Data Processing Addendum

This Data Processing Addendum ("DPA"), which includes Annexes I, II and III hereto, forms part of the Agreement between the Service User and the Company, as defined in the Terms of Service ("ToS") appearing on the Company's website, and listed in Annex I, and apply to the Processing of Personal Data, as specified in Annex II. The purpose of the clauses contained in this DPA is to ensure compliance with applicable Data Protection Law, including specifically, in relation to the EU GDPR, compliance with Article 28(3) and (4) thereof. The clauses are without prejudice to obligations to which the Service Provider and the Company are subject under applicable Data Protection Law. In this DPA the use of the singular will include the plural, and vice versa. All capitalised terms not defined herein will have the meanings set forth in the ToS.

1 Definitions

1.1 "Agreement" means the agreement between the Service User and the Company arising from the use of the Service, as referred to in the ToS.

1.2 "Controller" has the meaning set out in the EU GDPR and, to the extent that Processing is done in terms of the Protection of Personal Information Act, 2013 ("POPIA"), includes a "Responsible Party" as defined herein.

1.3 "Data Protection Law" means all data protection laws and regulations applicable to Processing done under the Agreement, including, but

not limited to, the UK Data Protection Act 2018, the UK GDPR, the EU GDPR and POPIA.

1.4 "Data Subject" means the identified or identifiable natural person (living individual) to whom Personal Data relates and/or, where required in terms of POPIA or other Data Protection Law, the identified or identifiable legal (juristic) person to which Personal Data relates. An identifiable natural person (living individual) or legal (juristic) person is one who/which can be identified, directly or indirectly, as stipulated under applicable Data Protection Law.

1.5 "EU 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 (General Data Protection Regulation).

1.6 "EU SCCs" means the standard contractual clauses for the transfer of Personal Data to third countries, adopted by the European Commission in accordance with Article 46(2) of the EU GDPR.

1.7 "Operator" has the meaning assigned to it in POPIA.

1.8 "Personal Data" means any information relating to a Data Subject and, to the extent that Processing is done in terms of POPIA, includes "Personal Information" as defined herein.

1.9 "Personal Data Breach" means a breach of security during provision of the Services leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise Processed.

1.10 "Personal Information" has the meaning assigned to it in POPIA.

1.11 "Processing" means any operation or set of operations which is performed on Personal Data or on sets of Personal Data whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or

destruction, and “Process”, “Processed” and “Processes” have meanings concomitant therewith.

1.12 “Processor” means a natural or legal person, public authority, agency or other body which Processes Personal Data on behalf of the Controller and, to the extent that Processing is done in terms of POPIA, includes an Operator, as defined herein.

1.13 “Responsible Party” has the meaning assigned to it in POPIA.

1.14 “Restricted Area” means any territory which, under Data Protection Law, is not recognised by the European Commission as providing an adequate level of protection for Personal Data.

1.15 “RTS Data” means any and all Personal Data contained in the Recordings and Transcription Source supplied by the Service User to the Company for the performance of the Service in relation to a Specific Job in terms of the Agreement.

1.16 “SU Data” means any and all Personal Data provided to the Company by the Service User and in respect of which the Service User is the Data Subject.

1.17 “Sub-processor” means a third-party contracted by a Processor to Process Personal Data.

1.18 “UK GDPR” means the adaptation of the EU GDPR which is applicable to the United Kingdom, and which is supplementary to the UK Data Protection Act 2018.

1.19 “UK SCCs” means the standard contractual clauses for the international transfer of Personal Data provided in accordance with the UK GDPR and the Data Protection Act 2018.

2 Interpretation

This DPA shall be read and interpreted in the light of the provisions of applicable Data Protection Law and shall not be interpreted in a way that runs counter to the rights and obligations provided for therein or in a way that prejudices the fundamental rights or freedoms of Data Subjects.

Should any provision of this DPA be invalid or unenforceable, then the remainder of the provisions shall remain valid and in force.

3 Hierarchy

In the event of a contradiction between the clauses of this DPA and the provisions of related agreements between the Service User and the Company, existing at the time when these clauses are agreed to, or entered into thereafter, these clauses shall prevail.

4 Instructions and acknowledgements

4.1 The Service User acknowledges and confirms that the Company will act as a Processor in respect of RTS Data and as a Controller in respect of SU Data and that the Company shall be entitled to appoint Processors and/or Sub-processors for the purpose of Processing the SU Data and RTS Data.

4.2 The Service User further acknowledges and confirms that the Company may authorise any Sub-processor, as contemplated in 4.1, to appoint, in turn, further Sub-processor(s), as required in connection with the provisions of the Service, provided that any such further Sub-processor appointed shall be bound by way of a contract which imposes on the latter, in substance, the same data protection obligations as the ones imposed on the Company in accordance with the clauses of this DPA. The Company shall ensure that such further Sub-processor complies with the obligations to which the Company is subject pursuant to this DPA and to applicable Data Protection Law.

4.3 The Company will comply with all of its obligation under Data Protection Law in respect of the SU Data and RTS Data.

4.4 The Service User will comply with all of its obligations as a Controller under Data Protection Law in respect of RTS Data. The Service User warrants that it has obtained all consents, rights and authorisations necessary for it to instruct the Company to Process such RTS Data.

4.5 The Company will Process Personal Data only on documented instructions from the Service User, including with regard to transfers of Personal Data to a third country or an international organisation, unless required to do so by any law to which the Company is subject, in which case the Company will inform the Service User of that legal requirement before the relevant Processing of that Personal Data, unless that law prohibits such information on important grounds of public interest. Subsequent instructions may also be given by the Service User throughout the duration of the Processing of Personal Data. These instructions shall always be documented.

4.6 The Company shall immediately inform the Service User if, in the Company's opinion, instructions given by the Service User infringe any Data Protection Law.

5. Purpose Limitation

The Processor shall process the Personal Data only for the specific purpose(s) of the Processing, as set out in Annex II, unless it receives further instructions from the Service User.

6. Duration of the Processing of Personal Data

Processing by the Processor shall only take place for the duration specified in Annex II.

7. Security of Processing

7.1 The Company shall at least implement the technical and organisational measures specified in Annex III to ensure the security of the Personal Data. This includes protecting the Personal Data against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to the Personal Data (Personal Data Breach). In assessing the appropriate level of security, the Company and the Service User shall take due account of the state of the art, the costs of implementation, the

nature, scope, context and purposes of processing and the risks involved for the Data Subjects.

7.2 The Company shall grant access to the SU Data and RTS Data undergoing Processing to members of its Personnel only to the extent strictly necessary for implementing, managing and monitoring of the Agreement. The Company will ensure that persons authorised to Process the Personal Data received have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

7.3 In compliance with the requirements of s19 of POPIA, the Company will implement appropriate, reasonable technical and organisational measures to prevent:

7.3.1 loss of, damage to, or unauthorised destruction of Personal Information; and

7.3.2 unlawful access to or Processing of Personal Information.

7.4 In order to give effect to clause 7.3, the Company will take reasonable measures to:

7.4.1 identify all reasonably foreseeable internal and external risks to Personal Information in its possession or under its control;

7.4.2 establish and maintain appropriate safeguards against the risks identified;

7.4.3 regularly verify that the safeguards are effectively implemented; and

7.4.4 ensure that the safeguards are continually updated in response to new risks or deficiencies in previously implemented safeguards.

7.5 The Company will have due regard to generally accepted information security practices and procedures which may apply to it generally or be required in terms of specific industry or professional rules and regulations.

7.6 The Service User is responsible for using the Service in a manner which enables the Company to comply with Data Protection Law,

including implementing appropriate technical and organisational measures.

8. Sensitive Data

If the Processing 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 ("Sensitive Data"), the Company shall apply such specific restrictions and/or additional safeguards as may be agreed with the Service User.

9. Documentation and Compliance

9.1 The Company and the Service User shall be able to demonstrate compliance with the clauses of this DPA.

9.2 The Company shall deal promptly and adequately with enquiries from the Service User about the processing of Personal Data in accordance with this DPA.

9.3 The Company shall make available to the Service User all information necessary to demonstrate compliance with the obligations that are set out in this DPA and stem directly from applicable Data Protection Law. At the Service User's request, the Company shall also permit and contribute to audits of the Processing activities covered by this DPA, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or an audit, the Service User may take into account relevant certifications held by the Company.

9.4 The Service User may choose to conduct the audit by itself or mandate an independent auditor. Audits may also include inspections at the premises or physical facilities of the Company and shall, where appropriate, be carried out with reasonable notice.

9.5 The Company and the Service User shall make the information referred to in this clause, including the results of any audits, available to the competent supervisory authority/ies on request.

10. Use of Sub-Processors

10.1 The Company has the Service User's general authorisation for the engagement of Processors/Sub-processors from an agreed list. The Company shall specifically inform in writing the Service User of any intended changes to that list through the addition or replacement of Processors/Sub-processors at least 7 days in advance, thereby giving the Service User sufficient time to be able to object to such changes prior to the engagement of the concerned Processor(s)/ Sub-processor(s). The Company shall provide the Service User with the information necessary to enable the Service User to exercise the right to object.

10.2 Where the Company engages a Processor/Sub-processor for carrying out specific Processing activities in respect of SU Data, and/or RTS Data (on behalf of the Service User), in performance of the Service under the Agreement, it shall do so by way of a contract which imposes on the Processor/Sub-processor, in substance, the same data protection obligations as the ones imposed on the Company in accordance with the clauses of this DPA. The Company shall ensure that the Processor/Sub-processor complies with the obligations to which the Company is subject pursuant to this DPA and to applicable Data Protection Law.

10.3 At the Service User's request, the Company shall provide to the Service User a copy of such a Processor/Sub-processor agreement and any subsequent amendments. To the extent necessary to protect business secret or other confidential information, including Personal Data, the Company may redact the text of the agreement prior to sharing the copy.

10.4 The Company shall remain fully responsible to the Service User for the performance of the Company's obligations in accordance with the Agreement. The Company shall notify the Service User of any failure by the Processor/Sub-processor to fulfil its contractual obligations.

10.5 The Company shall agree a third-party beneficiary clause with the Processor/Sub-processor whereby – in the event the Company has factually disappeared, ceased to exist in law or has become insolvent – the Service User shall have the right to terminate the Processor/Sub-processor contract and to instruct the Processor/Sub-processor to erase or return the Personal Data.

11. International transfers

11.1 Any transfer of Personal Data to a third country or an international organisation by the Company shall be done only on the basis of documented instructions from the Service User or in order to fulfil a specific requirement under Data Protection Law to which the Company is subject and shall take place in compliance with Data Protection Law (which in respect of the EU GDPR means Chapter V thereof).

11.2 In accordance therewith, the Service User hereby specifically acknowledges and agrees that, subject to the provisions of this clause 11, the SU Data and/or RTS Data may be transferred to a third country or countries for the purposes of providing the Service under the Agreement.

11.3 The Service User agrees that where the Company engages a Processor or Sub-processor, in accordance with clause 10.1 of this DPA, for carrying out specific Processing activities, either on behalf of the Service User or the Company, in performance of the Services, and those Processing activities involve a transfer of Personal Data to a third country (under the EU GDPR, within the meaning of Chapter V thereof), the Company, Processor and Sub-processor can ensure

compliance with Data Protection Law by adhering to either clause 11.4 or 11.5 hereunder, whichever is applicable in the circumstances.

11.4 In respect of a transfer of Personal Information which falls within the ambit of s72 of POPIA, the provisions set out therein will be complied with.

11.5 In respect of a transfer of Personal Data which is governed by the provisions of either the EU GDPR or UK GDPR, to a country outside of the EEA or which is situated in a Restricted Area, the Service User agrees that the Company, the Processor and Sub-processor can ensure compliance with the EU GDPR or UK GDPR, as the case may be, by using standard contractual clauses, being either the EU SCCs or the UK SCCs, whichever is appropriate in the circumstances, provided the conditions for the use of those standard contractual clauses are met.

12. Assistance to the Service User

12.1 The Company shall promptly notify the Service User of any request it has received from the Data Subject. It shall not respond to the request itself, unless authorised to do so by the Service User.

12.2 The Company shall assist the Service User in fulfilling its obligations to respond to Data Subjects' requests to exercise their rights, taking into account the nature of the processing. In fulfilling its obligations in accordance with 12.1 and 12.2, the Company shall comply with the Service User's instructions.

12.3 In addition to the Company's obligation to assist the Service User pursuant to clause 12.2, the Company shall furthermore assist the Service User in ensuring compliance with the following obligations, taking into account the nature of the Processing and the information available to the Company:

12.3.1 the obligation to carry out an assessment of the impact of the envisaged Processing operations on the protection of Personal Data (a "Data Protection Impact Assessment") where a type of processing

is likely to result in a high risk to the rights and freedoms of natural persons;

12.3.2 the obligation to consult the competent supervisory authority/ies prior to Processing where a Data Protection Impact Assessment indicates that the Processing would result in a high risk in the absence of measures taken by the Service User to mitigate the risk;

12.3.3 the obligation to ensure that Personal Data is accurate and up to date, by informing the Service User without delay if the Company becomes aware that the Personal Data it is Processing is inaccurate or has become outdated;

12.3.4 the obligations in Article 32 of the EU GDPR, where such law is applicable, or similar obligations in other Data Protection Law, as appropriate.

12.4 The Company and the Service User shall set out in Annex III the appropriate technical and organisational measures by which the Company is required to assist the Service User in the application of this clause as well as the scope and the extent of the assistance required.

13. Notification of Personal Data Breach

(a) Data Processed by the Service User

In the event of a Personal Data Breach, the Company shall co-operate with and assist the Service User for the Service User to comply with its obligations under Data Protection Law, as Controller, which, in the case of the EU GDPR, means its obligations under Articles 33 and 34, taking into account the nature of Processing and the information available to the Company.

13.1 In the event of a Personal Data Breach concerning data Processed by the Service User, the Company shall assist the Service User:

13.1.1 in notifying the Personal Data Breach to the competent supervisory authority/ies without undue delay after the Service User

has become aware of it, where relevant (unless the Personal Data Breach is unlikely to result in a risk to the rights and freedoms of natural persons);

13.1.2 in obtaining the following information which, pursuant to Article 33(3) of the EU GDPR, where same is applicable, shall be stated in the Service User's notification and must at least include:

13.1.2.1 the nature of the Personal Data, including, where possible, the categories and approximate number of Data Subjects concerned and the categories and approximate number of Personal Data records concerned;

13.1.2.2 the likely consequences of the Personal Data Breach;

13.1.2.3 the measures taken or proposed to be taken by the Service User to address the Personal Data Breach, including, where appropriate, measures to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notifications shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

13.1.3 in complying (in relation to the EU GDPR, pursuant to Article 34 thereof) with the obligation to communicate without undue delay the Personal Data Breach to the Data Subject, when the Personal Data Breach is likely to result in a high risk to the rights and freedoms of natural persons.

(b) Data Processed by the Company

13.2 In the event of a Personal Data Breach concerning Personal Data Processed by the Company, the Company shall notify the Service User without undue delay after the Company having become aware of the breach. Such notification shall contain, at least:

13.2.1 a description of the nature of the breach (including, where possible, the categories and approximate number of Data Subjects and data records concerned);

13.2.2 the details of a contact point where more information concerning the Personal Data Breach can be obtained;

13.2.3 its likely consequences and the measures taken or proposed to be taken to address the breach, including to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this 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.

The Company and Service User shall set out in Annex III all other elements to be provided by the Company when assisting the Service User in the compliance with the Service User's obligations under Data Protection Law, which in respect of the EU GDPR means Articles 33 and 34 of that Regulation.

14. Non-compliance with this DPA and termination

14.1 Without prejudice to any provisions of Data Protection Law, in the event that the Company is in breach of its obligations under this DPA, the Service User may instruct the Company to suspend the Processing of Personal Data until the latter complies with these clauses or the Agreement is terminated. The Company shall promptly inform the Service User in case it is unable to comply with these clauses, for whatever reason.

14.2 The Service User shall be entitled to terminate the Agreement insofar as it concerns Processing of Personal Data in accordance with this DPA if:

14.2.1 the Processing of Personal Data by the Company has been suspended by the Service User pursuant to point 14.1 and if compliance with the clauses of this DPA is not restored within a

reasonable time and in any event within one month following suspension;

14.2.2 the Company is in substantial or persistent breach of the clauses of this DPA or its obligations under Data Protection Law;

14.2.3 the Company fails to comply with a binding decision of a competent court or the competent supervisory authority/ies regarding its obligations pursuant to these clauses or under Data Protection Law.

14.3 The Company shall be entitled to terminate the Agreement insofar as it concerns Processing of Personal Data under the clauses of this DPA where, after having informed the Service User that its instructions infringe applicable legal requirements in accordance with clause 4.6 hereof, the Service User insists on compliance with the instructions.

14.4 Following termination of the Agreement, as contemplated herein, the Company shall, at the choice of the Service User, delete all personal data processed on behalf of the Service User and certify to the Service User that it has done so, or return all the Personal Data to the Service User and delete existing copies unless Data Protection Law or any other law requires storage of the Personal Data. The provisions of clause 15 of this DPA shall apply in respect of the notification requirements, time limits and procedure for deletion or return of the Personal Data.

15. Deletion or return after completion of a Specific Job or upon termination

15.1 Unless a timeous request for retention or return of Personal Data is received by the Company from the Service User, all copies of SU Data and/or RTS Data relating to a Specific Job will be automatically deleted between 60 and 90 days after the date of completion or termination of such Specific Job.

15.2 Notwithstanding the provisions of 15.1, the Company and/or any Processor and/or Sub-processor appointed in terms of clause 10.1 hereof, may retain SU Data and/or RTS Data to the extent that Data Protection Law or any other applicable law or regulation requires retention thereof.

15.3 Until the Personal Data is deleted or returned, the Company shall continue to ensure compliance with the clauses of this DPA.

16. Invariability of the clauses of this DPA

16.1 The Service User and Company undertake that, save as provided in clause 16.2, this DPA will not be modified during the existence of the Agreement between them for the performance of a Specific Job, except for the addition of information to the Annexes or the updating of them.

16.2 The above undertaking does not prevent the addition, by agreement between the Service User and the Company, of further clauses or safeguards, provided that those clauses or safeguards do not directly or indirectly contradict the clauses of this DPA or detract from the fundamental rights or freedoms of Data Subjects.

Annex I

List of parties

Controller(s): The Service User, in respect of RTS Data. Address and contact details as per information provided to the Company separately via the Company website.

Way With Words Ltd/Way With Words SA (Pty) Ltd, in respect of SU Data. Addresses, contact details and DPO information provided on the Company website.

Processor(s): Way With Words Ltd/Way With Words SA (Pty) Ltd, in respect of RTS Data. Addresses, contact details and DPO information provided on the Company website.

Annex II

Description of the Processing

Categories of Data Subjects whose Personal Data is Processed:
SU Data: Service Users (clients)
RTS Data: the categories of Data Subjects whose Personal Data is contained in the Recordings and Transcription Source are determined by the Service User for the purposes of a Specific Job

Categories of Personal Data Processed (subject matter):
SU Data: information necessary for and related to the contractual relationship between the Service User and Company, including, but not limited to, the Service User's name, physical and email address/es, and other contact information, as well as banking and/or credit card, PayPal or similar details.
RTS Data: information contained in the audio/video files and/or other source material provided by the Service User for the purposes of the provision of the Service, which may include, but not be limited to, Data Subject names, physical and email addresses.

Sensitive Data Processed (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved:
SU Data: N/A
RTS Data: The Service User is required to apply adequate restrictions and safeguards to protect any Sensitive Data contained in the Recording and Transcription Source before supplying same to the Company for the performance of the Service under the Agreement, including, but not limited to, anonymisation. The Company will keep a record of access to the Sensitive Data and apply such additional security measures, as may be possible and agreed upon between the Company and the Service User.

Nature of the Processing:
SU Data: The nature of the Processing is determined by the information necessary for the performance of the Service under the Agreement, to permit the exchange of information and payment by the Service User to the Company.
RTS Data: The nature of the Processing is determined by the type of Service to be provided in terms of the Agreement for a Specific Job.

Purpose(s) for which the Personal Data is Processed.
SU Data and RTS Data: The purpose of the Processing under the Agreement is the provision of the Service for a Specific Job, as specified by the Service User and for accounting and billing purposes related thereto.

Duration of the Processing:
SU Data and RTS Data: The duration of the Processing under the Agreement is determined by the Service performed for the Service User.

Annex III

Technical and organisational measures, including technical and organisational measures to ensure the security of the Personal Data

Below is a description of the technical and organisational security measures implemented by the Company (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the Processing, as well as the risks for the rights and freedoms of natural persons.

Measures of pseudonymisation and encryption of Personal Data
Personal Data at rest is encrypted and stored in an AWS bucket in the Service User's region. Access to Personal Data is restricted by storing files using resource IDs in buckets outside the workflow system server. It is only accessible by Company Personnel and the Service User. Arrangements can be made for extra safeguarding where Sensitive Data may be present.

Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services
The Company's servers are monitored for vulnerabilities, sometimes by means of a pen testing tool.
The Company's website is PCI-DSS compliant.
The Company has a strong SHA-256 with RSA encryption certificate.

Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident
The Company's website is backed up daily by its host. Running a restore for this instance takes 2 to 4 hours.
The Company's workflow system is backed up by version control while the workflow database is backed up nightly by its host and the backups are then downloaded to an offsite server.
In case of a catastrophic failure this data can be restored within about 48 hours.

Measures for user identification and authorisation
Users are authenticated using passwords. Transcriber accounts have additional checks to see that they're not accessing files from outside their contracted regions.

Measures for the protection of data during transmission
Secure connection through https.
Only the Company's workflow system IP address is allowed to access the Company's workflow system database.

Measures for the protection of data during storage
User data (files) are encrypted and stored in AWS buckets.

Measures for ensuring physical security of locations at which Personal Data is processed and measures for ensuring events logging
The host of the Company's workflow system has the following security accreditations:
ISO 27001
ISO 9001:2015
ISO 22301:2012
ISO 20000: 2011
ISO 14001:2015
ISO 500001:2011

Measures for certification/assurance of processes and products
The Company is currently working towards ISO 270001 certification

Measures for ensuring limited data retention and measures for allowing portability and ensuring erasure
After 60 days have expired from the completion of a Specific Job, the Personal Data is marked for deletion before being removed from the Company's workflow system in accordance with the contractual provisions for data storage/removal contained in the Agreement. Custom retention periods are available upon request from the Service User.