MASTER SERVICES AGREEMENT

This master services agreement ("**Agreement**") governs the Services purchased under the applicable Order and/or SOW between Supplier and Customer (each a "**party**" and collectively the "**parties**").

AGREED TERMS

1. DEFINITIONS

1.1 **Affiliate(s)** means any third party that controls, is controlled by, or is under common control with the applicable party. As used herein, "control" means the possession, direct or indirect, of the power to direct or cause the direction of the management and policies of said party, whether through ownership of voting securities, by contract or otherwise.

1.2 **AI** means a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments.

1.3 **AI Services** means the features and functionality within the Subscription Services powered by AI.

1.4 **Applicable Law(s)** means worldwide laws and regulations in force from time to time that are applicable to each party in its performance of its obligations under the Agreement.

1.5 **Authorized User(s)** means the nominated personnel of Customer, its Affiliates or its partners who are issued with a unique live login to the Subscription Services.

1.6 **Beta Service(s)** means a version or feature of the Services that Supplier has not made generally available for production use, is in its early development, or is otherwise identified as such by Supplier, including but not limited to Beamery Labs.

1.7 **Confidential Information** means any information (regardless of its form), which is designated by a party, its Affiliates or Sub-Processors, as being confidential (whether or not it is marked) or which can reasonably be expected to be confidential, that the other party obtains in connection with this Agreement, including but not limited to: Customer Data; Documentation; pricing; the terms and conditions of this Agreement; technical information or know-how; recordings of the Services; trade or business secrets; and commercial information.

1.8 **Contact** means a single candidate, prospect, lead, or other individual (other than an Authorized User) whose information and Personal Data is submitted to the Subscription Services.

1.9 **Customer** means the customer entity (as identified in the Order) purchasing the Services.

1.10 **Customer Data** means the data provided by Customer for the purpose of Customer's use of the Services including Contact information, text, graphics, information, documentation, content, notes, images, data, and other materials.

1.11 **Data Protection Law(s)** means worldwide data protection and privacy laws and regulations in force from time to time, and the guidance and codes of practice issued by the relevant data protection or supervisory authority, that are applicable to a party in its use or provision of the Services and Personal Data, including, where applicable and in each case as may be amended or superseded from time to time Regulation (EU) 2016/679 (General Data Protection Regulation "GDPR"), UK GDPR and US equivalents.

1.12 **Documentation** means the applicable Order, SOW, and training materials provided to Customer by Supplier.

1.13 **DPA** means the Data Processing Agreement in Exhibit 1.

1.14 **Fees** mean the fees payable by Customer to Supplier agreed between the parties in applicable Order or SOW.

1.15 **Force Majeure** means any cause preventing a party from performing any or all of its obligations which arises from or is attributable to acts, events, omissions or accidents beyond the reasonable control of the party so prevented including, without limitation, act of God, war, riot, computer viruses and malware, epidemics, pandemics, compliance with any law or governmental order, rule, regulation or direction, flood or storm, except for strike or lockout of the party's own staff shall not entitle them to claim that to be a force majeure event.

1.16 **Intellectual Property Rights** means all tangible and intangible rights associated with works of authorship throughout the world, including, but not limited to, copyrights, moral rights, and mask works; trademarks and trade name rights and similar rights; trade secret rights; patents, designs, algorithms, and other intellectual or industrial property rights (of every kind and nature) whether registered, registerable or otherwise arising by operation of law, contract, license, or otherwise; and all registrations, initial applications, renewals, extensions, continuations, divisions, or reissues now or hereafter in force (including any rights in the foregoing).

1.17 **Order** means an order form document entered into between Supplier and Customer or their Affiliates for Supplier's Services.

1.18 **Professional Services** means implementation, integration, consulting, advising, and/or training services set out in an Order or SOW.

1.19 **Restricted Information** means payment card information; financial information (or similar data regulated by GLBA or equivalent legislation); social security numbers; passport numbers; driving license numbers; insurance information; physical or mental health information or medical conditions (or similar data regulated by HIPAA or equivalent legislation); political opinions; religious or philosophical beliefs; trade union membership; genetic data; biometric data; sex life; criminal information and/or background checks; or information of children. Restricted Information does not include voluntarily-given self-identification data such as gender, sexual orientation, racial or ethnic data.

1.20 **Security Policies** means Supplier's documentation with regards to information security and data privacy at https://trust.beamery.com/ as amended from time to time. Supplier shall not materially diminish the technical and organizational measures set out in its Security Policies.

1.21 **Services** means, collectively (as applicable), the Subscription Services and Professional Services.

1.22 **SLA** means the "service level agreement (SLA)" at https://beamery.com/terms-and-conditions, as amended from time to time. Supplier shall not materially diminish the service levels set out in the SLA.

1.23 **Statement of Work/SOW** means an order for Professional Services entered into by Supplier and Customer or their Affiliates.

1.24 **Sub-Processor(s)** means Supplier's sub-processors set out under "Sub-Processors" at https://beamery.com/terms-and-conditions, as updated from time to time. Changes in the Sub-Processors shall be made in accordance with the DPA.

1.25 **Supplier** means the applicable Beamery entity identified in the Order.

1.26 **Subscription Services** means Supplier's software as a service tools and platform, any ancillary products and services, including website hosting and support services, that are set out in the applicable Order.

1.27 **Third Party Services** means any applications, products, applicant tracking systems, links, and services not provided by Supplier that are used by Customer in conjunction (for example, via integration) with the Services. For clarity, Third Party Services do not include any services provided by Supplier's Sub-Processors.

1.28 **Updates** means adding to, removing, or replacing existing features, functionality, integrations, or models from time to time that (in Supplier's reasonable determination) are redundant, have been merged with other functionality/features, or have been superseded.

2. SUPPLY OF SERVICES

2.1 **Subscription Services**. Supplier shall provide Customer with access to the Subscription Services for the term set out in the applicable Order. Supplier may make Updates to the Services from time to time.

2.2 **Support and Service Levels.** Supplier shall provide support for the Subscription Services in accordance with the SLA.

2.3 **Professional Services.** Supplier will provide implementation, integration and training services relevant to Supplier's product and will not be doing any custom software development for Customer. Any request to change the scope of the Professional Services shall be set out in a change order signed between the parties. Supplier shall not be responsible for any delay in providing the Professional Services that is caused (in whole or in part) by an act or omission of Customer, its Affiliates, Authorized Users, or third parties.

2.4 **Beta Services**. Supplier may offer Customer the option to use Beta Services from time to time. Beta Services: (a) are provided AS IS with no warranty, indemnity, or liability; (b) are not subject to the SLA; and (c) may be subject to additional terms (as provided by Supplier). Supplier may modify or discontinue the provision of the Beta Services to Customer at any time in Supplier's sole discretion and without any liability to Customer.

2.5 **Third Party Services.** Customer may elect to use the Services in conjunction with Third Party Services. Customer acknowledges that its use of such Third Party Services is subject to the applicable third party's terms and conditions and Supplier makes no representations or warranties in relation to such Third Party Services, including but not limited to their availability.

2.6 **AI Services**.

a) **Responsible AI.** Supplier implements and maintains policies, procedures, and technical and administrative measures to develop the AI Services in accordance with ethical and responsible AI guidelines, including by developing such AI Services in a manner that promotes human oversight, transparency, accountability, fairness, safety, and security. Supplier will commission an independent third party to conduct an annual bias audit (for race, ethnicity and sex/gender) on applicable AI Services. Upon request, Supplier will share the final bias audit report with Customer. Customer acknowledges that such audits are done for illustrative purposes using test data, so Supplier makes no warranty that the results are fit for any particular use by Customer.

b) **Customer's Use of AI.** Customer is responsible for its use of the AI Services, including but not limited to maintaining human oversight.

c) **Future Laws.** Customer acknowledges that the legal framework applicable to and the interpretation of competent courts and authorities regarding the use of AI technologies is evolving. If a change in law or the interpretation of a competent court or authority results in (i) Supplier not being able to offer the AI Services in whole or in part, or (ii) Customer not being able to use the AI Services in compliance with Applicable Laws, Supplier may, without liability to Customer, reduce the functionality and/or scope of the AI Services (e.g. cease providing the AI Services in a given country), or remove the AI Services altogether. The same applies where Supplier can no longer provide any part of the AI Services that are powered by AI licensed from a third party.

3. SUPPLIER WARRANTIES

3.1 **Performance Warranty.** Supplier warrants that it shall perform the: (a) Services in accordance with the Documentation; and (b) Professional Services with due care, skill and ability in accordance with recognized industry standard practices. If the Services do not conform to the performance warranty in this Section 3.1 Supplier will, at its expense, correct any such non-conformance, or provide Customer with an alternative means of accomplishing the performance. If Supplier cannot correct or substitute such non-conformance, either party may terminate the non-conforming Services and Supplier shall issue a pro-rata refund to the Customer for such non-conforming Services. Such correction, substitution, or termination with a pro-rata refund constitutes Customer's sole and exclusive remedy in connection with any non-conformance with this performance

warranty. Supplier shall not be liable for any non-conformance to the extent that such arises due to the use of the Services by or on behalf of Customer contrary to this Agreement, Documentation, Supplier's express instructions, or any modification of the Services by or on behalf of Customer.

3.2 **Legal Warranty.** Supplier warrants that it shall comply with all Applicable Laws in its performance of the Services.

3.3 **Viruses**. Supplier will use industry-standard measures to avoid introducing viruses into the Subscription Services.

3.4 **DISCLAIMER**. EXCEPT AS STATED IN THIS AGREEMENT, SUPPLIER MAKES NO WARRANTY WITH RESPECT TO THE SERVICES, AND DISCLAIMS ALL STATUTORY OR IMPLIED WARRANTIES, INCLUDING WITHOUT LIMITATION WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR CUSTOMERS' BUSINESS REQUIREMENTS. SUPPLIER DOES NOT WARRANT THAT THE SERVICES ARE ERROR-FREE, ACCURATE, UNINTERRUPTED, OR CONTINUOUS, OR THAT IT IS COMPATIBLE WITH CUSTOMER'S SYSTEMS (OTHER THAN AS SPECIFIED IN THE DOCUMENTATION). SUPPLIER SHALL HAVE NO LIABILITY FOR ANY LOSS, OR DAMAGE THAT IS CAUSED BY ERRORS OR OMISSIONS IN ANY INFORMATION, DATA, INSTRUCTIONS, OR SCRIPTS PROVIDED TO SUPPLIER BY CUSTOMER, OR ANY ACTIONS TAKEN BY SUPPLIER AT CUSTOMER'S DIRECTION.

4. CUSTOMER OBLIGATIONS

4.1 **Users and Limits**. Customer shall use the Subscription Services in accordance with the limits in the applicable Order and Supplier's "fair use policy" (available at https://beamery.com/terms-and-conditions/). Customer shall promptly notify Supplier if it becomes aware that it is over its limits or if any Authorized User's login details have been shared, compromised, or subject to unauthorized disclosure. If Authorized Users have shared login details with another person or Customer is otherwise over its limits, then without prejudice to Supplier's other rights, Customer shall pay to Supplier an amount equal to the Fees that would have been payable for the additional limits. Customer is responsible for the acts and omissions of its Authorized Users.

4.2 Prohibited and Unauthorized Use. Customer shall not:

(a) use the Service to collect, manage or process Restricted Information;
(b) use the Services to email purchased lists without proper consent from the recipient;
(c) attempt to gain unauthorized access to the Services;
(d) use the Services in a way that threatens the security, integrity, or availability of the Services, including but not limited to uploading content or files that contains viruses, malware, or malicious code and sending spam emails;
(e) directly or indirectly, reverse engineer, decompile, disassemble or otherwise attempt to discover or disclose to any third party the source code, object code, underlying structure, ideas, know-how or algorithms relevant to the Services;
(f) sell, resell, license, sublicense, or make available the Services or Documentation to any third party;
(g) use the Services as part of any automated decision-making process or without taking into account other factors beyond the Services' recommendations when making final decisions; and
(h) use the Services in a manner that facilitates or generates content that promotes discrimination, violence, or is otherwise harmful.

4.3 **Legal Warranty.** Customer shall use the Services in compliance with all Applicable Laws. Customer acknowledges that the Subscription Services inc functionality to enable Customer's compliance with certain laws (for example accessibility, data protection, hiring, and artificial intelligence) however Customer is responsible for using such functionality in compliance with Applicable Laws.

4.4 **Suspension for Unauthorized Use.** Supplier may suspend, in its reasonable discretion, any user's access to the Services, for breach of Sections 4.2 or 4.3. Supplier will notify Customer of such suspension as soon as practicably possible. Any suspension shall be as limited in scope and duration as reasonably possible.

5. FEES & PAYMENT

5.1 **Fees.** Fees are set out in the applicable Order or SOW. Fees for the Subscription Services will remain fixed for the term of the applicable Order. Unless otherwise stated, all Fees are non-refundable.

5.2 **Invoicing**. Unless otherwise set out in an Order or SOW, Supplier will invoice Customer for the Fees on or around the effective date of the applicable Order or SOW, and annually thereafter with respect to the Subscription Services. Customer shall pay all undisputed invoices (without deduction or set off) within thirty (30) days from the "Invoice Date" set out in Supplier's invoice. Supplier does not accept checks. Customer shall provide Supplier with all information required to correctly submit an invoice to Customer, including but not limited to the PO number and instructions for use of Customer's electronic invoicing system, within five days of the effective date of the applicable Order or SOW to billing@beamery.com.

5.3 **Non-Payment.** Supplier will not exercise its rights under this Section 5.3 if the Fees are under reasonable and good-faith dispute and Customer is cooperating diligently to resolve the dispute. If Supplier has not received payment by the due date, it shall promptly notify Customer ("**Non-Payment Notice**"). If such payment remains outstanding ten (10) days after the Non-Payment Notice, without prejudice to any of its other rights and remedies, Supplier may: (a) without liability to Customer, suspend all Services while the invoice(s) remain unpaid; and (b) charge Customer interest at the rate of one percent per month on any overdue sums from the due date until the date Supplier's receives payment by Customer (inclusive).

5.4 **Taxes.** All Fees are exclusive of any taxes, duties, or similar governmental assessments of any nature, including, for example, value-added, sales, use or withholding taxes, assessable by any jurisdiction (collectively, "**Taxes**"). Customer agrees to pay any Taxes applicable to the Services purchased by it during the Term. Customer shall have no liability for any Taxes based upon Supplier's (or its Affiliates') gross revenues or net income. Customer shall inform Supplier which state(s) it should charge sales tax in. If Customer is Tax exempt or pays Taxes directly, then prior to invoicing, Customer will provide Supplier with a copy of a current tax exemption certificate issued by the appropriate state taxing authority for the given jurisdiction. . Should

Customer be required by any regulation to make any deduction on account of tax, including but not limited to withholding tax, or otherwise on any sum payable under the Agreement, the Fees payable shall be increased by the amount of such tax to ensure that Supplier receives a sum equal to the amount to be paid under the applicable Order.

5.5 **Expenses**. Supplier's travel-related expenses will be reimbursed by Customer provided that such have been approved in writing (email sufficient) by Customer.

6. TERM & TERMINATION

6.1 **Term.** This Agreement shall govern all Orders and SOWs and shall continue until the earlier of expiry of all Orders and SOWs or termination in accordance with this Agreement ("**Term**")**.**

6.2 **Termination for Cause.** Without affecting any right or remedy available to it, a party may terminate this Agreement and the applicable Order or SOW, by giving written notice of such termination to the other party:

a) in the case of Supplier, if Customer fails to pay any invoice in accordance with this Agreement and remains in default for thirty (30) days after being notified in writing to make such payment;

b) if the other party commits a material breach of any term of this Agreement, Order, or SOW (as applicable to the breach) and fails to remedy that breach within a period of thirty (30) days after being notified in writing to do so; or

c) immediately upon the occurrence of the other party having a receiver, administrative receiver or an administrator appointed, passing a resolution for winding up or a court of competent jurisdiction making an order to that effect, becoming subject to an administration order, entering a voluntary arrangement with its creditors or any equivalent to the foregoing occurring under national or local law, except where for the purposes of a solvent and bona fide amalgamation or reorganization.

6.3 **Effect of Termination.** Upon termination or expiration of the Term:

a) all rights granted hereunder to use the Services shall terminate immediately;

b) Customer shall promptly pay any Fees, taxes, or other amounts due or outstanding for the remainder of the term set out in the applicable Order and/or SOW; and

c) in the case of termination by Customer for cause under Section 6.2(b) Supplier will issue a pro-rata refund to Customer of any Fees paid in advance for any Professional Services not performed under a SOW or any Subscription Services for the remainder of the term in the applicable Order, as applicable to the breach.

6.4 **Retrieval & Deletion of Customer Data.** Customer may export copies of Customer Data in NDJSON at any time during the Term. Unless otherwise agreed with Customer or legally prohibited, Supplier will, delete in accordance with industry standards, all Customer Data in its production environment within thirty (30) days of termination or expiration of this Agreement and all backups ninety (90) days thereafter.

7. PROPRIETARY RIGHTS

7.1 **Customer's Proprietary Rights.** Customer remains the sole owner of all Intellectual Property Rights in Customer Data. Customer warrants that Supplier's use of Customer Data in connection with this Agreement shall not cause Supplier to infringe any Applicable Laws or third-party Intellectual Property Rights.

7.2 **Supplier's Proprietary Rights**. This is an Agreement for access to and use of the Services as set out herein. Supplier and its licensors remain the sole owner of all Intellectual Property Rights and other right, title, and interest in the Documentation, Supplier's trademarks and service marks, the Services, and any related software. Supplier does not grant Customer any Intellectual Property Rights under this Agreement.

7.3 **Feedback**. Customer may provide feedback regarding any part of the Services, productus, business or development plans, or technology roadmaps ("**Feedback**"). Supplier may collect data from Customer's use of the Services ("**Learnings**") for lawful business purposes, including but not limited to understanding, improving, and developing the Services, artificial intelligence learning, benchmarking, and analytics. However, Supplier will not disclose Learnings externally unless it is aggregated or de-identified.

8. CONFIDENTIALITY

8.1 **Confidentiality Undertaking**. Each party shall (a) not use the other party's Confidential Information other than as required for the performance of its obligations or as permitted under this Agreement; (b) not disclose the other party's Confidential Information to any third party (except its Affiliates, Sub-Processors, professional advisors or as required by Applicable Law) without the prior written consent of the other party; and (c) use reasonable efforts (not less than it uses to protect its own confidential information) to prevent the unauthorized disclosure of the other party's Confidential Information. Notwithstanding the foregoing, Customer permits Supplier to disclose, under obligations of confidentiality no less onerous than those set out herein, that Customer is a customer of Supplier to actual or potential clients, partners, and investors.

8.2 **Exceptions**. Confidential Information shall not include any information which: (a) is or becomes publicly known other than through any act or omission of the receiving party; b) was in the other party's lawful possession before the disclosure; (c) is lawfully disclosed to the receiving party by a third party without restriction on disclosure; or (d) was or is independently developed by the receiving party without reference to the Confidential Information of the other party.

8.3 **Required Disclosure**. If a receiving party is required to disclose Confidential Information of the other party under applicable law, court order or other governmental authority lawfully demanding the Confidential Information, the receiving party shall: (a) to the extent legally permissible, give to the disclosing party prompt written notice of the request and a reasonable opportunity to object to the disclosure and to seek a protective order or other appropriate remedy; (b) use reasonable efforts

to limit disclosure; (c) disclose only the Confidential Information specifically required and only to the extent compelled to do so; and (d) continue to maintain confidentiality after the required disclosure.

9. DATA & SECURITY

9.1 **Data Protection**. Both parties shall comply with their obligations under Data Protection Law and in the DPA.

9.2 **Security**. Supplier will maintain appropriate administrative, physical, and technical safeguards for protection of the security, confidentiality, and integrity of Customer Data, as further described at the Security Policy and Annex 2 of the DPA. Those safeguards will include, but will not be limited to, measures designed to protect against the unauthorized access to or disclosure of Customer Data in accordance with ISO 27001 and SOC2 Type 2.

9.3 **Customer Data Protection.** Customer acknowledges that it is the Controller of the Customer Data and as such Customer warrants that it shall use the Services in compliance with all applicable Data Protection Laws and that it has all necessary consents (or other lawful basis) to transfer the Customer Data to Supplier. Customer will defend and indemnify Supplier and its Affiliates (and their respective employees, directors, and representatives) from all claims or demands by a third party, including all damages, liabilities, costs, reasonable attorneys' fees, and fines imposed by legal or regulatory bodies, to the extent resulting from, alleged to have resulted from or in connection with any violation by Customer or its Affiliates of any applicable Data Protection Law or applicable employee hiring laws.

10. INDEMNIFICATION

10.1 **Supplier Indemnification**. Supplier shall defend and indemnify Customer and its Affiliates against any losses, costs, expenses (including reasonable legal costs) and damages in connection with any third-party claim or action brought against Customer to the extent that such claim directly arises from an allegation that the use of the Services (or any part thereof) infringes the Intellectual Property Rights of a third party ("**IP Claim**"). This Section shall not apply to the extent the IP Claim is attributable to: (a) use of the Services (or any part thereof) by or on behalf of Customer other than in accordance with the terms of this Agreement; (b) any use by or on behalf of Customer of the Services in combination with any item not supplied or recommended by Supplier; or (c) fraud, fraudulent misrepresentation, negligence or wilful misconduct by or on behalf of Customer.

10.2 **Conditions**. If any third party makes a claim under any indemnity under this Agreement, or notifies an intention to make such claim against the indemnified party, the indemnified party must: (a) as soon as reasonably practicable, give written notice of the claim to the indemnifying party; (b) not make any admission of liability, agreement or compromise in relation to the claim without the prior written consent of the indemnifying party; (c) allow the indemnifying party to have full control of the claim and the authority to settle or otherwise dispose of the claim, provided that the indemnifying party shall not make any admission of liability without the prior written consent of the indemnified party (such consent not to be unreasonably withheld or delayed); (d) use reasonable efforts to mitigate any damages, costs, losses, liabilities, and expenses resulting from any relevant claim; and (e) give the indemnifying party and its professional advisers reasonable assistance to enable them to assess, defend and/or settle the claim.

10.3 **Replacement or Modification**. If the Services (or any part thereof) infringes the Intellectual Property Rights of a third party (or Supplier reasonably believes such is likely), Supplier may (at its sole discretion and expense):

a) modify or replace any part of the Service so that it ceases to be infringing; or

b) procure for Customer the right to continue to use the infringing Services (or any component part thereof).

If after a reasonable amount of time Supplier does not provide Customer with one of the options above either party may terminate the infringing Services with immediate effect and Supplier will issue a pro-rata refund to Customer for any prepaid Fees for the infringing Services covering the remainder of the Term. Subject to Supplier's indemnity for IP Claims in Section 10.1, this Section 10.3 states Customer's sole and exclusive rights and remedies in respect of any intellectual property infringement of the Services under this Agreement.

11. LIMITATION OF LIABILITY

11.1 **NO LIMITATION**. NOTHING IN THIS AGREEMENT EXCLUDES EITHER PARTY'S LIABILITY FOR: (A) DEATH OR PERSONAL INJURY; (B) GROSS NEGLIGENCE, WILLFUL MISCONDUCT, FRAUD OR FRAUDULENT MISREPRESENTATION; (C) CUSTOMER'S LIABILITY FOR PAYMENT OF FEES; (D) SUPPLIER'S LIABILITY FOR AN IP CLAIM UNDER SECTION 10.1; OR (E) ANY LIABILITY THAT CANNOT BE LAWFULLY LIMITED OR EXCLUDED.

11.2 **EXCLUDED DAMAGES**. IN NO EVENT SHALL EITHER PARTY HAVE ANY LIABILITY TO THE OTHER PARTY FOR ANY INDIRECT, CONSEQUENTIAL, OR SPECIAL DAMAGES, WHETHER SUCH ARISE IN CONTRACT, TORT (INCLUDING NEGLIGENCE) OR OTHERWISE, INCLUDING BUT NOT LIMITED TO ANY: (A) LOSS OF PROFITS; (B) LOSS OF ANTICIPATED SAVINGS; (C) LOSS OR CORRUPTION OF CUSTOMER DATA EXCEPT TO THE EXTENT THAT SUPPLIER HAS BREACHED THE AGREEMENT; (D) LOSS OF GOODWILL AND REPUTATION; (E) COST OF REPLACEMENT OF SUBSTITUTE GOODS; (F) LOSS OF BUSINESS OPPORTUNITY; OR (G) WASTED EXPENDITURE.

11.3 **LIMITATION OF LIABILITY**. IF EITHER PARTY IS DETERMINED TO HAVE ANY LIABILITY TO THE OTHER PARTY OR ANY THIRD PARTY UNDER OR IN CONNECTION WITH THIS AGREEMENT, EACH PARTY'S AGGREGATE LIABILITY, TOGETHER WITH THAT OF ITS OFFICERS, DIRECTORS, EMPLOYEES AFFILIATES AND AGENTS, WILL BE LIMITED TO THE TOTAL AMOUNT OF FEES PAID OR PAYABLE UNDER THE APPLICABLE ORDERS OR SOWS IN THE TWELVE-MONTH PERIOD PRECEDING THE EVENT GIVING RISE TO ANY CLAIM.

12. INSURANCE

12.1 During the Term, Supplier shall, at its own cost and expense, obtain and maintain, comprehensive insurance to cover its potential liabilities to Customer and such insurance as is legally required and appropriate to its business. Upon Customer's written request (not more than once annually), Supplier will provide insurance certificates. All insurance policies are placed with insurers rated equivalent to "A-" or better by A.M. Best.

13. MISCELLANEOUS

13.1 **Notices**. Any notice or other communication required to be given under this Agreement shall be in writing and shall be delivered by email, in the case of Supplier to contract.notices@beamery.com.

13.2 **Export Controls**. In the event that the Services are subject to applicable U.S., UK, or EU export control and economic sanctions laws, the parties agree to comply strictly with all such domestic and international export laws and economic sanctions regulations as they apply to the Services or use thereof, and to the extent consistent with the Agreement, to obtain any necessary license or other authorization to export, re-export, or transfer the Services.

13.3 **References**. Upon go-live of the Services and at the reasonable request of Supplier, Customer shall provide references to potential customers of Supplier.

13.4 **No Waiver.** No failure or delay by a party to exercise any right or remedy, in whole or in part, provided under this Agreement or by law shall constitute a waiver of that or any other right or remedy, nor shall it prevent or restrict the further exercise of that or any other right or remedy.

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

13.6 **Entire Agreement**. This Agreement and its exhibits contain the whole agreement between the parties relating to the subject matter hereof and supersedes all prior agreements, arrangements and understandings between the parties relating to that subject matter. No variation or amendment of this Agreement shall be effective unless it is in writing and signed by the parties.

13.7 **Third Party Rights**. Nothing in this Agreement, express or implied, is intended to or shall confer upon any third-party person or entity any right, benefit or remedy of any nature whatsoever under or by reason of this Agreement or under the Contracts (Rights of Third Parties) Act 1999 (to the extent applicable).

13.8 **Relationship of the Parties**. Nothing in this Agreement is intended to, or shall be deemed to, establish any partnership or joint venture between any of the parties, constitute any party the agent of another party, or authorize any party to make or enter any commitments for or on behalf of any other party.

13.9 **Assignment**. Neither party shall assign any of their rights or obligations under this Agreement without the prior written consent of the other party, which consent shall not unreasonably be withheld. However, consent is not required for an assignment of this Agreement in connection with a change of control, merger, stock transfer, sale or other disposition of substantially all the assets of the assigning party's business. This Agreement will bind and inure to the benefit of each party's successors and assigns.

13.10 **Force Majeure**. Except for Customer's payment obligations, neither party shall in any circumstances be in breach of this Agreement nor liable for delay in performing, or failure to perform, any of its obligations under this Agreement if such delay or failure results from an event of Force Majeure. If the Force Majeure event prevents the affected party's performance of its obligations for a continuous period of more than four (4) weeks, the party not affected by the Force Majeure event may terminate this Agreement by giving one (1) week's written notice to the affected party.

13.11 **Survival**. In addition to any provisions that expressly survive, the following Sections shall survive the expiration or termination of this Agreement: 6 (*Term & Termination*), 7 (*Proprietary Rights*), 8 (*Confidentiality*), 9 (*Data Protection & Security*), 11 (*Limitation of Liability*), 13 (*Miscellaneous*), and 14 (*Governing Law & Jurisdiction*).

13.12 **Interpretation.** A reference to a statute or statutory provision is a reference to it as amended, extended, or re-enacted from time to time. In the event of any conflict or ambiguity between any provision contained in an Order or SOW and in the Agreement, the provision in the Order or SOW shall take precedence.

13.13 **Authority**. Each party confirms that it has the legal power and authority to, and hereby does, enter into this Agreement and any Order and SOW in accordance with applicable law and with all due authority.

13.14 **Attorney's Fees.** In the event of a dispute or claim, each party shall be responsible for their own legal fees.

14. GOVERNING LAW AND JURISDICTION

14.1 **Governing Law**. This Agreement and any dispute, or claim arising out of or in connection with it shall be governed by and construed in accordance with the laws of [England / the state of New York].

14.2 **Jurisdiction**. The parties consent and submit to the exclusive jurisdiction of the courts of [England / New York, New York] for any litigation arising out of or relating to this Agreement.

EXHIBIT 1 - DATA PROCESSING AGREEMENT

1. DEFINITIONS

1.1 **Controller**, **Processor**, **Data Subject**, **Personal Data, Processing** (and **Process**) and **Personal Data Breach** shall have the meanings given in the GDPR, or the material equivalent under other applicable Data Protection Law.

1.2 **Restricted Transfer** means a transfer of Personal Data from the European Economic Area or UK (as applicable) to a country outside of the European Economic Area or UK (as applicable) which is not subject to an adequacy determination.

1.3 **Standard Contractual Clauses** or **SCCs** means the contractual clauses annexed to the European Commission's Implementing Decision 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council ("**EU SCCs**") or the UK Addendum to the EU SCCs issued by the UK Information Commissioner's Office, as applicable. Completed SCCs can be found at https://beamery.com/terms-and-conditions/.

1.4 **Data Privacy Framework** means the EU/UK/Swiss to US Data Privacy Framework self-certification program operated by the US Department of Commerce.

1.5 **Data Privacy Principles** means the Data Privacy Framework principles (as supplemented by the Supplemental Principles).

2. PERSONAL DATA PROCESSING

2.1 Supplier shall process Personal Data on Customer's behalf to perform its obligations under this Agreement and, as such, Customer is the Controller and Supplier is the Processor for the purposes of the Data Protection Law. Annex 1 sets out the details of the data processing to be undertaken by Supplier.

2.2 Customer can use the Services to assist it with its obligations under the GDPR, including its obligations to respond to requests from Data Subjects. Taking into account the nature of the processing, Customer agrees that it is unlikely that Supplier would become aware that Customer Data transferred under the Agreement is inaccurate or outdated. Nonetheless, if Supplier becomes aware that Customer Data transferred under the Agreement is inaccurate or outdated, it will inform Customer without undue delay. Supplier will cooperate with Customer to erase or rectify inaccurate or outdated Customer Data transferred under the Agreement by providing the tools within the Services so that Customer can use it to erase or rectify Customer Data.

2.3 Each party will comply with all applicable Data Protection Law.

3. SUPPLIER OBLIGATIONS

3.1 Supplier shall, in relation to any Personal Data processed by Supplier in connection with the performance of its obligations under this Agreement:

a) Process Personal Data only for the purpose of fulfilling the terms of the Agreement or on the documented instructions of Customer, unless otherwise required to do so under applicable Data Protection Law.

b) Ensure that each of its employees, agents, subcontractors, Sub-Processors or any persons acting under the authority of Supplier are made aware of Supplier's obligations with regard to the confidentiality of the Personal Data and require that they enter into binding obligations with the Supplier in order to maintain such confidentiality.

c) Assist Customer in ensuring compliance with the Customer's obligations pursuant to applicable Data Protection Law in respect of security of processing, notification of Personal Data Breaches to the appropriate supervisory authority, communication of Personal Data Breaches to the Data Subject, data protection impact assessments and prior consultation with the appropriate supervisory authority where appropriate.

d) Make available to the Customer all information necessary to demonstrate compliance with Article 28 of the GDPR and allow for and contribute to audits (subject to Section 6.3 below).

e) Promptly notify the Customer if, in its opinion, it is asked to do something that infringes Data Protection Laws.

f) Maintain a record of all categories of processing activities carried out on behalf of the Customer.

g) Where applicable, cooperate with the appropriate supervising authority in the performance of its tasks.

h) Not Sell (as defined in the CCPA/CPRA) any Personal Data.

4. DATA DELETION

4.1 Supplier shall delete all of Customer's Personal Data in the production environment within 30 days of termination or expiration of the Agreement and all existing backups within 90 days thereafter unless applicable Data Protection Law requires storage of the Personal Data or as otherwise agreed between the parties. Supplier will provide a certification of deletion of Personal Data (as described in clause 8.5 of the SCCs) upon Customer's written request.

5. DATA SUBJECT RIGHTS

5.1 Supplier shall assist Customer in the fulfilment of Customer's obligation to respond to or action a Data Subject request under Data Protection Law. If a Data Subject makes a request to Supplier, Supplier will forward such request to Customer without undue delay. Customer authorizes Supplier to respond to any Data Subject who makes a request to Supplier, to confirm that Supplier has forwarded the request to Customer.

5.2 Supplier shall notify Customer without undue delay following confirmation of a Personal Data Breach affecting Customer's Personal Data. The notification will include, to the extent such information is available: (a) the nature of the Personal Data

Breach including where possible, the categories and approximate number of Data Subjects concerned and the categories and approximate number of Personal Data records concerned; (b) the name and contact details of the data protection officer or other contact point where more information can be obtained; (c) the likely consequences of the Personal Data Breach; (d) the measures taken or proposed to be taken by Supplier to address the Personal Data Breach, including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue delay. Customer agrees that an unsuccessful security incident will not be subject to this Section. An unsuccessful security incident is one that results in no unauthorized destruction, loss, alteration, disclosure of, or access to Customer Data or Customer's Personal Data or to any of Supplier's equipment or facilities storing Customer Data.

6. SECURITY MEASURES AND AUDITS

6.1 In providing the Services, Supplier shall at all times, taking into account the nature, scope, context and purposes of the processing, the level of risk and severity for the rights and freedoms of natural persons that might result from a Personal Data Breach, technological developments, and the costs of implementing any measures, implement technical and organizational measures to protect against a Personal Data Breach, including as set out in Annex 2.

6.2 Supplier shall ensure that the security of Personal Data is protected by recognized industry standard policies and procedures (not less than set out in this DPA).

6.3 Upon Customer's request, and subject to the confidentiality obligations set forth in the Agreement, Supplier shall make available to Customer information regarding Supplier's compliance with the obligations set forth in this DPA in the form of third-party certifications. Supplier and Customer agree that such demonstration of compliance by Supplier is the preferred mechanism for meeting the requirements of Article 28(3)(h) of the GDPR and the SCCs. To the extent that Customer (acting reasonably) is not satisfied with such demonstration of compliance, Supplier may allow for and contribute to audits, by or on behalf of Customer in relation to the processing of the Customer Personal Data. Customer may contact information.security@beamery.com to request a remote audit of the procedures relevant to the protection of Personal Data, provided that Customer may not exercise this right more than once per year. Before the commencement of any such remote audit, the parties shall mutually agree upon the scope, timing, and duration of the audit. Customer shall promptly notify Supplier with information regarding any non-compliance discovered in an audit. Such audit shall not require Supplier to disclose to Customer any data or information relating to Supplier's other customers or Supplier's internal accounting, or any data information that, in Supplier's reasonable opinion, could compromise its security or cause Supplier to breach its obligations to a third party.

7. ONWARD TRANSFERS

7.1 In connection with the Services, the parties anticipate that Supplier (and its Sub-Processors) may process Personal Data outside of the European Economic Area (EEA), Switzerland, the UK, or the country where Customer, Authorized Users, or Contacts are located. The parties agree that when a transfer of Personal Data under this Agreement is a Restricted Transfer it shall be subject to the appropriate transfer mechanism. Supplier shall not (nor permit any Sub-Processor to) make a Restricted Transfer unless the Restricted Transfer is made in compliance with applicable Data Protection Laws.

7.2 **Transfer mechanisms for data transfers.** If, in the performance of the Services, Personal Data that is subject to Data Protection Laws that apply in EEA/UK/Switzerland is transferred out of such regions to countries which do not ensure an adequate level of data protection within the meaning of the applicable Data Protection Laws, the transfer mechanisms listed below shall apply to such transfers and can be directly enforced by the Parties to the extent such transfers are subject to the Data Protection Laws.

7.3 **Data Privacy Framework.** To the extent Beamery Inc. processes any Personal Data via the Services originating from the EEA/UK/Switzerland, Supplier represents that Beamery Inc. is self-certified under the Data Privacy Framework and complies with the Data Privacy Principles when processing any such Personal Data. To the extent that Customer is (a) located in the United States of America and is self-certified under the Data Privacy Framework or (b) located in the EEA or Switzerland, Supplier further agrees: (i) to provide at least the same level of protection to any Personal Data as required by the Data Privacy Principles; (ii) to notify Customer in writing, without undue delay, if its self-certification to the Data Privacy Framework is withdrawn, terminated, revoked, or otherwise invalidated (in which case, an alternative transfer mechanism will apply in accordance with applicable Data Protection Laws); and (iii) upon written notice, to work with Customer to take reasonable and appropriate steps to stop and remediate any unauthorized processing of personal data.

7.4 **Transfers from the EEA**. In relation to Personal Data protected by the EU GDPR that is not covered under the Data Privacy Framework, the EU SCCs will apply completed as follows:

a) Module Two will apply.
b) in Clause 7, the optional docking clause will apply;
c) in Clause 9, Option 2 "General Authorization" will apply, and the time period for prior notice of Sub-Processor changes shall be as set out in Section 8 of this DPA;
d) in Clause 11, the optional language will not apply;
e) in Clause 17, Option 1 will apply, and the EU SCCs will be governed by German law;
f) in Clause 18(b), disputes shall be resolved before the courts of Germany;
g) Annex I of the EU SCCs shall be deemed completed with the information set out in Annex 1 to this DPA;
h) Annex II of the EU SCCs shall be deemed completed with the information set out in Annex 2 to this DPA; and

i) Annex III of the EU SCCs is not needed as the parties have agreed to general authorization of Sub-Processors.

7.5 **Transfers from UK**. Where a Restricted Transfer is made from the UK, the UK Addendum is deemed executed between Customer and Supplier and the EU SCCs (as modified above) shall apply as amended by the UK Addendum.

7.6 **Transfers from Switzerland**. Where a Restricted Transfer is made from Switzerland in relation to data that is protected by the Swiss Federal Act on Data Protection, the EU SCCs (as modified above) are incorporated into this DPA, except that:

a) in Clause 13, the competent supervisory authority is the Swiss Federal Data Protection and Information Commissioner;

b) references to "Member State" shall refer to Switzerland; and

c) references to the "General Data Protection Regulation," "Regulation 2016/679," and "GDPR" in the EU SCCs shall refer to the Swiss Federal Act on Data Protection (as amended or replaced).

7.7 **Conflict**. If any provision of this DPA is inconsistent with any terms in the Agreement, this DPA will prevail. If any provision of this DPA is inconsistent with any terms in the SCCs, the SCCs will prevail.

8. SUB-PROCESSORS

8.1 Customer provides general authorization to Supplier appointing the Sub-Processors set out at https://beamery.com/terms-and-conditions (as amended from time to time with prior written notice to Customer) as third-party processors of Personal Data under this Agreement. Before each Sub-Processor processes Personal Data, Supplier shall: (a) carry out due diligence and enter into written contract with the Sub-Processor to ensure that the Sub-Processor shall provide the same level of protection for Personal Data as required by this DPA and Article 28(3) of the GDPR; and (b) if that arrangement involves a Restricted Transfer, ensure that such Sub-Processors have an appropriate transfer mechanism in place.

8.2 Customer may reasonably object to Supplier's use of a new Sub-Processor by notifying Supplier promptly in writing within fourteen (14) days of Supplier's notice. In the event Customer, acting reasonably, objects to a new Sub-Processor, Supplier will use commercially reasonable efforts to make available or recommend to Customer a change in the Services or configuration or use of the Services to avoid Processing of Personal Data by the objected-to new Sub-Processor without unreasonably burdening Customer.

8.3 Supplier shall remain liable for all acts or omissions of all Sub-Processors to the same extent Supplier would be liable if performing the services of each Sub-Processor directly under the terms of the Agreement.

9. GOVERNMENT ACCESS REQUESTS

9.1 In its role as a Processor, Supplier shall maintain appropriate measures to protect Personal Data in accordance with the requirements of Data Protection Laws. If Supplier receives a legally binding request to access Personal Data from a law enforcement agency, Supplier shall, unless legally prohibited: (a) promptly notify Customer including a summary of the request; (b) inform the requesting government authority that Supplier is a service provider and it is not authorized to disclose the Personal Data; (c) inform the requesting government authority that all requests for the Personal Data must be sent to Customer; and (d) not provide access to the Personal Data unless authorized by Customer in writing. To the extent Supplier is prohibited by law from providing such notification, Supplier shall use commercially reasonable efforts to obtain a waiver of the prohibition to enable Supplier to communicate to Customer as much information as possible, as soon as possible. Further, Supplier may challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful. Supplier may pursue possibilities of appeal and may request Customer to cover expenses for such appeal. Supplier shall promptly notify Customer if Supplier becomes aware of any direct access by a Public Authority to Personal Data and provide information available to Supplier, to the extent permitted by law. For the avoidance of doubt, this DPA shall not require Supplier to pursue action or inaction that could result in civil or criminal penalty for Supplier. Supplier shall not disclose Personal Data in a massive, disproportionate, and indiscriminate manner that goes beyond what is necessary in a democratic society. Supplier shall ensure that Sub-Processors involved in the processing of Personal Data are subject to the relevant commitments regarding government access requests in the SCCs. Supplier shall ensure that Sub-Processors are subject to the relevant commitments regarding such government access requests.

ANNEX 1 - DATA PROCESSING DETAILS

This Annex I forms part of the DPA and describes the processing that Supplier will perform on behalf of Customer.

A. LIST OF PARTIES

Controller(s) / Data exporter(s): [*Identity and contact details of the controller(s) /data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union*]

Name:	Customer
Address:	Customer's address as identified in the Order
Contact person's name, position and contact details:	Customer's email address as identified in the Order
Activities relevant to the data processed under these Clauses:	Customer will provide Personal Data to Supplier for Supplier to provide services to Customer pursuant to the Agreement.
Role (controller/processor):	Controller

Processor(s) / Data importer(s): *[Identity and contact details of the processor(s) /data importer(s), including any contact person with responsibility for data protection*]

Name:	Beamery Inc.
Address:	440 N Barranca Ave #9358 Covina, CA 91723
Contact person's name, position and contact details:	DPO, privacy@beamery.com
Activities relevant to the data processed under these Clauses:	The processing activities that are necessary for Supplier to provide its services to Customer, including but not limited to: hosting, support services, implementation of the SaaS, resume parsing, performance advisory and consulting services, and performance analytics.
Role (controller/processor):	Processor with respect to Customer Personal Data; Controller with respect to usage data

B. DESCRIPTION OF PROCESSING

Categories of Data Subjects whose personal data is processed:	● Customer's potential and actual candidates ● Individuals who have provided their data to Customer ● Customer's employees and representatives ● Customer's Authorized Users
Categories of personal data processed:	The Personal Data processed by Supplier is determined and controlled by Customer in its sole discretion. Anticipated categories: ● First and last name ● Business contact information (company, email, phone, business address) ● Personal contact information (email, phone, address) ● ID data (e.g. applicant number) ● Professional life data (title, position, employer, employment history) ● Personal life data (e.g. hobbies and interests) ● Connection data (e.g. referrals and LinkedIn account) ● Localization data ● Technical usage and device (e.g. IP address, device type, browser type) ● Notes and other data logged by users (e.g. feedback on candidates) ● Communication and calendar information (e.g., emails sent to candidates) ● Information regarding application forms, CVs, credentials, or qualifications.
Sensitive data processed (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks	The Processing may include sensitive data if such information is uploaded or transmitted via the software, at the sole discretion of the user of the software. Anticipated sensitive data would be race, gender, sexual

involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialized training), keeping a record of access to the data, restrictions for onward transfers or additional security measures:	orientation. Sensitive data should be collected by the Customer on a data subject explicit consent basis.
The frequency of the processing (e.g., whether the data is processed on a one-off or continuous basis):	Personal data will be processed continuously throughout the Term of the Agreement.
Nature of the processing:	For the provision of the Services purchased under the Agreement.
Purpose(s) of the data processing:	The data processing undertaken by Supplier will involve any such processing that is necessary for to provide the Services and fulfil its obligations as set out in the Agreement or as otherwise agreed between the parties in writing during the Term.
The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period:	Term of the Agreement and for 30 days from termination in the production environment and for 90 days thereafter in the back-up environments unless the personal data is deleted prior to the termination or expiration of that contract by the Customer or by the Supplier at the Customer's instruction. Data is deleted in accordance with NIST SP 800-88/DoD 5220.22-M standards.
For processing of (sub-) processors, also specify subject matter, nature and duration of the processing:	Personal data is processed to the Supplier's Sub-Processors for the purpose of providing the Supplier's Services to the Customer for the duration of the Agreement unless the personal data is deleted prior to the termination or expiration of that contract by the Customer or by the Supplier at the Customer's instruction.

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance (e.g., in accordance with Clause 13 SCCs)	Germany or UK (as applicable)

ANNEX 2 - TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

Description of the technical and organisational measures implemented by the processor(s) / data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

Supplier will maintain administrative, physical, and technical safeguards for protection of the security, confidentiality and integrity of any Personal Data uploaded to the Services or otherwise maintained on behalf of Customer (as Data Controller), as described in the documentation made accessible via Supplier's Trust Centre at https://trust.beamery.com/. Supplier reserves the right to update the documentation from time-to-time, provided that the amended technical and organizational measures are not less protective than those currently stated therein.

Measure	Description
Measures of pseudonymisation and encryption of personal data	Industry standard encryption technologies for Personal Data that is: (i) transmitted over public networks (*i.e.*, the Internet) or when transmitted wirelessly; or (ii) at rest. Supplier encrypts data in transit in accordance with TLS 1.2 or above and at rest in accordance with AES256.
Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services	Organisational management and dedicated staff responsible for the development, implementation and maintenance of Supplier's information security program. Data security controls which include at a minimum, but may not be limited to, logical segregation of data, restricted (e.g., role-based) access and monitoring, and utilisation of commercially available and industry standard encryption technologies for Personal Data, as described above. Network security controls that provide for the use of stateful firewalls and layered DMZ architectures and other traffic and event correlation procedures designed to protect systems from intrusion and limit the scope of any successful attack. Vulnerability assessment, patch management and threat protection technologies and scheduled monitoring procedures designed to identify, assess, mitigate and protect against identified security threats, viruses and other malicious code. Business resiliency/continuity and disaster recovery procedures designed to maintain service and/or recovery from foreseeable emergency situations or disasters.
Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident	Incident / problem management procedures designed to allow Supplier to investigate, respond to, mitigate and notify of events related to Supplier's technology and information assets.
Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing	Audit and risk assessment procedures for the purposes of periodic review and assessment of risks to Supplier's organisation, monitoring and maintaining compliance with Supplier's policies and procedures and reporting the condition of its information security and compliance to internal senior management.
Measures for user identification and authorisation	Logical access controls designed to manage electronic access to data and system functionality based on authority levels and job functions, (e.g., granting access on a need-to-know and least privilege basis, use of unique IDs and passwords for all users, periodic review and revoking/changing access promptly when employment terminates or changes in job functions occur). Password controls designed to manage and control password strength, expiration and usage including prohibiting users from sharing passwords and requiring that Supplier's passwords that are assigned to its employees: (i) be at least ten (10) characters in length, (ii) not be stored in readable format on Supplier's computer systems, (iii) must have defined complexity, and (iv) must have a history threshold to prevent reuse of recent passwords. Multi-factor authentication, where available, must always be used.

Measures for the protection of data during transmission	Industry standard encryption technologies for Personal Data that is transmitted over public networks (*i.e.*, the Internet) or when transmitted wirelessly.
Measures for the protection of data during storage	Supplier encrypts data at rest in accordance with AES256. Backup files are encrypted at rest and in transit between primary and secondary storage locations.
Measures for ensuring physical security of locations at which personal data are processed	Physical and environmental security of data centre, server room facilities and other areas containing Personal Data designed to: (i) protect information assets from unauthorised physical access, (ii) manage, monitor and log movement of persons into and out of Supplier facilities, and (iii) guard against environmental hazards such as heat, fire and water damage.
Measures for ensuring events logging	System audit or event logging and related monitoring procedures to proactively record user access and system activity for routine review.
Measures for ensuring system configuration, including default configuration	Operational procedures and controls to provide for configuration, monitoring and maintenance of technology and information systems according to prescribed internal and adopted industry standards, including secure disposal of systems and media to render all information or data contained therein as undecipherable or unrecoverable prior to final disposal or release from Supplier's possession.
Measures for internal IT and IT security governance and management	Change management procedures and tracking mechanisms designed to test, approve and monitor all changes to Supplier's technology and information assets.
Measures for certification/assurance of processes and products	Organisational management and dedicated staff responsible for the development, implementation and maintenance of Supplier's information security program.
Measures for ensuring data minimisation	Not applicable to Supplier. Supplier is processing the Personal Data on behalf of the Customer for the sole purpose of providing services to the Supplier for the duration of the services agreement entered into between the Supplier and the Customer. The Customer has complete control over the collection, modification, and deletion of Personal Data (subject to the data retention section, below).
Measures for ensuring data quality	Not applicable to Supplier. Supplier is processing the Personal Data on behalf of the Customer for the sole purpose of providing services to the Supplier for the duration of the services agreement entered into between the Supplier and the Customer. The Supplier does not have the ability to monitor the quality of the Personal Data.
Measures for ensuring limited data retention	Customer is permitted to set its own retention rules per a dedicated feature within the application and can self-service delete the personal data it has collected at any point during the term of the underlying services agreement. All Personal Data in the Customer's production environment is deleted thirty (30) days after termination or expiration of this Agreement and all backups ninety (90) days thereafter.
Measures for ensuring accountability	Supplier takes responsibility for complying with the EU GDPR and the UK GDPR, at the highest management level and throughout the organisation. Supplier keeps evidence of the steps taken to comply with the EU GDPR and the UK GDPR. Supplier puts in place appropriate technical and organisational measures, such as: (i) adopting and implementing data protection policies (where proportionate), (ii) putting written contract in place with organisations that process personal data on our behalf, (iii) maintaining documentation of our processing activities, (iv) implementing appropriate security measures, (v) recording and, where necessary, reporting personal data breaches, and (vi) carrying out data protection impact assessments for uses of personal data that are likely to result in high risk to individuals' interests. Supplier reviews and updates accountability measures at appropriate intervals.
Measures for allowing data portability and ensuring erasure	Customer Data can be exported in .NDJSON format at any time. Customer data is retained as long as the contract is active and is securely deleted

	from production within 30 days of contract termination and within further 90 days from backups. Media and equipment assets are disposed of securely using NIST SP 800-88/DoD 5220.22-M approved destruction standards. The disposal of printed materials must be witnessed secure shredding and placed in locked secure disposal bins.

For transfers to (sub-) processors, also describe the specific technical and organisational measures to be taken by the (sub-) processor to be able to provide assistance to the controller (and, for transfers from a processor to a sub-processor, to the data exporter).

Measure	Description
Self-Service Features	At all times during the term of the underlying services agreement, Customer will have access to its own Beamery account and the ability to delete or modify any personal data stored therein. Any deletions or modifications by Customer will automatically be reflected in Supplier's databases as well.

EXHIBIT 2 - TALENTGPT ADDENDUM

This Exhibit 2 shall apply if Customer opts to utilize TalentGPT as part of the Services. To the extent that any Section in this Exhibit 2 conflicts with the main body of this Agreement or any other Exhibit, this Exhibit 2 shall prevail with respect to TalentGPT.

1. Definitions

1.1. "**TalentGPT**" means generative AI that is powered by Microsoft Azure's OpenAI LLM which has been fine-tuned using Supplier's own proprietary models. As of the Effective Date, TalentGPT is a Beta Service.

1.2. Authorized Users may provide prompts to TalentGPT ("**Prompt(s)**"), and receive a response generated and returned by TalentGPT based on the Prompt and/or Customer Data ("**Response(s)**").

2. **Ownership.** As between Supplier and Customer, Customer will own any Responses and Supplier hereby assigns all Intellectual Property Rights (if any) in the Responses to Customer. However, Customer acknowledges that Responses may not be unique, and the same or similar Responses may be provided to other users and customers; So Responses may not qualify for intellectual property protection, and Supplier makes no warranties or indemnities with regard to the Responses' infringement of third-party rights.

3. **Third Parties**. Supplier does not permit any third party (including Microsoft) to use Customer Data to train their machine learning models.

4. **Reinforced Learning and Human Feedback**. Customer acknowledges that Supplier uses reinforced learning and human feedback to monitor TalentGPT's performance, which involves Supplier's personnel manually reviewing Prompts, Responses and other TalentGPT output. Supplier may use such learnings for improving and developing TalentGPT. For clarity, Customer Data is not automatically fed into TalentGPT's underlying AI models for training.

5. **DISCLAIMER**. While Supplier has developed TalentGPT with a variety of talent-focused situations in mind, Customer's use of TalentGPT with Customer Data may result in new and untested results and outcomes. Supplier does not make any warranty in relation to the Prompts, Responses, or other TalentGPT output, including their accuracy or fitness for purpose. Customer understands and agrees that the use of TalentGPT is done at Customer's sole discretion and it should not rely on any assertions in the Responses or other TalentGPT output without independently fact-checking them.

EXECUTION PAGE

THIS AGREEMENT IS DATED AND TAKES EFFECT ON THE EFFECTIVE DATE

SIGNED FOR AND ON BEHALF OF SUPPLIER

Signed ……

Print name ……

Title ……

SIGNED FOR AND ON BEHALF OF CUSTOMER

Signed ……

Print name ……

Title ……