear and plain language using the form set out in Form 3 (Notification of personal data breach to data subject). The completed form must be sent to the affected data subjects by appropriate means. The appointed person must keep a record of all notifications, and all other communications with the affected data subjects relating to the breach, as part of the personal data breach register of the company.

7.5 The company has no obligation to notify the affected data subject of a personal data breach if:

(a) the company has implemented appropriate technical and organisational protection measures (in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption), and those measures have been applied to the personal data affected by the personal data breach;

(b) the company has taken subsequent measures which ensure that a high risk to the rights and freedoms of data subjects is no longer likely to materialise;

(c) it would involve disproportionate effort (in which case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner),

providing that the appointed person shall be responsible for determining whether this subsection 7.5 applies, and the appointed person must create a record of any decision not to notify the affected data subjects. This record should include the appointed person's reasons for believing that the breach does not need to be notified to the affected data subjects. This record shall be stored as part of the personal data breach register of the company.

7.6 If the company is not required by this section 7 to notify affected data subjects of a personal data breach, the company may nonetheless do so where such notification is in the interests of the company and/or the affected data subjects.

8. Other notifications

8.1 Without affecting the notification obligations set out elsewhere in this policy, the appointed person should also consider whether to notify any other third parties of a personal data breach. Notifications may be required under law or contract. Relevant third parties may include:

(a) the police;
(b) other law enforcement agencies;
(c) insurance companies;
(d) professional bodies;
(e) regulatory authorities;
(f) financial institutions; and/or
(g) trade unions or other employee representatives.

9. Reviewing and updating this policy

9.1 Person(s) or group(s) shall be responsible for reviewing and updating this policy.

9.2 This policy must be reviewed and, if appropriate, updated annually on or around 25th of May.

9.3 This policy must also be reviewed and updated on an ad hoc basis if reasonably necessary to ensure:

(a) the compliance of the company with applicable law, codes of conduct or industry best practice;
(b) the security of data stored and processed by the company; or
(c) the protection of the reputation of the company.

9.4 The following matters must be considered as part of each review of this policy:

(a) changes to the legal and regulatory environment;
(b) changes to any codes of conduct to which the company subscribes;
(c) developments in industry best practice;
(d) any new data collected by the company;
(e) any new data processing activities undertaken by the company; and
(f) any security incidents affecting the company.

FORM 1 (NOTIFICATION OF PERSONAL DATA BREACH TO SUPERVISORY AUTHORITY)

1. Introduction
2. Description of personal data breach
3. Categories of data subject affected
4. Number of data subjects affected
5. Categories of personal data concerned
6. Number of records concerned
7. Likely consequences of breach
8. Measures taken to address breach
9. Has breach been notified to data subjects?
10. Late report of breach
11. Contact details

FORM 2 (NOTIFICATION OF PERSONAL DATA BREACH TO DATA CONTROLLER)

1. Introduction
2. Description of personal data breach
3. Categories of data subject affected
4. Number of data subjects affected
5. Categories of personal data concerned
6. Number of records concerned
7. Likely consequences of breach
8. Measures taken to address breach
9. Contact details

FORM 3 (NOTIFICATION OF PERSONAL DATA BREACH TO DATA SUBJECT)

1. Introduction
2. Description of personal data breach
3. Categories of data subject affected
4. Likely consequences of breach
5. Measures taken to address breach
6. Steps to mitigate breach
7. Contact details

SIGNED ON BEHALF OF THE PROVIDER

Signed:

Name:

Matt Masson

Title:

Managing Director

Date:
24th October 2024

SIGNED ON BEHALF OF THE CUSTOMER

Signed:

Name:

Title:

Date:
