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it is unlikely that Supplier would become aware that Customer Data transferred under the Agreement is inaccurate or outdated. Nonetheless, if Supplier becomes aware that Customer Data transferred under the Agreement is inaccurate or outdated, it will inform Customer without undue delay. Supplier will cooperate with Customer to erase or rectify inaccurate or outdated Customer Data transferred under the Agreement by providing the tools within the Services so that Customer can use it to erase or rectify Customer Data.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.