DATA PROCESSING ADDENDUM

This Data Processing Addendum (DPA) 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. 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 "Contracted Processor" means the Company or a Sub-processor.

1.3 "Controller" means a natural or legal person, public authority, agency or other body which determines the purposes and means of the Processing of Personal Data 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.

1.4 "Data Protection Law" means all applicable data protection laws and regulations, including, but not limited to, the UK Data Protection Act 2018, the GDPR and the Protection of Personal Information Act, 2013 (POPIA).

1.5 "Data Subject" means the identified or identifiable natural person to whom Personal Data relates and, where required in terms of specific Data Protection Law, includes an identified or identifiable natural or juristic person to whom Personal Data relates.

1.6 “EU Model Clauses” means the standard contractual clauses for Processors as approved by the European Commission pursuant to Decision C (2010) 593, as they may be amended or replaced from time to time.

1.7 “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).

1.8 “Operator” has the meaning assigned to it in the Protection of Personal Information Act, 2013 (POPIA).

1.9 “Personal Data” means any information relating to a Data Subject and, to the extent that Processing is done in terms of the Protection of Personal Information Act, 2013 (POPIA), includes “Personal Information” as defined herein.

1.10 “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.

1.11 “Personal Information” has the meaning assigned to it in the Protection of Personal Information Act, 2013 (POPIA).

1.12 “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.

1.13 “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 the

Protection of Personal Information Act, 2013 (POPIA), includes an "Operator", as defined herein.

1.14 "Responsible Party" has the meaning assigned to it in the Protection of Personal Information Act, 2013 (POPIA).

1.15 "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.

1.16 "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.

1.17 "Sub-processor" means any third-party Processor, engaged to Process RTS Data in performance of the Service under the Agreement.

2 Processing

2.1 The Service User acknowledges and consents that the Company will act as a Processor in respect of RTS Data.

2.2 The Service User will comply with all of its obligations as a Controller under Data Protection Law in respect of the 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.

2.3 The Company will comply with all of its obligations as Processor under Data Protection Law in respect of the RTS Data and will Process such 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 Processor is subject, in which case the Company will inform the Service User of that legal requirement before the relevant Processing of that RTS Data, unless that law prohibits such information on grounds of public interest.

2.4 The subject-matter and type of Personal Data to be Processed under the Agreement is determined by the Recordings and Transcription Source referred to in 1.16.

2.5 The duration of the Processing under the Agreement is determined by the Service User in respect of a Specific Job.

2.6 The purpose of the Processing under the Agreement is the provision of the Service for a Specific Job as specified by the Service User.

2.7 The nature of the Processing is determined by the type of Service to be provided in terms of the Agreement for a Specific Job.

2.8 The categories of Data Subjects are determined by the Service User for the purposes of a Specific Job.

3. Sub-processing

3.1 The Company will respect the conditions referred to in paragraphs 2 and 4 of Article 28 of the GDPR regarding the engagement of Sub-processors and other similar obligations under Data Protection Law.

3.2 Subject to 3.3 and 3.4 hereunder, the Servicer User acknowledges and consents that the Company may engage Sub-processor/s, who may, in turn, be authorised by the Company to engage other Sub-processors, as required in connection with the provision of the Service. Sub-processors will be permitted to obtain RTS Data only as required for the provision of the Service and for no other purpose.

3.3 Each Sub-processor will be contractually bound by the same data protection obligations, mutatis mutandis, as are set out in the DPA.

3.4 Where any Sub-processor fails to fulfil its data protection obligations, as referred to herein, the Company will be liable to the Service User for the performance of such obligations.

4. Confidentiality

The Company will ensure that all persons authorised by it to Process RTS Data have committed themselves to confidentiality or are under an appropriate Statutory obligation of confidentiality.

5. Security

5.1 Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the Company will implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk during the provision of the Service, including, inter alia, as appropriate, the pseudonymisation and encryption of RTS Data and/or other measures referred to in Article 32 of the GDPR or otherwise under Data Protection Law.

5.2 In particular, in accordance with the requirements of s19 of the Protection of Personal Information Act, 2013 (POPIA), the Company will implement appropriate, reasonable technical and organisation measures to prevent:

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

5.2.2 unlawful access to or processing of Personal Information.

5.3 In order to give effect to clause 5.2, the Company will take reasonable measures to:

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

5.3.2 establish and maintain appropriate safeguards against the risks identified;

5.3.3 regularly verify that the safeguards are effectively implemented; and

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

5.4 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.

5.5 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.

6. Personal Data Breach Management and Notification

6.1 The Company will assist the Service User in ensuring compliance with the obligations pursuant to Articles 32 to 36 of the GDPR or other similar obligations under Data Protection Law, taking into account the nature of processing and the information available to the Company.

6.2 The Company will notify the Service User without undue delay upon becoming aware of a Personal Data Breach affecting RTS Data. The Company will provide the Service User with sufficient information to allow the Service User to meet any obligations to report or inform Data Subjects of the Personal Data Breach under Data Protection Law.

6.3 The Company will co-operate with the Service User and take such reasonable commercial steps as are directed by the Service User to assist in the investigation, mitigation and remediation of each such Personal Data Breach.

7. Data Protection Impact Assessment and Prior Consultation

To the extent required by Data Protection Law, the Company will, upon reasonable notice, provide reasonably requested information regarding the Service in respect of a Specific Job to enable the Service User to carry out a data protection impact assessment and/or a prior consultation with data protection authorities.

8. Data Subject's Rights

8.1 Taking into account the nature of the Processing, the Company will assist the Service User by implementing appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Service User's obligation to respond to a request from any Data Subject referred to in the Recordings and Transcription Source being Processed for a Specific Job under the Agreement for the exercising of such Data Subject's rights under Chapter III of the GDPR or otherwise in terms of Data Protection Law.

8.2 The Company will promptly notify the Service User if any Contracted Processor receives a request from a Data Subject under any Data Protection Law in respect of the RTS Data.

8.3 The Company will ensure that the Contracted Processor does not respond to the request referred to in 8.2 except on the documented instructions of the Service User or as required by Data Protection Law to which the Contracted Processor is subject, in which case the Company will, to the extent permitted by Data Protection Law, inform the Service User of that legal requirement before the Contracted Processor responds to the request.

9. Deletion or return of Service User Personal Data

9.1 Subject to 9.2 and 9.3, the Service User may, by written notice sent to the Company and received by it within 30 days of the completion or termination of any Specific Job in relation to the Processing of RTS Data (the "Cessation Date"), require the Company to either return or delete all RTS Data and delete all existing copies of such RTS Data. The Company will promptly comply with any such written notice received.

9.2 If no written notice, as referred to in 9.1, is received by the Company the RTS Data and existing copies of RTS Data will be deleted by the Company between 90 and 120 days after the Cessation Date.

9.3 Notwithstanding 9.1 and 9.2 each Contracted Processor may retain RTS Data to the extent that Data Protection Law or any other law or regulation requires storage thereof.

10. Audit Rights

10.1 Subject to 10.2, the Company will make available to the Service User, on request, all information necessary to demonstrate compliance with the obligations laid down in Article 28 of the GDPR, or any similar obligations under Data Protection Law, and will allow for and contribute to audits, including inspections, by the Service User or another auditor mandated by the Service User in relation to the Processing of RTS Data by the Contracted Processors.

10.2 With regard to 10.1, the Company will immediately inform the Service User if, in its opinion, an instruction infringes the GDPR or other Data Protection Law.

11. Data Transfers and Exports

11.1 Subject to 11.2 and 11.3, the Service User acknowledges and agrees that the RTS Data may be Processed in any locations around the world where Contracted Processors maintain data processing operations as necessary to provide the Service as set forth in the Agreement.

11.2 In respect of a transfer of Personal Information which falls within the ambit of s72 of the Protection of Personal Information Act, 2013 (POPIA), the Company will comply with the provisions set out therein.

11.3 In respect of a transfer of Personal Data to a Restricted Area, the Service User hereby grants the Company the authority, wherever necessary, to enter into the EU Model Clauses on Service User’s behalf, with Sub-processor/s based anywhere in such Restricted Area.

11.4 The Service User acknowledges and consents that the Company may authorise Sub-processor/s, in turn, to engage other Sub-

processor/s, as required in connection with the provisions of the Service, and who may be in a Restricted Area, or foreign country as envisaged by the Protection of Personal Information Act, 2013 (POPIA), provided that the provisions of 11.2 and 11.3 will apply, mutatis mutandis, in respect of any such engagement and any such transfer.

12. General

12.1 In the event of any conflict between the DPA and any privacy-related provisions in the Agreement, the terms of the DPA will prevail.

12.2 The Company may modify the terms of the DPA, as provided in the Agreement, (i) if required to do so by a supervisory authority or other government or regulatory entity, or (ii) if it is necessary to comply with Data Protection Law, or (iii) to implement or adhere to standard contractual clauses, approved codes of conduct or certification, binding corporate rules, or other compliance mechanisms which may be permitted under Data Protection Law. Supplemental terms may be added as an Annex or Appendix to the DPA where such terms only apply to the processing of Personal Data under the Data Protection Law of specific countries or jurisdictions. The Company will provide notice of such changes to the Service User and the modified DPA will become effective, in accordance with the terms of the Agreement or as otherwise provided on the Company's website if not specified in the Agreement.

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