ADDENDUM
TO INCLUDE EU/UK STANDARD CONTRACTUAL CLAUSES (where applicable)
NOVEMBER 2021

The Parties acknowledge and agree that the following provisions will apply in respect of the sharing of any Personal Data (to which EU Data Protection Legislation applies) by the Controller with Beamery as a Processor.

COMMISSION IMPLEMENTING DECISION (EU) 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.

STANDARD CONTRACTUAL CLAUSES – Module 2: MODULE TWO: Transfer controller to processor. The full text of the Module 2: Transfers Controller to Processor is available at: https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?uri=CELEX:32021D0914&locale=en (the "**EU SCCs**")

Note: Completed EU SCCs Clauses as well as Annex 1 and Annex 2 are provided below.

In relation to Personal Data that is protected by the EU GDPR, the EU SCCs will apply completed as follows:

(i) Module Two will apply;

(ii) in Clause 7, the optional docking clause will apply;

(iii) in Clause 9, Option 2 "General Authorisation" will apply, and the time period for prior notice of sub-processor changes shall be 14 days. List of Sub-processors can be found here;

(iv) in Clause 11, the optional language will not apply;

(v) in Clause 17, Option 1 will apply, and the EU SCCs will be governed by German law;

(vi) in Clause 18(b), disputes shall be resolved before the courts of Germany;

(vii) Annex I of the EU SCCs shall be deemed completed with the information set out in Annex I;

(viii) Annex II of the EU SCCs shall be deemed completed with the information set out in Annex II; and

In the event that any provision of an underlying agreement contradicts, directly or indirectly, the EU SCCs, the EU SCCs shall prevail.

UK STANDARD CONTRACTUAL CLAUSES

In relation to Personal Data that is protected by the UK GDPR, the UK SCCs will apply completed as follows:

(1) For so long as it is lawfully permitted to rely on UK SCCs for the transfer of personal data to processors set out in the European Commission's Decision 2010/87/EU of 5 February 2010 ("UK SCCs") for transfers of personal data from the United Kingdom, the UK SCCs shall apply between the Controller and the Processor on the following basis:

a. Appendix 1 shall be completed with the relevant information set out in Annex I;

b. Appendix 2 shall be completed with the relevant information set out in Annex II; and

c. the optional illustrative indemnification Clause will not apply.

(2) Where the Controller and the Processor are lawfully permitted to rely on the EU SCCs for transfers of personal data from the United Kingdom subject to completion of a "UK Addendum to the EU SCCs" ("UK Addendum") issued by the Information Commissioner's Office under s.119A(1) of the Data Protection Act 2018, then:

a. The EU SCCs, completed as set out above shall also apply to transfers of such Data, subject to sub-section (b) below;

b. The UK Addendum shall be deemed executed between the transferring Controller and the Processor, and the EU SCCs shall be deemed amended as specified by the UK Addendum in respect of the transfer of such Controller Data.

(3) If neither section above applies, then the Controller and the Processor shall cooperate in good faith to implement appropriate safeguards for transfers of such Personal Data as required or permitted by the UK GDPR without undue delay.

(4) In the event that any provision of an underlying agreement contradicts, directly or indirectly, the UK SCCs, the UK SCCs shall prevail.

Annex 1 - DATA PROCESSING details

This Annex I forms part of the SCCs and describes the processing that the Processor will perform on behalf of the Controller.

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*]

1.	Name:	See Agreement
	Address:	See Agreement
	Contact person's name, position and contact details:	See Agreement
	Activities relevant to the data transferred under these Clauses:	The Controller is a customer of Processor's that will provide Personal Data to Processor in order to allow Processor to provide services to Controller pursuant to a services agreement entered by and between the parties.
	Signature and date:	*The parties agree that these Standard Contractual Clauses are effective as of the underlying Agreement Date*
	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*]

1.	Name:	Beamery Inc.
	Address:	340 S Lemon Ave #9358, Walnut, CA 91789
	Contact person's name, position and contact details:	Beamery DPO, privacy@beamery.com
	Activities relevant to the data transferred under these Clauses:	The processing activities that are necessary in order to provide Beamery's SaaS and other services to the Controller, which shall include hosting, storage, providing customer service, implementation of the SaaS, resume parsing, and performance analytics.
	Signature and date:	*The parties agree that these Standard Contractual Clauses are effective as of the underlying Agreement Date*
	Role (controller/processor):	Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred:	● Controller's or its Affiliates' Authorized Users – being the individuals who use the Subscription Service;

	● Controller's or its Affiliates' representatives who are involved in the receipt of Services; and ● Contacts who are interested in employment with the Controller or its Affiliates or who are approached by the Controller, its Affiliates or their Authorized Users and get in contact via the Subscription Service.
Categories of personal data transferred:	The Personal Data transferred to Processor is determined and controlled by the Controller in its sole discretion. Anticipated categories: First and last name ● Business contact information (company, email, phone, business address) ● Personal contact information (email, phone, address) ● Employment information (title, position, employer, professional life data (including employment history) ● ID data ● Personal life data ● Connection data ● Localization data ● Technical usage and telecommunications data as well as telecommunications metadata (e.g. IP address, browser history, information regarding the used devices, operating system and browser) ● 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 qualification.
Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures:	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, vaccination status, sexual orientation.
The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis):	Personal data will be transferred continuously throughout the Term of the Agreement.

Nature of the processing:	Supplier is a provider of web-based candidate relationship management and marketing applications, tools, platform and associated Professional Services. These services consist primarily of the provision of Supplier's Subscription Service that enables the Controller to manage its talent acquisition and CRM recruitment efforts, including developing and managing relationships with Contacts (in the Controller's sole discretion). Supplier will also provide a number of associated services to the Controller in connection with the Subscription Service, including Professional Services and other Services.
Purpose(s) of the data transfer and further processing:	The data processing undertaken by Supplier will involve any such processing that is necessary for the purposes set out in the Agreement, any subsequent Addenda, 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 Controller or by the Processor at the Controller's instruction.
For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing:	Personal data is transferred to the Processor's sub-processors for the purpose of providing the Processor's Services to the Controller for the duration of the Agreement, unless the personal data is deleted prior to the termination or expiration of that contract by the Controller or by the Processor at the Controller's instruction.

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance (e.g. in accordance with Clause 13 SCCs)	**Germany**

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.

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 Processor'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 Processor to investigate,

	respond to, mitigate and notify of events related to Processor'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 Processor's organisation, monitoring and maintaining compliance with Processor'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 Processor'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 Processor'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 center, 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 Processor 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 Processor'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 Processor'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 Processor's information security program.
Measures for ensuring data minimisation	Not applicable to Processor. Processor is processing the Personal Data on behalf of the Controller for the sole purpose of providing services to the Processor for the duration of the services agreement entered into between the Processor and the Controller. The Controller 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 Processor. Processor is processing the Personal Data on behalf of the Controller for the sole purpose of providing services to the Processor for the duration of the services agreement entered into between the Processor and the Controller. The Processor does not have the ability to monitor the quality of the Personal Data.
Measures for ensuring limited data retention	The Controller 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 Agreement. All Personal Data in the Controller's account is automatically deleted ninety (90) days following expiration or termination of the services agreement entered into between the Controller and Processor, or earlier upon request, subject to the Processor's standard 30 day backup schedule.
Measures for ensuring accountability	The Processor takes responsibility for complying with the EU GDPR and the UK GDPR, at the highest management level and throughout our organisation. The Processor keeps evidence of the steps taken to comply with the EU GDPR and the UK GDPR. The Processor 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. We review and update our accountability measures at appropriate intervals.
Measures for allowing data portability and ensuring erasure	Controller's data can be exported in CSV format at any time. Controller's 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).

[redacted]

Processor Self-Service Features	At all times during the term of the underlying services Agreement, the Controller 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 Controller will automatically be reflected in Supplier's databases as well.