VOCAL VIDEO
DATA PROCESSING ADDENDUM

This Data Processing Addendum ("**DPA**") supplements the Vocal Video Terms of Service available at https://vocalvideo.com/tos, as updated from time to time, or other agreement between Customer and Vocal Video governing Customer's use of the Vocal Video Services (the "**Agreement**") when the GDPR applies to your use of the Vocal Video Services to process Customer Data. This DPA is an agreement between you and the entity you represent ("**Customer**", "**you**", or "**your**") and Vocal Video Inc., a California corporation ("**Vocal Video**"). Unless otherwise defined in this DPA or in the Agreement, all capitalized terms used in this DPA will have the meanings given to them in Section 14 ("Definitions") of this DPA.

1) **Data Processing**

   a) **Scope and Roles.** This DPA applies when Customer Data is processed by Vocal Video. In this context, Vocal Video will act as processor to Customer, who will act as controller of Customer Data.

   b) **Customer Controls.** Customer can use the Account Controls to assist it with its obligations under the GDPR, including its obligations to respond to requests from data subjects. Considering the nature of the processing, Customer agrees that it is unlikely that Vocal Video would become aware that Customer Data transferred under the Standard Contractual Clauses is inaccurate or outdated. Nonetheless, if Vocal Video becomes aware that Customer Data transferred under the Standard Contractual Clauses is inaccurate or outdated, it will inform Customer without undue delay. Vocal Video will cooperate with Customer to erase or rectify inaccurate or outdated Customer Data transferred under the Standard Contractual Clauses by providing the Account Controls that Customer can use to erase or rectify Customer Data.

   c) **Details of Data Processing**

      i) **Subject Matter.** The subject matter of the data processing under this DPA is Customer Data.

      ii) **Duration.** As between Vocal Video and Customer, the duration of the data processing under this DPA is determined by Customer.

      iii) **Purpose.** The purpose of the data processing under this DPA is the provision of the Services initiated by Customer from time to time.

      iv) **Nature of the Processing.** Video or audio collection, video production, video hosting and such other Services as described in the Terms of Service and initiated by Customer from time to time.

      v) **Type of Customer Data.** Customer Data uploaded to the Services under Customer's Vocal Video account or provided by Customer's Respondents (as defined in the Terms of Service).

      vi) **Categories of data subjects.** The data subjects could include Customer's customers, reviewers, employees, or other respondents.

   d) **Compliance with Laws**. Each party will comply with all laws, rules, and regulations applicable to it and binding on it in the performance of this DPA, including the GDPR.

2) **Customer Instructions.** The parties agree that this DPA and the Agreement constitute Customer's

documented instructions regarding Vocal Video's processing of Customer Data ("**Documented Instructions**"). Vocal Video will process Customer Data only in accordance with Documented Instructions. Additional instructions outside the scope of the Documented Instructions (if any) require prior written agreement between Vocal Video and Customer, including agreement on any additional fees payable by Customer to Vocal Video for carrying out such instructions. Customer is entitled to terminate this DPA and the Agreement if Vocal Video declines to follow instructions requested by Customer that are outside the scope of, or changed from, those given or agreed to be given in this DPA. Considering the nature of the processing, Customer agrees that it is unlikely Vocal Video can form an opinion on whether Documented Instructions infringe the GDPR. If Vocal Video forms such an opinion, it will immediately inform Customer, in which case, Customer is entitled to withdraw or modify its Documented Instructions.

3) **Confidentiality of Customer Data.** Vocal Video will not access or use, or disclose to any third party any Customer Data, except, in each case, as necessary to maintain or provide the Services, or as necessary to comply with the law or a valid and binding order of a governmental body (such as a subpoena or court order). If a governmental body sends Vocal Video a demand for Customer Data, Vocal Video will attempt to redirect the governmental body to request that data directly from Customer. As part of this effort, Vocal Video may provide Customer's basic contact information to the governmental body. If compelled to disclose Customer Data to a governmental body, then Vocal Video will give Customer reasonable notice of the demand to allow Customer to seek a protective order or other appropriate remedy unless Vocal Video is legally prohibited from doing so.

4) **Confidentiality Obligations of Vocal Video Personnel.** Vocal Video restricts its personnel from processing Customer Data without authorization by Vocal Video as described in the Vocal Video Security Standards. Vocal Video imposes appropriate contractual obligations upon its personnel, including relevant obligations regarding confidentiality, data protection, and data security.

5) **Security of Data Processing**

    a) Vocal Video has implemented and will maintain the technical and organizational measures for its network as described in the Vocal Video Security Standards and this section. In particular, Vocal Video has implemented and will maintain the following technical and organizational measures:

        i) security of its network as set out in Section 1.a of the Vocal Video Security Standards;

        ii) physical security of the facilities as set out in Section 1.b of the Vocal Video Security Standards;

        iii) measures to control access rights for Vocal Video employees and contractors to its network as set out in Section 1.a of the Vocal Video Security Standards;

        iv) processes for regularly testing, assessing, and evaluating the effectiveness of the technical and organizational measures implemented by Vocal Video as described in Section 2 of the Vocal Video Security Standards;

        v) measures to ensure the ongoing confidentiality, integrity, availability, and resilience of the processing systems and services that are operated by Customer;

        vi) measures to backup and archive appropriately in order to restore availability and access to Customer Data in a timely manner in the event of a physical or technical incident; and

        vii) encryption to ensure an appropriate level of security for Customer data inflight and at rest.

6) **Sub-Processing**

    a) **Authorized Sub-Processors.** Customer provides general authorization to Vocal Video's use of sub-processors to provide processing activities on Customer Data on behalf of Customer ("**Sub-Processors**") in accordance with this section. Vocal Video currently uses the following

Sub-Processors:

Service Provider	Location	Processing Activity
Amazon Web Services, Inc.	USA	Web hosting
EngineYard Enterprises, Inc.	USA	Developer operations
Stripe, Inc.	USA	Payment processing
HelpScout, Inc.	USA	Customer support
Functional Software, Inc. dba Sentry.io	USA	Error and performance monitoring
Mailgun Technologies, Inc.	USA	Email
Convertkit LLC	USA	Email

At least thirty (30) days before Vocal Video engages a Sub-Processor, Vocal Video will update the applicable website. To object to a Sub-Processor, Customer can: (i) terminate the Agreement pursuant to its terms; or (ii) cease using the Service for which Vocal Video has engaged the Sub-Processor.

b) **Sub-Processor Obligations.** Where Vocal Video authorizes a Sub-Processor as described in Section 6(a):

i) Vocal Video will restrict the Sub-Processor's access to Customer Data only to what is necessary to provide or maintain the Services in accordance with the Terms of Service, and Vocal Video will prohibit the Sub-Processor from accessing Customer Data for any other purpose;

ii) Vocal Video will enter into a written agreement with the Sub-Processor and, to the extent that the Sub-Processor performs the same data processing services provided by Vocal Video under this DPA, Vocal Video will impose on the Sub-Processor the same contractual obligations that Vocal Video has under this DPA; and

iii) Vocal Video will remain responsible for its compliance with the obligations of this DPA and for any acts or omissions of the Sub-Processor that cause Vocal Video to breach any of Vocal Video's obligations under this DPA.

7) **Vocal Video Assistance with Data Subject Requests.** Considering the nature of the processing, the Account Controls are the technical and organizational measures by which Vocal Video will assist Customer in fulfilling Customer's obligations to respond to data subjects' requests under the GDPR. If a data subject makes a request to Vocal Video, Vocal Video will promptly forward such request to Customer once Vocal Video has identified that the request is from a data subject for whom Customer is responsible. Customer authorizes on its behalf Vocal Video to respond to any data subject who makes a request to Vocal Video, to confirm that Vocal Video has forwarded the request to Customer. The parties agree that Customer's use of the Account Controls and Vocal Video forwarding data subjects' requests to Customer in accordance with this section, represent the scope and extent of Customer's required assistance.

8) **Security Incident Notification**

a) **Security Incident.** Vocal Video will (i) notify Customer of a Security Incident without undue delay after becoming aware of the Security Incident, and (ii) take appropriate measures to address the Security Incident, including measures to mitigate any adverse effects resulting from the Security

Incident.

b) **Vocal Video Assistance.** To enable Customer to notify a Security Incident to supervisory authorities or data subjects (as applicable), Vocal Video will cooperate with and assist Customer by including in the notification under Section 8(a)(i) such information about the Security Incident as Vocal Video is able to disclose to Customer, considering the nature of the processing, the information available to Vocal Video, and any restrictions on disclosing the information, such as confidentiality. Considering the nature of the processing, Customer agrees that it is best able to determine the likely consequences of a Security Incident.

c) **Unsuccessful Security Incidents.** Customer agrees that:

i) 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 to any of Vocal Video's equipment or facilities storing Customer Data, and could include, without limitation, pings and other broadcast attacks, unsuccessful log-on attempts, denial of service attacks, or similar incidents; and

ii) Vocal Video's obligation to report or respond to a Security Incident under this section is not and will not be construed as an acknowledgement by Vocal Video of any fault or liability of Vocal Video with respect to the Security Incident.

d) **Communication.** Notification(s) of Security Incidents, if any, will be delivered to one (1) or more of Customer's administrators by any means Vocal Video selects, including via email. It is Customer's sole responsibility to ensure Customer's administrators maintain accurate contact information with Vocal Video at all times.

9) **Transfers of Personal Data**

a) **Regions.** Vocal Video will transfer Customer Data from the region in which Customer is located as necessary to provide the Services initiated by Customer, or as necessary to comply with the law or binding order of a governmental body. Your information collected through our website will be stored and processed in the United States.

b) **Application of Standard Contractual Clauses.** Subject to Section 9(c), the Standard Contractual Clauses will only apply to Customer Data that is transferred, either directly or via onward transfer, to any Third Country, (each a "**Data Transfer**").

i) Since the Customer is acting as a controller, the Controller-to-Processor Clauses will apply to a Data Transfer.

c) **Alternative Transfer Mechanism.** The Standard Contractual Clauses will not apply to a Data Transfer if Vocal Video has adopted Binding Corporate Rules for Processors or an alternative recognized compliance standard for lawful Data Transfers.

10) **Termination of the DPA.** This DPA will continue in force until the termination of the Agreement (the "**Termination Date**").

11) **Deletion of Customer Data**. At any time up to the Termination Date, Vocal Video will delete all Customer Data upon Customer request. Thirty (30) days following the Termination Date, subject to the terms and conditions of the Agreement, Vocal Video will delete Customer Data.

12) **Duties to Inform.** If any Customer Data should become subject to confiscation during bankruptcy or insolvency proceedings, or similar measures by third parties while being processed by Vocal Video,

Vocal Video will inform Customer without undue delay. Vocal Video will, without undue delay, notify all relevant parties in such action (for example, creditors, bankruptcy trustee) that any Customer Data subjected to those proceedings is Customer's property and area of responsibility and that Customer Data is at Customer's sole disposition.

13) **Entire Agreement; Conflict**. This DPA incorporates the Standard Contractual Clauses by reference. Except as amended by this DPA, the Agreement will remain in full force and effect. If there is a conflict between the Agreement and this DPA, the terms of this DPA will control, except that the Agreement will control over this DPA. Nothing in this document varies or modifies the Standard Contractual Clauses.

14) **Definitions.** Unless otherwise defined in the Agreement, all capitalized terms used in this DPA will have the meanings given to them below:

"Account Controls" means the controls, including video visibility settings, video and audio response deletion, and published video deletion features that the Services provide, as described in the Terms of Service.

The term "**controller**" shall have the meaning given to such term in the GDPR.

"**Controller-to-Processor Clauses**" means the standard contractual clauses between controllers and processors for Data Transfers, as approved by the European Commission Implementing Decision (EU) 2021/914 of June 4, 2021, attached hereto as Exhibit B.

"**Customer Data**" means the "personal data" (as defined in the GDPR) that is uploaded to the Services through or on behalf of Customer's Vocal Video accounts or provided by Customer's Respondents directly.

"**EEA**" means the European Economic Area.

"**GDPR**" means Regulation 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, and repealing Directive 95/46/EC (General Data Protection Regulation).

The term "**processing**" shall have the meaning given to such term in the GDPR and "process", "processes" and "processed" will be interpreted accordingly.

The term "**processor**" shall have the meaning given to such term in the GDPR.

"Security Incident" means a breach of Vocal Video's security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Data.

"Standard Contractual Clauses" means the Controller-to-Processor Clauses.

"Third Country" means a country outside the EEA not recognized by the European Commission as providing an adequate level of protection for personal data (as described in the GDPR).

"**Vocal Video Network**" means Vocal Video's hardware, servers, facilities, networking equipment, and other systems that are within Vocal Video's control and are used to provide the Services.

"**Vocal Video Security Standards**" means the security standards attached to the Agreement, or if none are attached to the Agreement, attached to this DPA as Exhibit A.

Exhibit A

Vocal Video Security Standards

Capitalized terms not otherwise defined in this document have the meanings assigned to them in the Agreement.

1) **Information Security Program.** Vocal Video will maintain an information security program (including the adoption and enforcement of internal policies and procedures) designed to (a) help Customer secure Customer Data against accidental or unlawful loss, access, or disclosure, (b) identify reasonably foreseeable and internal risks to security and unauthorized access to the network, and (c) minimize security risks, including through risk assessment and regular testing. Vocal Video will designate at least one (1) employee to coordinate and be accountable for the information security program. The information security program will include the following measures:

    a) **Network Security.** Vocal Video's network will be electronically accessible to employees, contractors, and any other person as necessary to provide the Services. Vocal Video will maintain access controls and policies to manage what access is allowed to the network from each network connection and user, including the use of firewalls or functionally equivalent technology and authentication controls. Vocal Video will maintain corrective action and incident response plans to respond to potential security threats.

    b) **Physical Security**

        i) **Physical Access Controls.** Physical components of the network are housed in nondescript facilities (the "**Facilities**"). Physical barrier controls are used to prevent unauthorized entrance to the Facilities both at the perimeter and at building access points. Passage through the physical barriers at the Facilities requires either electronic access control validation (for example, card access systems, etc.) or validation by human security personnel (for example, contract or in-house security guard service, receptionist, etc.). Employees and certain contractors are assigned photo-ID badges that must be worn while the employees and contractors are at any of the Facilities. Visitors and any other contractors are required to sign-in with designated personnel, must show appropriate identification, are assigned a visitor ID badge that must be worn while the visitor or contractor is at any of the Facilities, and are continually escorted by authorized employees or contractors while visiting the Facilities.

        ii) **Limited Employee and Contractor Access.** Vocal Video provides access to the Facilities to those employees and contractors who have a legitimate business need for such access privileges. When an employee or contractor no longer has a business need for the access privileges assigned to them, the access privileges are promptly revoked, even if the employee or contractor continues to be an employee of Vocal Video or its affiliates.

        iii) **Physical Security Protections.** All access points (other than main entry doors) are maintained in a secured (locked) state. All physical access to the Facilities by employees and contractors is logged and routinely audited.

2) **Continued Evaluation**. Vocal Video will conduct periodic reviews of the security of its network and adequacy of its information security program as measured against industry security standards and its policies and procedures. Vocal Video will continually evaluate the security of its network and associated Services to determine whether additional or different security measures are required to respond to new security risks or findings generated by the periodic reviews.

Exhibit B

Controller-to-Processor Clauses

Standard Contractual Clauses
Controller-to-Processor Transfers

This attachment is attached to and forms part of the Vocal Video Data Processing Addendum (DPA). Unless otherwise defined in this attachment, capitalised terms used in this attachment have the meanings given to them in the DPA.

SECTION I

Clause 1
Purpose and scope

a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of 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)[1] for the transfer of personal data to a third country.

b) The Parties:

   i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter "entity/ies") transferring the personal data, as listed in Annex I.A. (hereinafter each "data exporter"), and

   ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A. (hereinafter each "data importer")

   iii) have agreed to these standard contractual clauses (hereinafter: "Clauses").

c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

---

[1] Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295 of 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the Standard Contractual Clauses included in Decision 2021/915.

Clause 2

Effect and invariability of the Clauses

a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 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, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

   i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

   ii) Clause 8.1(b), 8.9(a), (c), (d) and (e);

   iii) Clause 9(a), (c), (d) and (e);

   iv) Clause 12(a), (d) and (f);

   v) Clause 13;

   vi) Clause 15.1(c), (d) and (e);

   vii) Clause 16(e);

   viii) Clause 18(a) and (b).

b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7 - Optional

Not used

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data 4 importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter "personal data breach"). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(a) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the

information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(b) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter "sensitive data"), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (in the same country as the data importer or in another third country, hereinafter "onward transfer") if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 of Regulation (EU) 2016/679 with respect to the processing in question;

iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 **Documentation and compliance**

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

(a) The data importer has the data exporter's general authorisation for the engagement of subprocessor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of subprocessors at least 30 days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects.[2] The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a subprocessor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third -party beneficiary clause with the sub-processor whereby - in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent - the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set

[2] This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11

Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its / their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

(a) Where the data exporter is established in an EU Member State: The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679: The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority. Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679: The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

(c) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clause

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards [3];

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these

---

[3] As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative timeframe. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimization

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a 11 reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of the Grand Duchy of Luxembourg.

Clause 18

Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of the district of Luxembourg City.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

ANNEX I

A. **LIST OF PARTIES**

Data exporter(s):

Name: The entity identified as “Customer” in the Addendum.

Address: The address for Customer associated with its Vocal Video account or as otherwise specified in the Addendum or the Agreement.

Contact person’s name, position and contact details: The contact details associated with Customer’s account, or as otherwise specified in the Addendum or the Agreement.

Activities relevant to the data transferred under these Clauses: The activities specified in Section 1.c of the Addendum.

Signature and date: By using the Vocal Video services to transfer Customer Data to Third Countries, the data exporter will be deemed to have signed this Annex I.

Role (controller / processor): Controller

Data importer(s):

Name: "Vocal Video” as identified in the Addendum.

Address: The address for Vocal Video specified in the Agreement.

Contact person’s name, position and contact details: The contact details for Vocal Video specified in the Addendum or the Agreement.

Activities relevant to the data transferred under these Clauses: The activities specified in Section 1.c of the Addendum.

Signature and date: By transferring Customer Data to Third Countries on Customer's instructions, the data importer will be deemed to have signed this Annex I.

Role (controller / processor): Processor

B. **DESCRIPTION OF TRANSFER**

Categories of data subjects whose personal data is transferred

Categories of data subjects are specified in Section 1.c of the Addendum.

Categories of personal data transferred

The personal data is described in Section 1.c of the Addendum.

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 data exporter might include sensitive personal data in the personal data described in Section 1.c of the Addendum.

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis)

Personal data is transferred in accordance with Customer's instructions as described in Section 9 of the Addendum.

Nature of the processing

The nature of the processing is described in Section 1.c of the Addendum.

Purpose(s) of the data transfer and further processing

To provide the Services.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

Not applicable because the data exporter determines the duration of processing in accordance with the terms of the Addendum.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

The subject matter, nature and duration of the processing are described in Section 1.c of the Addendum.

C. **COMPETENT SUPERVISORY AUTHORITY**

Identify the competent supervisory authority/ies in accordance with Clause 13

The data exporter's competent supervisory authority will be determined in accordance with the GDPR.

ANNEX II

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 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

The technical and organizational measures (including the certifications held by the data importer) as well as the scope and the extent of the assistance required to respond to data subjects' requests, are described in the Addendum.

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.

The technical and organisational measures that the data importer will impose on sub-processors are described in the Addendum.

ANNEX III

ADDITIONAL CLAUSES

The Limitations of Liability section of the Agreement (Section 4(h) of the Vocal Video Terms of Service) is an additional clause pursuant to Clause 2 of these Clauses.

Exhibit C

United Kingdom GDPR Addendum

1. **Applicability.** Except as otherwise set out in this UK Addendum, the terms of the Vocal Video DPA will apply to Customer's use of the Services to process United Kingdom ("UK") Customer Data, and all references to (i) "GDPR" in the Vocal Video DPA will be replaced with "UK GDPR", (ii) "Customer Data" in the Vocal Video DPA will be replaced with "UK Customer Data", (iii) "Standard Contractual Clauses" will be replaced with "UK Standard Contractual Clauses", (iv) "Controller-to-Processor Clauses" will be replaced with "UK Controller-to-Processor Clauses", and (v) "Processor-to-Processor Clauses" will be replaced with "UK Processor-to-Processor Clauses".

2. **Transfers of UK Customer Data.** When this UK Addendum applies, Sections 9(b) ("Application of Standard Contractual Clauses") and 9(c) ("Alternative Transfer Mechanism") of the Vocal Video DPA will not apply, and the following Sections will apply:

   "9(b) **Application of UK Standard Contractual Clauses.** Subject to Section 9(b), the UK Standard Contractual Clauses will only apply to UK Customer Data that is transferred, either directly or via onward transfer, to any UK Third Country, (each a "**UK Data Transfer**").

   9(b)(i) Since Customer is acting as a controller, the UK Controller-to-Processor Clauses will apply to a UK Data Transfer.

   9(c) **Alternative Transfer Mechanism.** The UK Standard Contractual Clauses will not apply to a UK Data Transfer if Vocal Video has adopted Binding Corporate Rules (as defined in the UK GDPR) for Processors or an alternative recognized compliance standard for lawful UK Data Transfers."

3. **Definitions.** The following capitalized terms used in this UK Addendum have the meaning given to them below:

   "**International Data Transfer Addendum**" means the international data transfer addendum to the Standard Contractual Clauses issued by the Information Commissioner's Office under section 119A of the Data Protection Act 2018 on February 2, 2022, and located in Annex A of this UK Addendum.

   "**UK Controller-to-Processor Clauses**" means the Controller-to-Processor Clauses, as amended by the International Data Transfer Addendum.

   "**UK Processor-to-Processor Clauses**" means the Processor-to-Processor Clauses, as amended by the International Data Transfer Addendum.

   "**UK Standard Contractual Clauses**" means the UK Controller-to-Processor Clauses, as in accordance with Section 9(b)(i).

   "**UK Customer Data**" means the "personal data" (as defined in the UK GDPR) that is uploaded to the Services under Customer's Vocal Video accounts.

   "**UK GDPR**" means the "applied GDPR" as defined in section 3 of the Data Protection Act 2018.

   "**UK Third Country**" means a country outside the UK not recognized by the Secretary of State or the Data Protection Act 2018 as providing an adequate level of protection for personal data (as described in the UK GDPR)."

4. **International Data Transfer Addendum.** Annex A ("International Data Transfer Addendum to the Standard Contractual Clauses") of this UK Addendum will apply in accordance with Section 2 of this UK Addendum.

5. **Entire Agreement; Conflict.** Except as supplemented by this UK Addendum, the Vocal Video DPA

(if applicable) and the Agreement will remain in full force and effect. Where both this UK Addendum and the Vocal Video DPA apply to a processing activity, both will apply concurrently. This UK Addendum, together with the Vocal Video DPA and the Agreement: (a) is intended by the parties as a final, complete and exclusive expression of the terms of their agreement, and (b) supersedes all prior agreements and understandings between the parties with respect to the subject matter hereof.

Annex A

International Data Transfer Addendum to the Standard Contractual Clauses (the "Addendum")

This Addendum is attached to and forms part of the UK Addendum. The parties hereby enter into this Addendum as a legally binding contract for the purpose of making UK Data Transfers. Unless otherwise defined in this Addendum, all capitalised terms used in this Addendum will have the meanings given to them in the UK Addendum.

Part 1: Tables

Table 1: Parties

Start date	The date that Customer starts to use the Services to transfer UK Customer Data to UK Third Countries.	
The Parties	**Exporter (who sends the Restricted Transfer)**	**Importer (who receives the Restricted Transfer)**
Parties' details	Full legal name: The entity identified as "Customer" in the Vocal Video DPA. Trading name (if different): If different, the trading name for Customer associated with its Vocal Video account or as otherwise specified in the Vocal Video DPA or the Agreement. Main address (if a company registered address): The address for Customer associated with its Vocal Video account or as otherwise specified in the Vocal Video DPA or the Agreement. Official registration number (if any) (company number or similar identifier): If any, the official registration number for Customer associated with its Vocal Video account or as otherwise specified in the Vocal Video DPA or the Agreement.	Full legal name: "Vocal Video" as identified in the Vocal Video DPA. Trading name (if different): N/A Main address (if a company registered address): The address for Vocal Video specified in the Agreement. Official registration number (if any) (company number or similar identifier): If any, the official registration number for Vocal Video specified in the Agreement.
Key Contact	Job Title: The job title for the contact associated with Customer's Vocal Video account, or as otherwise specified in the Vocal Video DPA or the	Job Title: The job title for the contact for Vocal Video specified in the Vocal Video DPA or the Agreement.

	Agreement. Contact details including email: The contact details associated with Customer's Vocal Video account, or as otherwise specified in the Vocal Video DPA or the Agreement.	Contact details including email: The contact details for Vocal Video specified in the Vocal Video DPA or the Agreement.
Signature (if required for the purposes of Section 2)	By using the Services to transfer UK Customer Data to UK Third Countries, the Exporter will be deemed to have signed this Addendum.	By transferring UK Customer Data to UK Third Countries on Customer's instructions, the Importer will be deemed to have signed this Addendum.

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: The date that Customer starts to use the Services to transfer Customer Data to Third Countries. Reference (if any): N/A Other identifier (if any): This Addendum is appended by reference to the following versions of the Approved EU SCCs: • the Controller-to-Processor Clauses attached hereto in Exhibit B

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:

Data exporter(s):
Name: The entity identified as "Customer" in the Vocal Video DPA.
Address: The address for Customer associated with its Vocal Video account or as otherwise specified in the Vocal Video DPA or the Agreement.
Contact person's name, position and contact details: The contact details associated with Customer's Vocal Video account, or as otherwise specified in the Vocal Video DPA or the Agreement.
Activities relevant to the data transferred under these Clauses: The activities specified in Section 1.c of the Vocal Video DPA.
Signature and date: By using the Services to transfer Customer Data to Third Countries, the data exporter will be deemed to have signed Annex I.
Role (controller / processor): (I) where the Controller-to-Processor Clauses apply, the data exporter will be a controller; and (ii) where the Processor-to-Processor Clauses apply, the data exporter will be a processor.

Data importer(s):
Name: "Vocal Video" as identified in the Vocal Video DPA.

Address: The address for Vocal Video specified in the Agreement.
Contact person's name, position and contact details: The contact details for Vocal Video specified in the Vocal Video DPA or the Agreement.
Activities relevant to the data transferred under these Clauses: The activities specified in Section 1.c of the Vocal Video DPA.
Signature and date: By transferring Customer Data to Third Countries on Customer's instructions, the data importer will be deemed to have signed Annex I.
Role (controller / processor): Processor.

Annex 1B: Description of Transfer:

Categories of data subjects whose personal data is transferred
Categories of data subjects are specified in Section 1.c of the Vocal Video DPA.
Categories of personal data transferred
The personal data is described in Section 1.c of the Vocal Video DPA.
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 data exporter might include sensitive personal data in the personal data described in Section 1.c of the Vocal Video DPA.
The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis)
Personal data is transferred in accordance with Customer's instructions as described in Section 9 of the Vocal Video DPA.
Nature of the processing
The nature of the processing is described in Section 1.c of the Vocal Video DPA.
Purpose(s) of the data transfer and further processing
To provide the Services.
The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period
Not applicable because the data exporter determines the duration of processing in accordance with the terms of the Vocal Video DPA.
For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing
The subject matter, nature and duration of the processing are described in Section 1.c of the Vocal Video DPA.

Annex II: 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 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
The technical and organizational measures (including the certifications held by the data importer) as well as the scope and the extent of the assistance required to respond to data subjects' requests, are described in the Vocal Video DPA.
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.
The technical and organisational measures that the data importer will impose on sub-processors are described in the Vocal Video DPA.

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

A list of Sub-processors is set out in Section 6 of the Vocal Video DPA.

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.