DATA PROCESSING AGREEMENT

This Data Processing Addendum ("**DPA**") is between the customer ("**Customer**" or "**Controller**") and Beamery or its Affiliates (as applicable "**Supplier**" or "**Processor**") and supplements the Beamery Master Services Agreement available at https://beamery.com/terms-and-conditions, as updated from time to time, or any other agreement between Customer and Beamery governing Customer's use of the Beamery Services (the "**Agreement**"). This DPA is effective as of the effective date of the Agreement.

1. DEFINITIONS

1.1 **Controller**, **Processor**, **Data Subject**, **Personal Data** and **Processing** (and **Process**) shall have the meanings given in EU/UK Data Protection Law and the material equivalent under other applicable Data Protection Law;

1.2 **Data Protection Law** means all worldwide data protection and privacy laws and regulations, to the extent applicable to the parties and the nature of the personal data processed under the Agreement, including, where applicable, (a) EU/UK Data Protection Law; and (b) the California Consumer Privacy Act (the "**CCPA**");

1.3 **EU/UK Data Protection Law** means: (a) Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the Processing of Personal Data and on the free movement of such data (General Data Protection Regulation) (the "**EU GDPR**"); (b) the EU GDPR as saved into United Kingdom law by virtue of section 3 of the United Kingdom's European Union (Withdrawal) Act 2018 (the "**UK GDPR**"); (c) the EU e-Privacy Directive (Directive 2002/58/EC); and (d) any and all applicable national data protection laws made under, pursuant to or that apply in conjunction with any of (a), (b) or (c); in each case as may be amended or superseded from time to time;

1.4 **Restricted Transfer** means: (a) where the EU GDPR applies, a transfer of personal data from the European Economic Area to a country outside of the European Economic Area which is not subject to an adequacy determination by the European Commission; and (b) where the UK GDPR applies, a transfer of Personal Data from the United Kingdom to any other country which is not based on adequacy regulations pursuant to Section 17A of the United Kingdom Data Protection Act 2018; and

1.5 **Standard Contractual Clauses** means: (a) where the EU GDPR applies, 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**"); and (b) where the UK GDPR applies, standard data protection clauses adopted pursuant to or permitted under Article 46 of the UK GDPR ("**UK SCCs**") (collectively and as applicable the "**SCCs**").

2. PERSONAL DATA PROCESSING

2.1 Supplier shall process Personal Data on the Customer's behalf to perform its obligations under this Agreement and, as such, the Customer is the Controller and Supplier is the Processor for the purposes of the Data Protection Law.

2.2 Annex 1 sets out the details of the data processing to be undertaken by Supplier.

2.3 The Personal Data processed on behalf of the Customer by Supplier pursuant to this Agreement may be transferred or stored outside the EEA or the country where the Customer and the Authorized Users are located as necessarily required in order to carry out Supplier's obligations under this Agreement.

2.4 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 SCCs is inaccurate or outdated. Nonetheless, if Supplier becomes aware that Customer Data transferred under the SCCs 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 SCCs by providing the tools within the Services so that Customer can use it to erase or rectify Customer Data.

2.5 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:

3.2 Process Personal Data only for the purpose of fulfilling the terms of the Agreement in place between the Controller and the Processor. In no event shall the Processor use any of this Personal Data for its own purposes or for any other purpose other than the specific purpose which the use of such Personal Data has been authorized by the Controller. Processor shall not sell any Personal Data or Personal Information for purposes of CCPA.

3.3 Process Personal Data on the documented instructions of the Controller, including with regards to any transfer of data to third countries or international organizations unless required to do so by Union or Member State law to which the Processor shall inform the Controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest.

3.4 Ensure that any person acting under the authority of the Processor, who has access to Personal Data, is subject to a duty of confidentiality and that such individual's process such data in accordance with the Processors instructions only.

3.5 At all times, taking into account the nature of the processing, implement technical and organizational measures appropriate to the level of risk that shall provide:

a) The ability to ensure the ongoing confidentiality, integrity, availability, and resilience of processing systems and services,

b) Security against unauthorized or unlawful processing, access, disclosure, copying, modification, storage, reproduction, display or distribution of Personal Data,

c) The ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident,

d) A process for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

3.6 Ensure that the security of Personal Data is protected by recognised industry standard policies and procedures (not less than set out in Section 4.1 of this DPA) and reliable, well-trained staff.

3.7 Ensure that each of its employees, agents, subcontractors, Sun-Processors or any other persons acting under the authority of the Processor are made aware of the Processors obligations and duties with regard to the confidentiality, integrity, and availability of the Personal Data and shall require that they enter into binding obligations with the Processor in order to maintain the levels of confidentiality, security, and protection.

3.8 Assist the Controller by technical and organizational measures for the fulfilment of the Controller's obligation to respond to requests for exercising the Data Subject's rights laid down in EU/UK Data Protection Law.

3.9 Assist the Controller in ensuring compliance with the Controllers obligations pursuant to EU/UK 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.

3.10 The Processor shall notify the Controller without undue delay (and in no case later than the statutory maximum for notification under applicable Data Protection Law), after confirmation of a Security Breach. The notification will, to the extent such information is available: (a) describe 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) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained; (c) describe the likely consequences of the Personal Data breach; (d) describe the measures taken or proposed to be taken by the controller 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 access to Customer Data or Personal Data or to any of Supplier's equipment or facilities storing Customer Data.

3.11 Make available to the Controller all information necessary to demonstrate compliance with Article 28 of the GDPR and allow for and contribute to audits (subject to Section 4.2 below).

3.12 The Processor shall without undue delay (and in no case later than the statutory maximum for notification under applicable Data Protection Law) notify the Controller if, in its opinion, it is asked to do something that infringes Data Protection Laws.

3.13 Maintain a record of all categories of processing activities carried out on behalf of the Controller that is compliant with the Data Protection Law.

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

3.15 At the choice of the Controller, delete or return all Personal Data to the Controller within 30 days after the end of the provision of services relating to the processing and delete existing copies within 90 days of termination of the Agreement unless Union or Member State law requires storage of the Personal Data. Certification of deletion of Personal Data shall be provided only upon request.

4. SECURITY MEASURES AND AUDITS

4.1 In providing the Services in addition to the security measures set out in Annex 2, Supplier shall ensure that it has in place appropriate technical and organizational measures to protect against unauthorized or unlawful processing of Personal Data and against accidental loss or destruction of, or damage to, Personal Data ("**Security Breach**"), appropriate to the harm that might result from the unauthorized or unlawful processing or accidental loss, destruction or damage and the nature of the data to be protected, having regard to the state of technological development and the cost of implementing any measures (those measures may include, where appropriate, pseudonymization and encrypting Personal Data, ensuring confidentiality, integrity, availability and resilience of its systems and services, ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of the technical and organizational measures adopted by it).

4.2 Upon Customer's request, and subject to the confidentiality obligations set forth in the Agreement, Supplier shall make available to information regarding the 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. To the extent that Customer is not satisfied with such demonstration of compliance, Supplier may allow for and contribute to audits, by any Customer or an auditor mandated

by any 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 Controller 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 during the course of an audit.

5. ONWARD TRANFERS

5.1 Processor shall not participate in (nor permit any Sub-Processor to participate in) any other Restricted Transfers of Data (whether as an exporter or an importer of the Data) unless the Restricted Transfer is made in full compliance with Applicable Data Protection Law. Such measures may include (without limitation) transferring the Data to a recipient in a country that the European Commission has decided provides adequate protection for Personal Data, to a recipient that has achieved binding corporate rules authorization in accordance with Applicable Data Protection Law, or pursuant to Standard Contractual Clauses implemented between the relevant exporter and importer of the Data.

6. PERSONAL DATA TRANSFERS

6.1 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, and the UK. The parties agree that when the transfer of Data from Controller to Processor is a Restricted Transfer it shall be subject to the appropriate SCCs and completed SCCs can be found at https://beamery.com/terms-and-conditions/.

6.2 **Transfers from the EEA**. In relation to Data that is protected by the EU GDPR, the EU SCCs will apply completed as follows:

a) Module Two will apply. 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).

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 7 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 sup-processor completed with the information set out in Annex 2 to this DPA.

6.3 **Transfers from Switzerland**. Where a Restricted Transfer is made from Switzerland, the EU SCCs are incorporated into this DPA and apply to the transfer as modified above, except that:

a) in Clause 13, the competent supervisory authority is the Swiss Federal Data Protection and Information Commissioner if the Restricted Transfer is governed by the Swiss Federal Act on Data Protection;

b) references to "Member State" in the EU SCCs refer to Switzerland, and Data Subjects located in Switzerland may exercise and enforce their rights under the EU SCCs in Switzerland; and

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

6.4 **Transfers from United Kingdom**. in relation to Data that is protected by the UK GDPR, Customer and Supplier are lawfully permitted to rely on the EU SCCs for transfers of Personal Data from the UK subject to the completion of a "UK Addendum to the EU Commission Standard Contractual Clauses" ("UK Addendum") issued by the UK Information Commissioner's Office, then:

a) the EU SCCs apply as modified above; and

b) the UK Addendum is deemed executed between Customer and Supplier and the EU SCCs is deemed amended as specified by the UK Addendum with respect to the applicable Personal Data.

6.5 **Specific application of the SCCs**. the following terms apply to the SCCs:

a) Customer may exercise its audit rights under the SCCs as set out in the DPA; and

b) Supplier may appoint Subprocessors under the SCCs as set out in the DPA; and

c) With respect to Restricted Transfers made to Supplier, Supplier may neither participate in, nor permit any Subprocessor to participate in, any further Restricted Transfer unless the further Restricted Transfer is made in full compliance with Data Protection Laws and in accordance with applicable SCCs or an alternative legally compliant transfer mechanism adopted by the importer.

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

7. SUB-PROCESSORS

7.1 The Customer provides general authorization to Supplier appointing each of the Sub-Processors set out at https://beamery.com/terms-and-conditions as third-party processors of Personal Data under this Agreement and as amended from time to time with prior written notices to Customer. With respect to each Subprocessor, Supplier shall: (a) before the Subprocessor first processes Customer Personal Data, carry out adequate due diligence to ensure that the Subprocessor is capable of providing the level of protection for Customer Personal Data required by the Agreement; (b) ensure that the arrangement between the Subprocessor, is governed by a written contract including terms which offer at least the same level of protection for Customer Personal Data as those set out in this DPA and meet the requirements of Article 28(3) of the GDPR; and (c) if that arrangement involves a Restricted Transfer, ensure that the Standard Contractual Clauses are at all relevant times incorporated into the Agreement.

7.2 Customer may reasonably object to Supplier's use of a new Sub-processor by notifying Supplier promptly in writing within fourteen (14) after receipt of Supplier's notice of an update to Sub-processors. In the event Customer objects to a new Sub-processor, Supplier will use reasonable efforts to make available to Customer a change in the Services or recommend a commercially reasonable change to Customer's configuration or use of the Services to avoid Processing of Personal Data by the objected-to new Subprocessor without unreasonably burdening Customer. Where such a change cannot be made within ninety (90) days from Supplier's receipt of Customer's notice of objection, notwithstanding anything in the Agreement, Customer may by written notice to Supplier with immediate effect terminate the Agreement to the extent that it relates to the Services which require the use of the proposed Subprocessor. Any objection by Customer to a new or alternative Enrichment Data providing Sub-Processor will prevent the provision of such Enrichment Data, and this shall not constitute a breach of the Agreement by Supplier.

7.3 As between the Customer and Supplier, Supplier shall remain liable for all acts or omissions of all Sub-Processors appointed by it pursuant to this Agreement to the same extent Supplier would be liable if performing the services of each Sub-processor directly under the terms of this DPA, except as otherwise set forth in the Agreement.

8. DATA SUBJECT RIGHTS

8.1 Supplier shall assist Customer by appropriate technical and organizational measures in the fulfilment of Customer's obligation to respond to a Data Subject request under Data Protection Law. If a Data Subject makes a request to Supplier, Supplier will promptly forward such request to Customer. Customer authorises Supplier to respond to any Data Subject who makes a request to Supplier, to confirm that Supplier has forwarded the request to Customer. To the extent Customer does not have the ability to address a Data Subject request directly in the Services, Supplier shall upon Customer's request provide commercially reasonable efforts to assist Customer in responding to such Data Subject request, to the extent Supplier is legally permitted to do so and the response to such Data Subject request is required under Data Protection Laws.

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 Processor receives a legally binding request to access Personal Data from a Public Authority, 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. Processor shall not disclose Personal Data in a massive, disproportionate, and indiscriminate manner that goes beyond what is necessary in a democratic society. Processor 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.

Beamery

ANNEX 1 - DATA PROCESSING DETAILS

This Annex I forms part of the DPA 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*]

Name:	As set out in the applicable Order
Address:	As set out in the applicable Order
Contact person's name, position and contact details:	As set out in the applicable Order
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 the Agreement.
Signature and date:	*The parties agree this DPA is effective as of the underlying Agreement Effective 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*]

Name:	Beamery Inc.
Address:	340 S Lemon Ave #9358, Walnut, CA 91789
Contact person's name, position and contact details:	DPO, privacy@beamery.com
Activities relevant to the data transferred under these Clauses:	The processing activities that are necessary in order to provide Processor'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 this DPA is effective as of the underlying Agreement Effective Date*
Role (controller/processor):	Processor with respect to Customer Personal Data; Controller with respect to usage data

B. DESCRIPTION OF TRANSFER

Categories of Data Subjects whose personal data is transferred:	• Customer's or its Affiliates' Authorized Users – being the individuals who use the Subscription Service; • Customer's or its Affiliates' representatives who are involved in the receipt of Services; and • Contacts who are interested in employment with the Customer or its Affiliates or who are approached by the Customer, 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 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) • 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 specialized 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. Sensitive Data should be collected by the Controller on a data subject explicit consent basis.
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 Customer to manage its talent acquisition and CRM recruitment efforts, including developing and managing relationships with Contacts (in the Customer's sole discretion). Supplier will also provide a number of associated services to the Customer 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 Data Exporter or by the Data Importer at the Data Exporter's instruction. Data is deleted in accordance with NIST SP 800-88/DoD 5220.22-M standards.
For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing:	Personal data is transferred to the Data Importer's sub-processors for the purpose of providing the Data Importer's Services to the Data Exporter for the duration of the Agreement unless the personal data is deleted prior to the termination or expiration of that contract by the Data Exporter or by the Data Importer at the Data Exporter's instruction.

C. COMPETENT SUPERVISORY AUTHORITY

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

Beamery

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 Security and Privacy Centre at https://beamery.com/security. 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 Data Importer'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 Data Importer to investigate, respond to, mitigate and notify of events related to Data Importer'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 Data Importer's organisation, monitoring and maintaining compliance with Data Importer'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 Data Importer'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 Data Importer 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 Data Importer'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 Data Importer'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 Data Importer's information security program.
Measures for ensuring data minimisation	Not applicable to Data Importer. Data Importer is processing the Personal Data on behalf of the Data Exporter for the sole purpose of providing services to the Data Importer for the duration of the services agreement entered into between the Data Importer and the Data Exporter. The Data Exporter 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 Data Importer. Data Importer is processing the Personal Data on behalf of the Data Exporter for the sole purpose of providing services to the Data Importer for the duration of the services agreement entered into between the Data Importer and the Data Exporter. The Data Importer does not have the ability to monitor the quality of the Personal Data.
Measures for ensuring limited data retention	The Data Exporter 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 Data Exporter's account is automatically deleted ninety (90) days following expiration or termination of the services agreement entered into between the Data Exporter and Data Importer, or earlier upon request, subject to the Data Importer's standard 30 day backup schedule.
Measures for ensuring accountability	The Data Importer takes responsibility for complying with the EU GDPR and the UK GDPR, at the highest management level and throughout the organisation. The Data Importer keeps evidence of the steps taken to comply with the EU GDPR and the UK GDPR. The Data Importer 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 CSV 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
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.