ADDENDUM TO INCLUDE EU/UK STANDARD CONTRACTUAL CLAUSES
(where applicable)
MARCH 2022

TERMS OF THIS ADDENDUM:

1. This Addendum consists of the most recent version of the EU Standard Contractual Clauses and March 2022 UK ICO approved addendum to the SCCs (collectively the "**SCCs**"). The SCCs have been pre-signed by Beamery Inc. and its Affiliates as the data importer, per the signature on this page. The parties agree that the SCCs shall govern any data transfers by Beamery and its Affiliates as a Processor on behalf its Customer's as a Controller when the SCCs are deemed to be applicable to such transfers.

2. Complete the information in the signature box and sign below. Send the signed Addendum by email to privacy@beamery.com. Upon receipt of the validly completed Addendum at this email address, this Addendum will become legally binding. If you do not sign and return the attached by then, we will take your silence and continued processing of the personal data as your deemed acceptance of the SCCs and such terms shall apply to our processing of our Customer's personal data.

3. Signature below shall be deemed to constitute signature and acceptance of the Standard Contractual Clauses incorporated herein, including their Appendices. Where Customer wishes to separately execute the Standard Contractual Clauses and its Appendices, Customer should also complete the as the data exporter all sections highlighted in yellow.

On behalf of the Customer:

Name (written out in full): …

Position: …

Signature _____

On behalf of the Beamery and its Affiliates:

Name (written out in full): Nicolette Nowak

Position: Data Protection Officer

Signature Nicolette Nowak

EU STANDARD CONTRACTUAL CLAUSES

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 Addendum to EU SCCs

International Data Transfer Addendum to the EU Commission Standard Contractual Clauses. VERSION B1.0, in force 21 March 2022

This Addendum has been issued by the Information Commissioner for Parties making Restricted Transfers. The Information Commissioner considers that it provides Appropriate Safeguards for Restricted Transfers when it is entered into as a legally binding contract.

Part 1: Tables

Table 1: Parties

Start date	See Agreement	
The Parties	**Exporter (who sends the Restricted Transfer)**	**Importer (who receives the Restricted Transfer)**
Parties' details	Full legal name: See Annex 1 Trading name (if different): Main address (if a company registered address): See Annex 1 Official registration number (if any) (company number or similar identifier): See Annex 1	Full legal name: See Annex 1 Trading name (if different): Main address (if a company registered address): See Annex 1 Official registration number (if any) (company number or similar identifier): See Annex 1
Key Contact	Full Name (optional): Job Title: Contact details including email:	Full Name (optional): Job Title: Contact details including email:
Signature (if required for the purposes of Section 2)		See cover page

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs	☒ The version of the Approved EU SCCs which this Addendum is appended to, detailed below, including the Appendix Information: Date: Reference (if any): See above EU SCCs referenced Other identifier (if any): Or ☐ the Approved EU SCCs, including the Appendix Information and with only the following modules, clauses or optional provisions of the Approved EU SCCs brought into effect for the purposes of this Addendum:

Module	Module in operation	Clause 7 (Docking Clause)	Clause 11 (Option)	Clause 9a (Prior Authorisation or General Authorisation)	Clause 9a (Time period)	Is personal data received from the Importer combined with personal data collected by the Exporter?
1						
2						
3						
4						

Table 3: Appendix Information

"**Appendix Information**" means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this Addendum is set out in:

Annex 1A: List of Parties: See Annex 1

Annex 1B: Description of Transfer: See Annex 1

Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: Seen Annex 2

Annex III: List of Sub processors (Modules 2 and 3 only): 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

Table 4: Ending this Addendum when the Approved Addendum Changes

Ending this Addendum when the Approved Addendum changes	Which Parties may end this Addendum as set out in Section 19: ☒ Importer ☒ Exporter ☐ neither Party

Part 2: Mandatory Clauses

Entering into this Addendum

1. Each Party agrees to be bound by the terms and conditions set out in this Addendum, in exchange for the other Party also agreeing to be bound by this Addendum.

2. Although Annex 1A and Clause 7 of the Approved EU SCCs require signature by the Parties, for the purpose of making Restricted Transfers, the Parties may enter into this Addendum in any way that makes them legally binding on the Parties and allows data subjects to enforce their rights as set out in this Addendum. Entering into this Addendum will have the same effect as signing the Approved EU SCCs and any part of the Approved EU SCCs.

Interpretation of this Addendum

3. Where this Addendum uses terms that are defined in the Approved EU SCCs those terms shall have the same meaning as in the Approved EU SCCs. In addition, the following terms have the following meanings:

Addendum	This International Data Transfer Addendum which is made up of this Addendum incorporating the Addendum EU SCCs.
Addendum EU SCCs	The version(s) of the Approved EU SCCs which this Addendum is appended to, as set out in Table 2, including the Appendix Information.

Appendix Information	As set out in Table 3.
Appropriate Safeguards	The standard of protection over the personal data and of data subjects' rights, which is required by UK Data Protection Laws when you are making a Restricted Transfer relying on standard data protection clauses under Article 46(2)(d) UK GDPR.
Approved Addendum	The template Addendum issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18.
Approved EU SCCs	The Standard Contractual Clauses set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021.
ICO	The Information Commissioner.
Restricted Transfer	A transfer which is covered by Chapter V of the UK GDPR.
UK	The United Kingdom of Great Britain and Northern Ireland.
UK Data Protection Laws	All laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018.
UK GDPR	As defined in section 3 of the Data Protection Act 2018.

4. This Addendum must always be interpreted in a manner that is consistent with UK Data Protection Laws and so that it fulfils the Parties' obligation to provide the Appropriate Safeguards.

5. If the provisions included in the Addendum EU SCCs amend the Approved SCCs in any way which is not permitted under the Approved EU SCCs or the Approved Addendum, such amendment(s) will not be incorporated in this Addendum and the equivalent provision of the Approved EU SCCs will take their place.

6. If there is any inconsistency or conflict between UK Data Protection Laws and this Addendum, UK Data Protection Laws applies.

7. If the meaning of this Addendum is unclear or there is more than one meaning, the meaning which most closely aligns with UK Data Protection Laws applies.

8. Any references to legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, re-enacted and/or replaced after this Addendum has been entered into.

Hierarchy

9. Although Clause 5 of the Approved EU SCCs sets out that the Approved EU SCCs prevail over all related agreements between the parties, the parties agree that, for Restricted Transfers, the hierarchy in Section 10 will prevail.

10. Where there is any inconsistency or conflict between the Approved Addendum and the Addendum EU SCCs (as applicable), the Approved Addendum overrides the Addendum EU SCCs, except where (and in so far as) the inconsistent or conflicting terms of the Addendum EU SCCs provides greater protection for data subjects, in which case those terms will override the Approved Addendum.

11. Where this Addendum incorporates Addendum EU SCCs which have been entered into to protect transfers subject to the General Data Protection Regulation (EU) 2016/679 then the Parties acknowledge that nothing in this Addendum impacts those Addendum EU SCCs.

Incorporation of and changes to the EU SCCs

12. This Addendum incorporates the Addendum EU SCCs which are amended to the extent necessary so that:

    a. together they operate for data transfers made by the data exporter to the data importer, to the extent that UK Data Protection Laws apply to the data exporter's processing when making that data transfer, and they provide Appropriate Safeguards for those data transfers;

    b. Sections 9 to 11 override Clause 5 (Hierarchy) of the Addendum EU SCCs; and

c. this Addendum (including the Addendum EU SCCs incorporated into it) is (1) governed by the laws of England and Wales and (2) any dispute arising from it is resolved by the courts of England and Wales, in each case unless the laws and/or courts of Scotland or Northern Ireland have been expressly selected by the Parties.

13. Unless the Parties have agreed alternative amendments which meet the requirements of Section 12, the provisions of Section 15 will apply.

14. No amendments to the Approved EU SCCs other than to meet the requirements of Section 12 may be made.

15. The following amendments to the Addendum EU SCCs (for the purpose of Section 12) are made:

a. References to the "Clauses" means this Addendum, incorporating the Addendum EU SCCs;

b. In Clause 2, delete the words:

> "and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679";

c. Clause 6 (Description of the transfer(s)) is replaced with:

> "The details of the transfers(s) and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred) are those specified in Annex I.B where UK Data Protection Laws apply to the data exporter's processing when making that transfer.";

d. Clause 8.7(i) of Module 1 is replaced with:

> "it is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer";

e. Clause 8.8(i) of Modules 2 and 3 is replaced with:

> "the onward transfer is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer;"

f. References to "Regulation (EU) 2016/679", "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 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)" and "that Regulation" are all replaced by "UK Data Protection Laws". References to specific Article(s) of "Regulation (EU) 2016/679" are replaced with the equivalent Article or Section of UK Data Protection Laws;

g. References to Regulation (EU) 2018/1725 are removed;

h. References to the "European Union", "Union", "EU", "EU Member State", "Member State" and "EU or Member State" are all replaced with the "UK";

i. The reference to "Clause 12(c)(i)" at Clause 10(b)(i) of Module one, is replaced with "Clause 11(c)(i)";

j. Clause 13(a) and Part C of Annex I are not used;

k. The "competent supervisory authority" and "supervisory authority" are both replaced with the "Information Commissioner";

l. In Clause 16(e), subsection (i) is replaced with:

> "the Secretary of State makes regulations pursuant to Section 17A of the Data Protection Act 2018 that cover the transfer of personal data to which these clauses apply;";

m. Clause 17 is replaced with:

> "These Clauses are governed by the laws of England and Wales.";

n. Clause 18 is replaced with:

> "Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts."; and

o. The footnotes to the Approved EU SCCs do not form part of the Addendum, except for footnotes 8, 9, 10 and 11.

Amendments to this Addendum

16. The Parties may agree to change Clauses 17 and/or 18 of the Addendum EU SCCs to refer to the laws and/or courts of Scotland or Northern Ireland.

17. If the Parties wish to change the format of the information included in Part 1: Tables of the Approved Addendum, they may do so by agreeing to the change in writing, provided that the change does not reduce the Appropriate Safeguards.

18. From time to time, the ICO may issue a revised Approved Addendum which:

    a. makes reasonable and proportionate changes to the Approved Addendum, including correcting errors in the Approved Addendum; and/or
    b. reflects changes to UK Data Protection Laws;

The revised Approved Addendum will specify the start date from which the changes to the Approved Addendum are effective and whether the Parties need to review this Addendum including the Appendix Information. This Addendum is automatically amended as set out in the revised Approved Addendum from the start date specified.

19. If the ICO issues a revised Approved Addendum under Section 18, if any Party selected in Table 4 "Ending the Addendum when the Approved Addendum changes", will as a direct result of the changes in the Approved Addendum have a substantial, disproportionate and demonstrable increase in:

    a its direct costs of performing its obligations under the Addendum; and/or

    b its risk under the Addendum,

    and in either case it has first taken reasonable steps to reduce those costs or risks so that it is not substantial and disproportionate, then that Party may end this Addendum at the end of a reasonable notice period, by providing written notice for that period to the other Party before the start date of the revised Approved Addendum.

20. The Parties do not need the consent of any third party to make changes to this Addendum, but any changes must be made in accordance with its terms.

Alternative Part 2 Mandatory Clauses:

Mandatory Clauses	Part 2: Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18 of those Mandatory Clauses.

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:	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 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, which 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 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.

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 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	Incident / problem management procedures designed to allow Processor to investigate,

in a timely manner in the event of a physical or technical incident	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).

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.

HELLOSIGN

Audit trail

TITLE	Beamery_SCCs_Website_March2022
FILE NAME	Beamery_SCCs_Website_March2022.docx
DOCUMENT ID	2d04351abd2947ea5acd8139494497c26b7bb334
AUDIT TRAIL DATE FORMAT	DD / MM / YYYY
STATUS	● Signed

Document history

SENT	**14 / 03 / 2022** 13:23:29 UTC	Sent for signature to Nicolette Nowak (nicolette.nowak@beamery.com) from legal@beamery.com IP: 77.102.16.104
VIEWED	**14 / 03 / 2022** 13:25:23 UTC	Viewed by Nicolette Nowak (nicolette.nowak@beamery.com) IP: 51.198.41.36
SIGNED	**14 / 03 / 2022** 13:26:46 UTC	Signed by Nicolette Nowak (nicolette.nowak@beamery.com) IP: 51.198.41.36
COMPLETED	**14 / 03 / 2022** 13:26:46 UTC	The document has been completed.