

"Webrecruit ATS" Agreement

This Services Agreement ("Agreement") is entered into on the **DATE** for a period of **PERIOD** (Initial Term) from and including the Commencement Date between:

"WRG" (WR Group Ltd, trading as Webrecruit, company registration number 04838590) whose registered office is Queensgate House, 48 Queen Street, Exeter, Devon, EX4 3SR.

and

xxxxxxx (company registration number **xxxxxxx**) whose registered office is **xxxxxxx** (the "Customer")

OVERVIEW:

- ❖ Customer wishes to purchase and WRG wishes to provide a range of Services described herein;
- ❖ The parties agree that such Services shall be supplied in accordance with the terms of this Agreement. Words in the singular include the plural and in the plural include the singular.
- ❖ The terms and conditions in the Schedules supplement constitute those of the Agreement and in the event of a conflict between the terms of the Schedules and those of the Agreement, the terms of the Agreement shall prevail.
- ❖ Clause and Schedule headings shall not affect the interpretation of this Agreement.
- ❖ References to clauses and Schedules are, unless otherwise provided, references to the clauses of and schedules to this Agreement.
- ❖ 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 made under it.
- ❖ Unless a right or remedy of a party is expressed to be an exclusive right or remedy, the exercise of it by a party is without prejudice to that party's other rights and remedies.
- ❖ A reference to this Agreement includes a reference to the Schedules to this Agreement.
- ❖ A reference to one gender shall include reference to the other gender.
- ❖ A *person* includes a corporate or unincorporated body (whether or not having separate legal personality). Any phrase introduced by the words including, includes or in particular or for example or similar shall be construed as illustrative and shall not limit the generality of the related general words.

1. DEFINITIONS

The following definitions and rules of interpretation shall apply throughout this Agreement:

Applicant or Candidate:	A record in the System for a person who has registered or applied for a specific position or who has been entered into the System through an alternative method.
Commencement Date:	Upon WRG providing the Customer with access to System and / or advertising services estimated to be DATE . WRG will make the System available to the Customer in advance of the Commencement Date for training purposes.
Confidential Information:	any information, however conveyed or presented, that relates to the business, affairs, operations, customers, processes, budgets, pricing policies, product information, strategies, developments, trade secrets, know-how, personnel and suppliers of the disclosing party (and, in the case of the Customer, of the Customer's Group), together with all information derived by the receiving party from any such information and any other information clearly designated by a party as being confidential to it (whether or not it is marked "confidential"), or which ought reasonably be considered to be confidential.

Customer's Data:	any data (including any Personal Data relating to Candidates or employees of the Customer), documents, text, drawings, diagrams, images or sounds (together with any database made up of any of those), embodied in any medium, that are supplied to WRG by or on behalf of the Customer, or which WRG is required to generate, process, store or transmit pursuant to this Agreement.
Data Controller:	has the meaning set out in the GDPR or any future relevant legislation.
Data Processor:	has the meaning set out in the GDPR or any future relevant legislation.
Data Protection Legislation:	the UK General Data Protection Regulation (EU Retained GDPR 2016/679), Data Protection Act 2018, the Privacy and Electronic Communications Regulations 2003, the European General Data Protection Regulation where applicable and all other applicable laws and regulations relating to the processing of personal data and privacy whether in force at the time of this Agreement or which may come in to force from time to time following the date of this Agreement, including where applicable the guidance and codes of practice issued by the Information Commissioner.
Data Subject:	has the meaning set out in the GDPR or any future relevant legislation.
Fees:	the fees set out in Schedule 2.
Force Majeure Event:	any cause affecting the performance by a party of its obligations under this Agreement arising from acts, events, omissions or non-events beyond its reasonable control, including but not limited to acts of God, riots, war, acts of terrorism, fire, flood, storm or earthquake and any disaster.
Initial Term:	the period of PERIOD from the Commencement Date.
Intellectual Property Rights: (IPR's)	all intellectual property rights of any nature anywhere in the world whether registered, or otherwise, including patents, trademarks, registered designs and domain names, applications for any of the foregoing, trade or business names, goodwill, copyright and rights in the nature of copyright, design rights, rights in databases, moral rights, know-how and any other intellectual property rights which subsist in computer software, computer programs, websites, documents, information, techniques, business methods, drawings, logos, instruction manuals, lists and procedures and particulars of customers, marketing methods and procedures and advertising literature, including the "look and feel" of any websites.
Personal Data:	has the meaning set out in the GDPR (or any future relevant legislation) and relates only to personal data of which the Customer is the data controller and in relation to which WRG is providing the service.
Proprietary Database:	the Applicant or Candidate data collected and stored by WRG exclusively for the Customer and managed using software which is maintained according to the service levels set out in Schedule 3.
Services:	the services to be delivered by or on behalf of WRG under this Agreement as set out in Schedule 1.
Software	the software code included in the System and used to provide part of the Services.
System	the Webrecruit ATS system as adapted by WRG for the Customer for processing recruitment Data and information via the internet to facilitate the recruitment of personnel by the Customer, the specification of which is set out in the attached schedules.
Term:	the period of the Initial Term as may be varied by:

- (a) any extensions to this Agreement agreed in writing by the parties, or
- (b) the earlier termination of this Agreement in accordance with the Suspension and Termination rights

Termination Date: the date on which this Agreement terminates.

Termination Notice: notice to terminate this Agreement by either party in accordance with the Suspension and Termination rights

Working Day: Monday to Friday, excluding any public holidays in England and Wales.

1. COMMENCEMENT & DURATION

This Agreement shall take effect on the Commencement Date and shall continue until the end of the Initial Term, unless terminated in part or full by either party in accordance with the terms of this Agreement.

2. SERVICES

WRG will provide the Services (as set out in Schedule 1) during the Term to the Customer in return for the payment of the Fees and subject to the terms and conditions of this Agreement.

3. WRG'S OBLIGATIONS

In providing each of the Services, WRG shall at all times:

- (a) provide the Services described in Schedule 1 with all due care and skill and to a high standard which is no less than that which might reasonably be expected of a professional provider of services of such a type;
- (b) use all reasonable endeavours to meet the service levels set out in Schedule 1, at all times during the Term;
- (c) review the Services and performance with the Customer on a quarterly basis (or at such other intervals as the parties shall agree) and discuss in good faith any actions required by either party to enhance or improve the Services; and
- (d) provide the Services in accordance with all applicable laws, regulations and best practice.
- (e) provide the Customer promptly upon request with such information or cooperation as the Customer shall reasonably require in the event of any legal proceedings (including but not limited to in the Employment Tribunal) being intimated or commenced against the Customer by any Candidate or Applicant.

4. CUSTOMER'S RIGHTS AND OBLIGATIONS

The Customer:

- (a) shall at all times co-operate with the reasonable requests of WRG in providing the Services and shall promptly provide WRG with all information which WRG may reasonably request from the Customer in order to provide the Services; and
- (b) will comply with all applicable laws and regulations with respect to its activities under this Agreement.

5. CHARGING & INVOICING

- (a) In consideration of the provision of the Services by WRG the Customer shall pay the Fees.
- (b) WRG shall invoice the Customer for payment of the Fees at the intervals specified in Schedule 2
- (c) The Customer shall pay the undisputed Fees within thirty days (30) of the date of receipt of the invoice (the "*Due Date*").
- (d) If the Customer receives an invoice which it reasonably believes includes a sum which is not valid and properly due then the Customer shall notify WRG in writing within ten (10) working days. In the event that such notice is not given then full payment will be deemed due on the Due Date.
- (e) The Customer shall pay the balance of the invoice which is not in dispute by the Due Date;
 - (i) to the extent that the Customer is obliged, following resolution of the dispute, to pay an amount, then WRG may charge interest at the base rate for the time being of Barclays Bank Plc from the original Due Date until the date of payment; and
 - (ii) once the dispute has been resolved, where either party is required to make a balancing payment, it shall do so within ten (10) Working Days or, if later, by the Due Date.

- (f) Interest shall be payable on the late payment of any undisputed Fees properly invoiced under this Agreement at the rate of 3% per annum above the base rate for the time being of Barclays Bank Plc, calculated on a daily basis.
- (g) The Fees are stated exclusive of VAT, which shall be added at the prevailing rate as applicable and paid by the Customer following delivery of a valid VAT invoice.
- (h) The Customer shall be entitled to offset any service credits owed to it by WRG due pursuant to Schedule 3 against any fees due.

6. ACCEPTANCE OF SYSTEM

- (a) If, following the Launch Date, the Customer discovers any faults or deviations with the System that were not apparent during testing or training, it shall promptly notify WRG and WRG shall work to remedy such faults and/or deviations at no additional cost to the Customer.
- (b) If at any time (i.e. before or after the Launch Date) the Customer requires improvements or other modifications to be made to the System, the Customer may request that WRG develop such improvements and/or modifications and the parties shall negotiate in good faith the terms on which they shall be developed (including any additional Fees to be paid by the Customer).
- (c) Post Launch Date, WRG reserves the right to alter the structure of the data at any time to improve the efficiency and effectiveness of the System and/or Services save that it shall not thereby cause any diminution of the System and/or Service provided to the Customer.

7. GUARANTEE OF SYSTEM

- (a) WRG shall use all reasonable endeavours to ensure that:
 - (i) the System is available to the Customer during the Availability Period specified in Schedule 1; and
 - (ii) the System does not suffer delays in terms of page loading and information processing when in use by a number of Candidates and/or employees of the Customer, provided that such usage does not exceed the reasonable levels.

If the System and Services do become unavailable at any point and/or the System begins to suffer delays as described above, upon receipt of notification from the Customer, WRG shall use all reasonable endeavours to make the System and Services available again, and/or resolve the problems causing delay, as quickly as possible.

8. SYSTEM SECURITY AND SOFTWARE UPGRADES

- (a) WRG shall use all reasonable endeavours to ensure that the System software is free from any defects, viruses, worms, Trojan horses or other malware and that the data and System is secure and to prevent unauthorised access to the System and data and/or the destruction of any Data and/or computer and/or system by means of any defect or virus in the Software or mechanical failure.
- (b) WRG shall ensure that the Customer shall have prompt access to any revised versions of the Software that effect improvements to the System or their performance. For the avoidance of doubt, and unless agreed otherwise, this undertaking shall not extend to include substantial new developments beyond the Services as set out in Schedule 1.

9. INTELLECTUAL PROPERTY RIGHTS (IPR's)

In respect of Intellectual Property Rights (IPR's):

- (a) the Customer shall not acquire any right, title or interest in or to the IPR's of WRG or its licensors, including:
 - (i) the IPR's relating to the technology provided by WRG;
 - (ii) the IPR's relating to WRG documentation, processes and procedures; and
 - (iii) the IPR's relating to WRG know-how.
- (b) WRG shall not acquire any right, title or interest in or to the IPR's of the Customer or its licensors, including:
 - (i) the IPR's relating to the Customer's documentation, processes and procedures;
 - (ii) the IPR's relating to the Customer's know-how; and

- (iii) the IPR's relating to the Customer's Data.
- (c) WRG hereby grants the Customer a licence to use such intellectual property rights for the purposes of receiving and obtaining the full benefit of the System and Services as described in this Agreement.
- (d) Where either party acquires, by operation of law, title to IPR's of the other referred to in this clause, and this acquisition is inconsistent with the allocation of title set out in this clause, such IPR's shall be assigned by it to the other party on the request of the other party, whenever that request is made.
- (e) The Customer hereby grants WRG a licence to use those trademarks owned by it and featuring the Customer's name or logos for the duration of this Agreement, solely to the extent required for WRG to comply with its obligations under this Agreement.
- (g) Where the Customer provides its consent, in the event of the termination of this Agreement, the consent referred to in this clause shall terminate automatically.
- (h) The Customer agrees to take all reasonable steps to ensure that the Customer's employees respect the intellectual property rights, and that the Service and Data are not used in any way that might infringe these rights.

10. DATA PROTECTION

- (a) With respect to the parties' rights and obligations under this Agreement, the parties agree that the Customer is the Data Controller and that WRG is the Data Processor.
- (b) WRG shall take reasonable precautions to preserve the integrity of any Data which it processes and to prevent any corruption or loss of such Data.
- (c) WRG shall use the System:
 - (i) to process the Personal Data on behalf of the Customer, only for the purposes of performing this Agreement;
 - (ii) at all times comply with the provisions of the GDPR
- (c) WRG shall notify the Customer without any undue delay if it receives:
 - (i) a request from a data subject to have access to that person's Personal Data; or
 - (ii) a complaint or request relating to the Customer's obligations under the Data Protection Legislation.

The provisions of this clause 10 shall be without prejudice to the provisions of the data processing agreement entered into by the parties. In the event of any conflict discrepancy or inconsistency the provisions of the data processing agreement shall prevail.

11. CONFIDENTIALITY

- (a) Except to the extent set out in this clause 11, or where disclosure is expressly permitted elsewhere in this Agreement, neither party shall during the duration of this Agreement or thereafter without the prior written consent of the other party divulge or permit to be divulged by any employee or sub-contractor to any person or use or exploit any Confidential Information of the other party.
- (b) This clause shall not apply to the extent that:
 - (i) such information was in the possession of the party making the disclosure, without obligation of confidentiality, prior to its disclosure; or such information was obtained from a third party without obligation of confidentiality; or
 - (ii) such information was already in the public domain at the time of disclosure otherwise than through a breach of this Agreement; or such information was independently developed without access to the other party's Confidential Information.
- (c) Both parties agree that they shall not, and shall procure that their employees do not, use any of the other party's Confidential Information received otherwise than for the purposes of this Agreement.

12. FORCE MAJEURE

- (a) Neither party to this Agreement shall be liable to the other for any delay or non-performance of its obligations under this Agreement to the extent that such non-performance is due to a Force Majeure Event.
- (b) As soon as practicable following the commencement of a Force Majeure Event the affected party shall notify the other. On receipt of the affected party's notification, the parties shall consult with each other in good faith and use all reasonable endeavours to agree appropriate terms to mitigate the effects of the Force Majeure Event and to facilitate the continued performance of this Agreement.
- (c) The affected party shall notify the other party as soon as practicable after the Force Majeure Event ceases or no longer causes the affected party to be unable to comply with its obligations under this Agreement. Following such notification, this Agreement shall continue to be performed on the terms existing immediately prior to the occurrence of the Force Majeure Event unless agreed otherwise by the parties.

13. LIMITATIONS ON LIABILITY

- (a) WRG is liable for and shall indemnify and keep the Customer fully indemnified on demand from and against each and every action, proceeding, liability, loss, damage, cost, claim, fine, expense and/or demand suffered or incurred by the Customer which arise from or in connection with or pursuant to any act or omission of or the performance of WRG's obligations under this Agreement, including without limitation those arising out of third party demand, claim or action, or any breach of contract, negligence, fraud, wilful misconduct, breach of statutory duty or non-compliance with this Agreement or any part of the Data Protection Legislation by WRG or any claim that is referred to in Clause 13 (b) and Clause 13 (c).
- (b) WRG acknowledges and agrees with the Customer that Data Subjects who suffer loss, costs or damage (the "**Damages**") as a result or a consequence of the acts and/or omissions of or a breach of the provisions of this Agreement or any part of the Data Protection Legislation by or on behalf of WRG shall be entitled to receive compensation from WRG for such Damages.
- (c) WRG acknowledges and agrees with the Customer that it shall be liable (to the exclusion of the Customer, as between the Customer and WRG) for any such Damages that may be due to or awarded to any such Data Subject by any court, authority or person of competent jurisdiction and that the indemnity set out in Clause 13 (a) shall apply in respect of any such Damages.
- (d) Subject to clause 13 (e), the Customer's total liability under this Agreement shall in no circumstances exceed three times the annual licence fees paid to WRG under the Main Agreement at the time such loss is suffered (see separate Schedule for agreed licence fees).
- (e) Nothing in this Agreement will exclude, limit or restrict either party's liability for:
 - (i) death or personal injury resulting from the negligence of that party (or its officers, agents or employees);
 - (ii) fraud or fraudulent misrepresentation committed by that party (or its officers, agents or employees); or
 - (iii) any other matter in respect of which liability cannot by applicable law be limited.
- (f) Nothing in this clause 13 shall restrict or limit a party's general obligation at law to mitigate a loss it may suffer or incur as a result of an event that may give rise to a claim under the indemnity in clause 13 (a).
- (g) Except as expressly and specifically provided in this Agreement:
 - (i) The Customer assumes sole responsibility for results obtained from the use of the Services, and for conclusions drawn from such use. WRG shall have no liability for any damage caused by errors or omissions in any information, instructions or scripts provided to the Customer by any Candidate in connection with the Services; and
 - (ii) all and any interaction and communication between the Customer and any Candidate in connection with the Candidate's response to a recruitment campaign are the responsibility of the Customer, and WRG accepts no liability whatsoever therewith.

14. SUSPENSION AND TERMINATION RIGHTS

- (a) WRG shall be entitled to suspend performance of the Services either in whole or part whether temporarily or permanently without any liability if the Customer has not paid any undisputed Fees by the relevant Due Date provided that WRG has first served the Customer with written notice of such non-payment and given the Customer a reasonable period to rectify such non-payment.
- (b) Without prejudice to any other rights or remedies to which the parties may be entitled, either party may terminate this Agreement without liability to the other if:
 - (i) the other party commits a material breach of any of the terms of this Agreement and (if such a breach is remediable) fails to remedy that breach within thirty (30) days of that party being notified in writing of the breach; or
 - (ii) an order is made or a resolution is passed for the winding up of the other party, or circumstances arise which entitle a court of competent jurisdiction to make a winding-up order in relation to the other party; or
 - (iii) an order is made for the appointment of an administrator to manage the affairs, business and property of the other party, or documents are filed with a court of competent jurisdiction for the appointment of an administrator of the other party, or notice of intention to appoint an administrator is given by the other party or its directors; or
 - (iv) a receiver is appointed of any of the other party's assets or undertaking, or if circumstances arise which entitle a court of competent jurisdiction or a creditor to appoint a receiver or manager of the other party, or if any other person takes possession of or sells the other party's assets; or
 - (v) the other party makes any arrangement or composition with its creditors, or makes an application to a court of competent jurisdiction for the protection of its creditors in any way, or becomes bankrupt; or
 - (vi) the other party ceases, or threatens to cease, to trade.
 - (vii) The Customer shall have the right to terminate the agreement should WRG fail to comply with GDPR legislation
 - (viii) WRG shall have the right to terminate the contract if the Customer's privacy and data processing policies are non-compliant with relevant legislation.
- (c) Either party may, during the continuance of any Force Majeure Event affecting the other party's ability to comply with this Agreement, terminate this Agreement by written notice to that other party if a Force Majeure Event occurs that affects all or a substantial part of the Services and which continues for more than twenty (20) working days.
- (d) Termination of this Agreement, for any reason, shall not affect the accrued rights, remedies, obligations or liabilities of either party existing at termination.

15. GENERAL CONSEQUENCES OF EXPIRY AND TERMINATION

On the Termination Date:

- (a) the Customer shall pay any undisputed Fees which are owing, due or accrued to WRG in respect of the Services in accordance with the agreed provisions on invoicing and payment terms set out above.
- (b) WRG shall cease to handle any Customer Data and shall return to the Customer all documents and materials (and any copies) containing, reflecting, incorporating or based on the Customer's Confidential Information.
- (c) The Proprietary Database will not be available to the Customer and unless notified accordingly, this data will be destroyed. The Customer must notify WRG within thirty (30) days after the effective date of the termination or expiration of this Agreement, if the Customer requires the Proprietary Database data in the System to be transferred to the Customer. If the Customer so requires WRG shall promptly provide the Customer with a complete copy of the data in .csv format or such other format as the Customer shall reasonably require. Thereafter WRG shall delete such data from its systems
- (d) Upon the request of the Customer WRG shall provide reasonable assistance to the Customer in transferring to an alternative provider of recruitment services or bringing such activities in house. The Customer shall pay all reasonable costs incurred by WRG in providing this assistance to the Customer.

The provisions of clauses 10, 11, 15 shall survive the expiry or termination of this Agreement.

16. DISPUTE RESOLUTION PROCEDURE

- (a) The parties shall attempt, in good faith, to resolve any dispute promptly by negotiation. If within 21 days of either party being notified by the other of a dispute then the notifying party must record its grievance and submit it in writing to
 - (i) in the case of a Customer escalation to WRG, the matter must be addressed to the Managing Director, WRG; and
 - (ii) in the case of WRG escalating to the Customer, the matter must be addressed to the Managing Director.
- (b) Nothing in this clause shall prevent either party from instigating legal proceedings where an order for an injunction, disclosure or legal precedent is required.

17. ASSIGNMENT, NOVATION & SUBCONTRACTING

Neither party shall assign, novate or otherwise dispose of any or all of its rights and obligations under this Agreement without the prior written consent of the other (which consent shall not be unreasonably withheld or delayed).

WRG shall not sub-contract any part of the Services without the Customer's prior written consent (which consent is deemed to be given in respect of the hosting services to be provided by OVH). WRG shall remain fully liable to the Customer for the acts or omissions of any sub-contractor.

18. VARIATIONS AND CHANGE CONTROL

This Agreement may not be varied except by an Agreement in writing expressed to vary this Agreement signed by duly authorised representatives of the parties.

19. WAIVER AND ACCUMULATION OF REMEDIES

- (a) The rights and remedies provided by this Agreement may be waived only in writing by the relevant representative in a manner that expressly states that such waiver is intended for, and such waiver shall only be operative with regard to, the specific circumstances referred to.
- (b) Any failure to exercise, or any delay in exercising, a right or remedy by either party shall not constitute a waiver of that right or remedy, or of any other rights or remedies.
- (c) The rights and remedies provided by this Agreement are cumulative and, unless otherwise provided in this Agreement, are not exclusive of any right or remedies provided at law, in equity or otherwise under this Agreement.

20. RELATIONSHIP OF THE PARTIES

Nothing in this Agreement is intended to create a partnership or legal relationship of any kind that would impose liability on one party for the act or failure to act of the other party, or to authorise either party to act as agent for the other party. Neither party shall make representations, act in the name of, on behalf of or otherwise bind the other party.

21. SEVERANCE AND THIRD PARTY RIGHTS

- (a) If any provision of this Agreement is held invalid, illegal or unenforceable for any reason by any court of competent jurisdiction, such provision shall be severed without effect to the remainder of the provisions. If a provision of this Agreement that is fundamental to the accomplishment of the purpose of this Agreement is held to any extent to be invalid, WRG and the Customer shall immediately commence good faith negotiations to remedy such invalidity. Neither party shall unreasonably withhold or delay their Agreement to any such matters.
- (b) This Agreement does not create, and shall not be construed as creating, any right under the Contracts (Rights of Third Parties) Act 1999 which is enforceable by any person who is not party to this Agreement.

22. ENTIRE AGREEMENT

- (a) This Agreement and accompanying Data Processing Agreement constitutes the entire Agreement and understanding between the parties in respect of the matters dealt with in it and supersedes, cancels and nullifies any previous Agreement between the parties in relation to such matters notwithstanding the terms of any previous Agreement or arrangement expressed to survive termination.
- (b) Each of the parties acknowledges and agrees that, in entering into this Agreement it does not rely on, and shall have no remedy in respect of, any statement, representation, warranty or undertaking (whether negligently or innocently made) other than as expressly set out in this Agreement. The only remedy available to either party in respect of any such statement, representation, warranty or undertaking shall be for breach of contract under the terms of this Agreement. Nothing in this clause shall operate to exclude any liability for fraud.

23. NOTICES

Any notice required to be given under or in connection to this agreement shall be in writing, signed by or on behalf of the party giving it and shall be served by delivering it personally, or by sending it by pre-paid first-class post, recorded delivery or registered post to the registered business address for the attention of the relevant party notified for such purpose, or to such other address as that party may notify in the future to the other party.

24. COMPLIANCE WITH RELEVANT REQUIREMENTS AND MODERN SLAVERY ACT 2015

- (a) Bribery Act 2010 - WRG shall:
 - (i) comply with all applicable laws, statutes, regulations, and codes relating to anti-bribery and anti-corruption including but not limited to the Bribery Act 2010 ("Relevant Requirements");
 - (ii) not engage in any activity, practice or conduct which would constitute an offence under sections 1, 2 or 6 of the Bribery Act 2010 if such activity, practice or conduct had been carried out in the UK;
 - (iii) comply with The Customer's Ethics, Anti-bribery and Anti-corruption Policies as amended from time to time ("Relevant Policies").
 - (iv) have and shall maintain in place throughout the term of this agreement its own policies and procedures, including but not limited to adequate procedures under the Bribery Act 2010, to ensure compliance with the Relevant Requirements and the Relevant Policies, and will enforce them where appropriate;
 - (v) promptly report to The Customer any request or demand for any undue financial or other advantage of any kind received by WRG in connection with the performance of this agreement;
 - (vi) where requested by The Customer within three months of the date of this agreement, and annually thereafter, certify to The Customer in writing signed by an officer of WRG, compliance with this clause 24 by WRG and WRG shall provide such supporting evidence of compliance as The Customer may reasonably request.
- (b) WRG shall ensure that any person associated with WRG who is performing services or providing goods in connection with this agreement does so only on the basis of a written contract which imposes on and secures from such person terms equivalent to those imposed on WRG in this clause 24 ("Relevant Terms"). WRG shall be responsible for the observance and performance by such persons of the Relevant Terms, and shall be directly liable to The Customer for any breach by such persons of any of the Relevant Terms.
- (c) For the purpose of this clause 24, the meaning of adequate procedures and whether a person is associated with another person shall be determined in accordance with section 7(2) of the Bribery Act 2010 (and any guidance issued under section 9 of that Act), sections 6(5) and 6(6) of that Act and section 8 of that Act respectively. For the purposes of this clause 24 a person associated with WRG includes but is not limited to any subcontractor of WRG.
- (d) Modern Slavery Act 2015 - WRG shall:
 - (i) comply with all applicable laws, statutes, regulations and codes from time to time in force including but not limited to the Modern Slavery Act 2015
 - (ii) implement due diligence procedures for its own suppliers, subcontractors and other participants in its supply chains, to ensure that there is no slavery or human trafficking in its supply chains.
 - (iii) notify the Customer as soon as it becomes aware of:

- (A) any breach, or potential breach, of the Anti-slavery Policy; or
- (B) any actual or suspected slavery or human trafficking in a supply chain which has a connection with this agreement.

Breach of this clause 24 shall be deemed a material breach of the Contract including but not limited to for the purposes of clause 14 b. (i).

25. GOVERNING LAW AND JURISDICTION

This Agreement shall be governed by and construed in accordance with English law. Each party agrees to submit to the exclusive jurisdiction of the English courts.

For and on behalf of WR Group Limited:

For and on behalf of [Customer]:

Signed by _____

Signed by _____

Date _____

Date _____

Name _____

Name _____

Title _____

Title _____

Schedule 1 – Scope of Services

WR Group (“Webrecruit”) will provide the Customer with our proprietary recruitment ATS (Applicant Tracking System), Webrecruit ATS, within the Scope of this Agreement. Services will be provided in order to support the Customer’s recruitment activity in the UK.

Recruitment ATS – Webrecruit ATS – a fully-licensed Applicant Tracking System with an unlimited number of HR users and hiring managers provided and supported for the Term, consisting of:

- a. Applicant tracking and management
- b. Job creation and requisition
- c. Branding options
- d. Customisable email templates
- e. Reporting and equal opportunities/diversity monitoring
- f. Talent pool search tools
- g. Job board / aggregator posting (to Trovit, Jooble, Webrecruit Jobs)
- h. Agency management
- i. Interview management
- j. Referral management
- k. Onboarding management
- l. Task and calendar management
- m. Data retention management

The System and associated services will comply with and be supplied in accordance with the provisions of Schedule 3.

The System will at all times have sufficient functionality to enable the Customer to manage the end-to-end recruitment process through each of the following stages: advertising a job, receiving applications, interviewing candidates, rejecting unsuccessful candidates, progress successful candidates to offer stage. The functionality will also be sufficient to provide the Customer with management information to monitor advertising effectiveness and analyse activity volumes.

The System will be available to the Customer 24 hours a day, 365 days per annum (366 days per annum in a leap year) (the **"Availability Period"**) on a hosted basis (SaaS) for the purposes of facilitating the recruitment by the Customer of staff to work for the Customer.

Provision of technical and user support via telephone and the internet (e-mail and web) between the hours of 09:00 (UK time) and 17:30 on a Working Day (According to the table below in Schedule 3). WR Group shall promptly respond to all requests from the Customer for support and shall give priority to those requests concerning the operation/availability of the System. Resolution times in Schedule 3 cannot be guaranteed, however WR Group will use all reasonable endeavours to resolve issues within the target times defined.

In relation to any integrations with third-party products or software, WR Group will provide support in line with Schedule 3 where the issue is related to a technical fault with the System. Where it has been determined that resolution of a support issue is reliant on a third-party product or service provider with whom the Customer has a direct relationship, support of resolving that issue will not be governed by the scope of this agreement. However, in this circumstance WR Group will use all reasonable endeavors to assist in reaching a resolution.

The Webrecruit ATS CV anonymisation feature is built using advanced CV parsing technology to automate the creation of an anonymised CV. The automation is developed to build a structured version of a CV with the following data removed: name, email address, phone number, date of birth, age, gender and ethnicity. The structure and format of the original CV can impact how it is parsed and therefore WR Group cannot guarantee that every CV will have the correct data removed or retained.

WR Group cannot guarantee the length or type of coverage provided by job board aggregators or any free job boards integrated with Webrecruit ATS.

Software upgrades will be made to Webrecruit ATS as reasonably determined by WR Group in order to, improve functionality, address software defects, or other cases deemed necessary by WR Group. WR Group will use all reasonable efforts to schedule upgrades for times when they will cause the least disruption to the Customer.

Notes:

For the avoidance of doubt, the Customer;

- will have ownership over all candidate and vacancy data in their recruitment system and, at the point where they cease to use the system, will have the option to export and retain all candidate data (subject to complying with current data protection legislation)

Training

WR Group is able to provide two online training sessions (maximum 4 hours per session) free of charge with different sets of hiring managers. Additional training sessions can be arranged at a cost of £500 per day for onsite training (plus travel expenses) or online (maximum 4 hours per session) at a cost of £250 per session.

Implementation

WR Group will provide such implementation services as are necessary to facilitate the above services going live in accordance with the project plan to be agreed between the parties.

Schedule 2 – Fees

Fee Type	Amount (excl. VAT)	Job Boards / Service Description	Invoice Timing
----------	-----------------------	----------------------------------	----------------

Webrecruit ATS [Term Length] PRICE Licence		- Unlimited HR and Hiring Manager System Users - Branded Application Process - Fully Mobile Responsive System - Careers Site Integration - Customisable Email Templates - Application Tracking and Management System - Job Board / Aggregator Posting (to Adzuna, Trovit and WebrecruitJobs) - Interview Scheduling module - Reporting Module - Recruitment Agency Management module - Onboarding module - Ongoing system support and development	Payment Terms
---	--	--	----------------------

Schedule 3 – Webrecruit ATS

WR Group will ensure that the system availability level maintains at 99.9% during normal business hours (08:30 to 17:30 UK time) and 99.5% out of business hours, excluding scheduled maintenance. WR Group cannot be held in any way responsible for any access problems due to problems experienced by the Customer's Internet connection.

WR Group will:

- actively monitor at the server and platform level.
- leverage Zabbix to monitor and alert support staff of any conditions which pass specific server thresholds in respect of matters such as processing, memory, drive space, etc. This allows WR Group to respond to typical events that may arise through various usage conditions before they cause any adverse conditions.
- use Statuscake for platform monitoring; it sends external requests to the platform every 30 seconds to make sure it is responding. The request tests https response, DB response and Solr response which are the main components of the platform. We use this to track our platform uptime.

In the event that the system availability falls below the levels set out above in any given calendar month WR Group will pay to the Customer service credits calculated as follows:

If the System is available for less than:

- 99.9% of the time during normal business hours (being 08.30 to 17.30 each Working Day) in any Quarter; or
- 99.5% of the remaining Availability Period (but excluding any scheduled maintenance to the System notified to the Customer in advance) in any Quarter.

WR Group shall promptly pay the Customer a service credit of 10% of the equivalent monthly Webrecruit ATS Licence Fee for each Month that the above clause applies to ('service credit').

Where maintenance to the system is required, WR Group will use its reasonable efforts to ensure this maintenance is always scheduled to minimise disruption to Customer usage. Scheduled maintenance will take place outside a Working Day, during the hours of 09.00 to 17.30 (UK time).

WR Group shall use all reasonable efforts to maintain a server response time of 2 seconds or better.

LEVELS OF SUPPORT:

Category	Definition	Issue Resolution	Response Time	Resolution time
Critical	Prevents users from using crucial functionality of the Service	WR Group will immediately commence investigations and will work until the problem has been solved or an acceptable workaround devised. In the event of a software patch being required, this will be applied to a test environment first and as soon as possible after testing, will be installed into the production environment. WR Group will use all reasonable endeavours to resolve the problem such that the system is operating with all core functionality within 4 hours of the problem being reported.	Within 2 business hours by email or phone call.	Within 4 business hours
High	Prevents users from using the functionality of the Service. There is no workaround available, however the functionality is not considered crucial.	WR Group will commence investigations within 4 hours. In the event of a software patch being required, this will be applied to a test environment first and as soon as possible after testing, will be installed into the production environment. WR Group will use all reasonable endeavours to resolve the problem such that the system is operating with all core functionality within 8 business hours of the problem being reported.	Within 4 business hours by email or phone call.	Within 8 business hours
Medium	Prevents users from using the functionality of the Service. However there is a workaround available.	WR Group will respond to reports within 8 hours and use all reasonable efforts to resolve the problem within such timescale as the parties shall agree. Minor errors which do not materially affect functionality may be resolved this error in the regular software upgrade program. Within this program minor errors and enhancements will be patched in new releases.	Within 8 business hours by email or phone call.	Within next software upgrade release (On average, these are every 3 weeks).
Low	Prevents users from implementing a particular functionality outside of normal system usage. This may be an enhancement request.	WR Group and the Customer will agree whether the enhancement will be part of a new release or will be considered Consultancy. The Customer will benefit from new releases at no extra cost. Functionality which requires Consultancy will incur cost to the Customer and will be agreed in writing.	N/A	N/A

Incident Reporting

Both the Customer's staff and applicants are entitled to contact WR Group for support to any software related issues. It is extremely rare that applicants will contact us directly with any technical issues. Because the software and application process would all be Customer branded, it's more likely that applicants would contact you with any issues they encounter which in turn you would report to us. We'll maintain a record of any issues that get directly reported to us from applicants.

Initial issues should be reported to the Supplier's Software Support team (via support@webrecruit.co.uk). Any difficulties can then be escalated to the Supplier's Operations Director (Jasper Kashap) or Managing Director (David Jones). If required, the customer may change the category of a support call.

Hosting Partner

The server environment is provided by OVH (<https://ovh.co.uk>) and is fully managed by them with comprehensive monitoring tools.

OVH is a global hosting company with over 1.5 million customers. OVH provide innovative products and services, their own global network, continuous R&D and experts that are passionate about customer service. OVH has 30 data centres commissioned with a hosting capacity of over 1 million servers. OVH has been designing, managing and maintaining its own data centres since 2003.

Servers are physically located in OVH's Roubaix and London datacentres. At Roubaix and London, all access to the OVH premises is strictly monitored. To prevent any intrusions or hazards, every boundary is secured using barbed-wire fencing. Video surveillance and movement detection systems are also in continuous operation. Activity within the data centres and outside the buildings is monitored and recorded on secure servers, while the surveillance team are on site 24/7/365.

In order to control and monitor access to the OVH premises, strict security procedures have been put in place. Every member of staff receives a RFID name badge which is also used to restrict their access. Employee access rights are reassessed regularly, according to their remit. To access the premises, employees must hand in their badges for verification, before passing through the security doors.

The data centres buildings have an even higher level of protection, as only authorized personnel can gain entry. OVH installations are strictly for their own use. Every datacentre room is fitted with a fire detection and extinction system, as well as fire doors.

Access to production servers and data, via remote access, is granted to a restricted number of Webrecruit personnel that are required to maintain the service. This includes DevOps engineers who apply platform updates and infrastructure engineers who maintain servers and apply patches.

Please note that WR Group will have the right to change server provider at any time and the customer will be made aware of any such change provided that any change of provider shall be undertaken so as to minimise any disruption to the service and that the functionality, performance and security of the system and associated data shall not be in any way reduced

Platform

Database

Webrecruit ATS runs on a Microsoft SQL server 2022 database. The database runs on a dedicated set of servers that are physically within the same rack as all other servers which it serves.

Isolating and safeguarding data from other clients

Data from multiple clients are stored in the same datastore. Multi-tenancy is typical of most cloud-based services. WR Group uses several methods to ensure separation of data between clients. All relevant queries to the database require the validation of the client and/or user identifier to ensure that only data for that specific client is returned. Strong authentication and authorization methods are also used to prevent a user from accessing data from another client. All features undergo specific testing scenarios against multiple clients to confirm no data leakage has been introduced.

Enforcing data destruction policies and evidencing that data is no longer stored

In the event of termination of this Agreement, WR Group will upon request initiate a process whereby it will manually delete all your client data from the database. You can evidence this by working through the site and running any reporting or active dashboards to confirm everything is deleted.

Resilience

Network

To guarantee high speed, high quality bandwidth and low latency time, OVH has deployed its own global fibre-optic network. The network is managed using DWDM devices and is currently being migrated to 100G coherent technology, offering you to a total capacity of 7.5 Tbps to the worldwide web.

Data

Should a total utility power outage ever occur, all of OVH's data centre's power systems are designed to run uninterrupted, with every server receiving conditioned UPS (Uninterruptible Power Supply) power.

The OVH datacentres are powered by two separate electrical power supplies and are also equipped with UPS devices. Power generators have an initial autonomy of 48hrs to counteract any failure of the electricity supply network.

OVH data centres are accredited to PCI DSS, ISO27001, and ISAE 3402 Type II standards, ensuring sites and applications are secured by the best processes and technologies.

Backup arrangements

WR Group uses a high availability architecture to provide a resilient service. At our primary datacenter, the virtual machines are run on several physical host servers with an automatic failover should a single physical host require maintenance or replacement.

WR Group also uses the Zerto Disaster Recovery technology to provide a continuous backup and recovery solution to a secondary datacenter at a separate geographic location. This provides the necessary protection should our primary datacenter encounter a total failure.

The data on our production servers is backed up regularly. Our production SQL database performs transaction log backups at 15-minute intervals with full and intermediate backups being performed daily. Backup sets are retained for 28 days, and we can recover to any point in a 15-minute interval within that period.

A snapshot of each production virtual machine image is taken nightly and retained for 7 days. Critical security patches and updates are applied to all our infrastructure when necessary. These are applied initially to test environments to ensure no services will be affected, before being deployed to production.

The performance of all our infrastructure, applications and databases are monitored by a dedicated monitoring system that tracks key metrics in real-time and gives immediate feedback on any potential issues.

Any local corruption at the server or data level can be restored within approx. 1 hour. A full recovery at the secondary data centre would take 4 hours.

Security

Cloud Threat Protection

Though business, application, and infrastructure needs can vary widely across industries and workloads, OVH works to provide common tools and expertise that can effectively mitigate the risk of cyber security breaches to their hosted systems.

WR Group will maintain very strict restrictions at the front end of its network which keep all internal networks safe. Apart from only opening https inbound ports, WR Group provides key based VPN access to authorised employees which are renewed on a regular basis. This provides protection from intruders who are randomly scanning ports or who are targeting other vulnerable services that are listening on standard ports. Internally, WR Group manages all server policies and authentication through its domain controller. We have increased password complexity requirements and carefully manage who has access to specific servers. At a production level, only the DevOps responsible for releases and the infrastructure team have access. For various test and staging environments, WR Group may extend this access to developers and QA resources on a need to access basis.

Underneath the VMWare layer, WR Group will at all times maintain fully redundant servers powering the system with automatic failover on any physical hardware failure with capability to cope with failover of all servers to two of our three nodes at any point in time. Further, at a physical storage level, all storage is configured in RAID10. This entire physical infrastructure is managed by OVH and has a guaranteed availability SLA of 99.99%. Any maintenance that is done can be applied with no interruptions of service as we are able to shift running servers across the physical hardware.

WR Group will work with OVH to continually improve our physical hosting infrastructure along with our connectivity to the outside networks.

Data Encryption

WR Group will at all times protect user passwords in the database to prevent access to user accounts in the case of a data breach. All passwords are hashed and salted and no one within Webrecruit can access or know specific user passwords.

WR Group utilises the Transparent Data Encryption feature of SQL Server. The level of encryption used is AES-256. This prevents any unauthorised access to data should the physical media the data is stored on ever be compromised.

Data in Transit

WR Group ensures data is protected in transit through a combination of techniques. Primarily, all traffic uses encrypted connections at a minimum of TLS 1.2 and where available, TLS 1.3. Insecure cipher suites have been disabled in accordance with industry-standard best practices. In addition, HSTS is enabled to force HTTPS connections and prevent man-in-the-middle attacks.

On a network level, the WR Group infrastructure is protected by a dedicated firewall and all servers are located on an isolated internal network with no direct access to the wider Internet. This allows WR Group to monitor and control incoming and outgoing network traffic to protect against unauthorised access.

Access to the WR Group infrastructure is restricted to key staff only and is protected by a certificate-based VPN to ensure that impersonation of authorised users cannot be done. In addition, an IP address whitelist is also used to prevent access by unauthorised users to the infrastructure administration interface.

All these techniques ensure that user data is protected against tampering and eavesdropping and remains secure and encrypted between the server and the end-user.

Denial of Service Attacks

To protect our servers and services from attacks, OVH offers a mitigation solution based on VAC technology - an exclusive combination of techniques to:

- Analyse all packets at high speed in real time
- Vacuum your server's incoming traffic
- Mitigate i.e. singling out all the illegitimate IP packets, while allowing legitimate ones to pass through

Vulnerability Assessment

Vulnerability scans are considered an essential tool in our efforts for a secured computing environment. A scan produces a prioritised list of discovered vulnerabilities. Typically, this process is done by interacting with the active hosts and checking for specific vulnerabilities against active services and ports. The prioritised list serves then as a guide for decision making, and typically leads to certain configuration and actions to address each vulnerability. WR Group also conduct vulnerability scans on the web application on a monthly basis. Penetration testing is undertaken by a CREST-certified, independent third-party firm on an annual basis.

DATA PROCESSING AGREEMENT

BETWEEN

[CUSTOMER]

Company Registration Number: xxxxxxxx

[of ADDRESS]

and

WR Group Limited (t/a "Webrecruit")

Company Registration Number: 04838590

of Queensgate House, 48 Queen Street, Exeter, Devon, EX4 3SR

This Data Processing Agreement (the **"DPA"**), entered into by the Webrecruit customer (**"Customer"**) identified on the applicable Webrecruit ATS Agreement (**"Agreement"**) governs the processing of personal data that the Customer has submitted to Webrecruit or uploads. For the purpose of this agreement, Webrecruit is the **"Data Processor"** and the Customer is the **"Data Controller"**. The categories of **"Data Subjects"** governed by the agreement are individuals who have expressed interest in or potentially may be considered for employment with the Customer.

This DPA is incorporated into the relevant Webrecruit services agreement, referred to generically in this DPA as the **"Webrecruit Contract"**.

1. DEFINITIONS

"Customer Personal Data" means Personal Data (i) that the Customer uploads or otherwise provides Webrecruit with or (ii) is submitted to the Customer as part of a job application. This data includes names, e-mail addresses, responses to job application questions and CVs (inclusive of any personal information held within such as address, date of birth, work history and education), interview history, employment references, salary details, social media details and background information such as passport numbers, driving licence numbers and visa status.

"Data Controller" means the entity which alone or jointly with others, determines the purposes and means of processing Personal Data.

"Data Processor" means an entity which processes Personal Data on behalf of the Controller.

"Data Protection Laws" means legal requirements comprising the General Data Protection Regulation, Local Data Protection Laws, any subordinate legislation and regulation implementing the General Data Protection Regulation, and all Privacy Laws including legal requirements relating to (a) privacy, data security, consumer protection, marketing, promotion, and text messaging, email, and other communications; and (b) the use, collection, retention, storage, security, disclosure, transfer, disposal, and other processing of any Personal Data.

"Personal Data" means information about an individual that (a) can be used to identify, contact or locate a specific individual; (b) can be combined with other information that can be used to identify, contact or locate a specific individual; or (c) is defined as "personal data" or "personal information" by applicable laws or regulations relating to the collection, use, storage or disclosure of information about an identifiable individual.

"Personal Data Breach" means any accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Personal Data.

"Process" and its cognates mean any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

"Subprocessor" means any entity which provides processing services to Webrecruit in furtherance of Webrecruit's processing on behalf of Customer.

"Supervisory Authority" means an independent public authority which is established to promote and enforce legislation pursuant to Article 51 of the UK GDPR.

2. NATURE OF DATA PROCESSING

Each party agrees to process Personal Data received under the Agreement only for the purposes set forth in the Agreement.

3. COMPLIANCE WITH LAWS

The parties shall each comply with their respective obligations under all applicable Data Protection Laws.

4. CUSTOMER OBLIGATIONS

Customer agrees to comply with its protection, security and other obligations with respect to Customer Personal Data prescribed by Data Protection Laws for data controllers by: (a) establishing and maintaining a procedure for the exercise of the rights of the individuals whose Customer Personal Data are processed on behalf of Customer; (b) processing only data that has been lawfully and validly collected and ensuring that such data will be relevant and proportionate to the respective uses; and (c) ensuring compliance with the provisions of this Agreement by its personnel or by any third-party accessing or using Customer Personal Data on its behalf.

5. WEBRECRUIT OBLIGATIONS

5.1 Processing Requirements. Webrecruit will:

- a. Process Customer Personal Data (i) for the purpose of providing additional recruitment services with which the Customer has contractually engaged Webrecruit; and (ii) in compliance with the instructions received from Customer. Webrecruit will not use or process the Customer Personal Data for any other purpose;
- b. Inform Customer promptly if, in Webrecruit's opinion, an instruction from Customer violates applicable Data Protection Laws;
- c. If Webrecruit is collecting Customer Personal Data from individuals on behalf of Customer, follow Customer's instructions regarding such Customer Personal Data collection (including with regard to the provision of notice and exercise of choice);
- d. Take commercially reasonable steps to ensure that (i) persons employed by it and (ii) other persons engaged to perform on Webrecruit's behalf comply with the terms of the Agreement;
- e. Ensure that its employees, authorized agents and any Subprocessors are required to comply with and acknowledge and respect the confidentiality of the Customer Personal Data, including after the end of their respective employment, contract or assignment;
- f. Obtain consent from the Customer if it intends to engage Subprocessors to help it satisfy its obligations in accordance with this DPA or to delegate all or part of the processing activities to such Subprocessors. Webrecruit will (i) remain liable to the Customer for the Subprocessors' acts and omissions with regard to data protection and (ii) enter into contractual arrangements with such Subprocessors binding them to provide the same level of data protection and information security to that provided for herein;
- g. Upon request, provide Customer with a summary of Webrecruit's privacy and security policies.

5.2 Notice to Customer. Webrecruit will inform Customer if Webrecruit becomes aware of:

- a. Any non-compliance by Webrecruit or its employees within this DPA or the Data Protection Laws relating to the protection of Customer Personal Data processed under this DPA;
- b. Any legally binding request for disclosure of Customer Personal Data by a law enforcement authority, unless Webrecruit is otherwise forbidden by law to inform Customer, for example to preserve the confidentiality of an investigation by law enforcement authorities;
- c. Any notice, inquiry or investigation by a Supervisory Authority with respect to Customer Personal Data; or
- d. Any complaint or request (in particular, requests for access to, rectification or blocking of Customer Personal Data) received directly from data subjects of Customer.

5.3 Assistance to Customer. Webrecruit will provide reasonable assistance to Customer regarding:

- a. Any requests from Customer data subjects in respect of access to or the rectification, erasure, restriction, portability, blocking or deletion of Customer Personal Data that Webrecruit processes for Customer;
- b. The investigation of Personal Data Breaches and the notification to the Supervisory Authority and Customer's data subjects regarding such Personal Data Breaches;
- c. Where appropriate, the preparation of data protection impact assessments and, where necessary, carrying out consultations with any Supervisory Authority.

5.4 Required Processing. If Webrecruit is required by Data Protection Laws to process any Customer Personal Data for a reason other than providing the services described in the Agreement, Webrecruit will inform Customer of this

requirement in advance of any processing, unless Webrecruit is legally prohibited from informing Customer of such processing (e.g., as a result of secrecy requirements that may exist under UK GDPR and the Data Protection Act 2018).

5.5 Security. Webrecruit will:

- a. Maintain appropriate organizational and technical security measures (including with respect to personnel, facilities, hardware and software, storage and networks, access controls, monitoring and logging, vulnerability and breach detection, incident response, encryption of Customer Personal Data while in transit and at rest) to protect against unauthorized or accidental access, loss, alteration, disclosure or destruction of Customer Personal Data;
- b. Be responsible for the sufficiency of the security, privacy, and confidentiality safeguards of all Webrecruit personnel with respect to Customer Personal Data and liable for any failure by such Webrecruit personnel to meet the terms of this DPA;
- c. Take reasonable steps to confirm that all Webrecruit personnel are protecting the security, privacy and confidentiality of Customer Personal Data consistent with the requirements of this DPA; and
- d. Notify Customer of any Personal Data Breach by Webrecruit, its Subprocessors, or any other third-parties acting on Webrecruit's behalf without undue delay and in any event without any undue delay of becoming aware of a Personal Data Breach.

6. DATA RETURN AND DELETION

The parties agree that on the termination of the data processing services or upon Customer's reasonable request, Webrecruit shall, and shall cause any Subprocessors to, at the choice of Customer, return all the Customer Personal Data and copies of such data to Customer or securely destroy them and demonstrate to the satisfaction of Customer that it has taken such measures, unless Data Protection Laws prevent Webrecruit from returning or destroying all or part of the Customer Personal Data disclosed. In such case, Webrecruit agrees to preserve the confidentiality of the Customer Personal Data retained by it and that it will only actively process such Customer Personal Data after such date in order to comply with applicable laws.

7. THIRD PARTY DATA PROCESSORS

Customer acknowledges that in the provision of some services (such as integration with a third-party CRM), Webrecruit, on receipt of instructions from Customer, may transfer Customer Personal Data to and otherwise interact with third party data processors. The Customer agrees that if and to the extent such transfers occur, the Customer is responsible for entering into separate contractual arrangements with such third party data processors binding them to comply with obligations in accordance with Data Protection Laws. For avoidance of doubt, such third-party data processors are not Subprocessors.

8. TERM

This DPA shall remain in effect as long as Webrecruit carries out Personal Data processing operations on behalf of Customer.

9. LIABILITY

9.1 The Data Processor is liable for and shall indemnify and keep the Customer fully indemnified on demand from and against each and every action, proceeding, liability, loss, damage, cost, claim, fine, expense and/or demand suffered or incurred by the Customer which arise from or in connection with or pursuant to any act or omission of or the performance of the Data Processor's obligations under this Agreement, including without limitation those arising out of third party demand, claim or action, or any breach of contract, negligence, fraud, wilful misconduct, breach of statutory duty or non-compliance with this Agreement or any part of the Data Protection Legislation by the Data Processor or any claim that is referred to in Clause 9.2 and Clause 9.3.

9.2 The Data Processor acknowledges and agrees with the Customer that Data Subjects who suffer loss, costs or damage (the "Damages") as a result or a consequence of the acts and/or omissions of or a breach of the provisions of this Agreement or any part of the Data Protection Legislation by or on behalf of the Data Processor shall be entitled to receive compensation from the Data Processor for such Damages.

9.3 The Data Processor acknowledges and agrees with the Customer that it shall be liable (to the exclusion of the Customer, as between the Customer and the Data Processor) for any such Damages that may be due to or awarded to any such Data Subject by any court, authority or person of competent jurisdiction and that the indemnity set out in Clause 9.1 shall apply in respect of any such Damages.

9.4 Subject to clause 9.5, the Customer's total liability under this Agreement shall in no circumstances exceed three times the annual licence fees paid to WRG under the Main ATS Contract Agreement (issued separately) at the time such loss is suffered (see separate Schedule for agreed licence fees).

- 9.5 Nothing in this Agreement will exclude, limit or restrict either party's liability for:
- 9.5.1 death or personal injury resulting from the negligence of that party (or its officers, agents or employees);
- 9.5.2 fraud or fraudulent misrepresentation committed by that party (or its officers, agents or employees); or any other matter in respect of which liability cannot by applicable law be limited.
- 9.6 Nothing in this clause 9 shall restrict or limit a party's general obligation at law to mitigate a loss it may suffer or incur as a result of an event that may give rise to a claim under the indemnity in clause 9.1.
- 9.7 Except as expressly and specifically provided in this Agreement:
- 9.7.1 The Customer assumes sole responsibility for results obtained from the use of the Services, and for conclusions drawn from such use. WRG shall have no liability for any damage caused by errors or omissions in any information, instructions or scripts provided to the Customer by any Candidate in connection with the Services; and
- 9.7.2 all and any interaction and communication between the Customer and any Candidate in connection with the Candidate's response to a recruitment campaign are the responsibility of the Customer, and WRG accepts no liability whatsoever therewith.

10. GOVERNING LAW AND JURISDICTION

10.1 This Agreement and any dispute arising out of or in connection with it or its subject matter or formation (including non-contractual disputes or claims) shall be governed by and construed in accordance with the law of England and Wales.

10.2 The parties to this Agreement irrevocably agree, subject as provided below, the courts of England and Wales shall have exclusive jurisdiction over any dispute or claim arising out of or in connection with this Agreement or its subject matter or formation (including non-contractual claims). Nothing in this clause shall limit the right of the Customer to take proceedings against the Data Processor in any other court of competent jurisdiction, nor shall the taking of proceedings in any one or more jurisdictions preclude the taking of proceedings in any other jurisdictions, whether concurrently or not, to the extent permitted by the law of such other jurisdiction.

11. AGREEMENT FORM

For and on behalf of the Data Processor (Webrecruit):

For and on behalf of Data Controller [Customer]:

Signed by _____

Signed by _____

Date _____

Date _____

Name _____

Name _____

Title _____

Title _____