Data Processing Addendum

BACKGROUND:

(1) This Data Processing Addendum ("**DPA**") forms part of the Contract for the Supply of Services (the "**Principal Agreement**") between the entity identified as "Client" in the Principal Agreement and Take Note Ltd (the "**Service Provider**").

(2) The DPA is intended to ensure that the Client and the Service Provider are compliant with the requirements of Article 28(3) of the UK GDPR.

1. **Definitions and Interpretation**

1.1 In this DPA, unless the context otherwise requires, the following expressions have the following meanings:

"Client"	means the entity identified as "Client" in the Principal Agreement;
"Client Personal Data"	means any personal data to be processed by a Contracted Processor on behalf of the Client pursuant to or in connection with the Principal Agreement;
"Contracted Processor"	means the Service Provider or any of its Sub-processors;
"data controller", "data processor", "data subject", "personal data", "personal data breach" and "processing"	have the same meaning as set out in the Data Protection Legislation;
"Data Protection Legislation"	means any data protection legislation from time to time in force in the United Kingdom including, but not limited to, the Data Protection Act 2018, any legislation which succeeds or supplements that Act, the UK GDPR, the WA GDPR to the extent applicable, and, for as long as and to the extent that the law of the European Union has legal effect in the United Kingdom, the General Data Protection Regulation (EU) 2016/679 ("the GDPR") as well as any other directly applicable European Union data protection or privacy regulations;
"Data Transfer Bridge Period"	means the period commencing on 01 January 2021 and ending as set out in the provisions of Article FINPROV.10A(4) of the EU-UK Trade and Cooperation Agreement;
"EEA"	means the European Economic Area;

"EU-UK Trade and Cooperation Agreement"	means the Trade and Cooperation Agreement Between the European Union and the European Atomic Energy Community, of the one part, and the United Kingdom of Great Britain and Northern Ireland, of the other part;
"Portal"	means the Service Provider's secure web portal via which the Services are provided;
"Services"	means the services provided to the Client by the Service Provider, as defined in the Principal Agreement;
"Sub-processor"	means any person or entity appointed by or on behalf of a Contracted Processor to process personal data on behalf of the Client in connection with the DPA;
"Supervisory Authority"	has the same meaning as set out in the Data Protection Legislation;
"UK GDPR"	means the General Data Protection Regulation (EU) 2016/679 as incorporated in United Kingdom law by virtue of Section 3 of the European Union (Withdrawal) Act 2018;
"WA GDPR"	means the General Data Protection Regulation (EU) 2016/679 as in force on 31 December 2020 and as applicable to the processing of personal data pursuant to Article 71 of the Withdrawal Agreement;
"Withdrawal Agreement"	means the Agreement on the Withdrawal of the United Kingdom of Great Britain and Northern Ireland from the European Union and the European Atomic Energy Community (2019/C 384 I/01).

1.2 Unless the context otherwise requires, each reference in this DPA to:

1.2.1 "writing", and any cognate expression, includes a reference to any communication effected by electronic transmission or similar means;

1.2.2 a statute or a provision of a statute is a reference to that statute or provision as amended or re-enacted at the relevant time;

1.2.3 a Schedule is a schedule to this DPA;

1.2.4 a Clause or Paragraph is a reference to a Clause of this DPA (other than the Schedules) or a Paragraph of the relevant Schedule; and

1.2.5 a "Party" or the "Parties" refer to the parties to this DPA.

1.3 The headings used in this DPA are for convenience only and have no effect

upon the interpretation of the DPA.

1.4 Words imparting the singular number include the plural and vice versa.

1.5 References to any gender include the other gender.

1.6 References to persons include corporations.

2. Scope and Roles

2.1 The provisions of this DPA apply when personal data is processed by the Service Provider on behalf of the Client.

2.2 In the context of this DPA:

2.2.1 the Service Provider acts as a data processor; and

2.2.2 the Client may act as either a data controller or a data processor.

3. Processing of Client Personal Data

3.1 Both Parties shall comply with the Data Protection Legislation in the processing of Client Personal Data.

3.2 The Client instructs the Service Provider to process Client Personal Data in order to facilitate the provision of the Services.

3.3 The Service Provider shall:

3.3.1 not process Client Personal Data other than on the documented instructions of the Client, including in respect of international transfers, unless required to do so by law to which the Service Provider is subject;

3.3.2 promptly comply with any request from the Client requiring the Service Provider to amend, transfer, delete, or otherwise dispose of Client Personal Data;

3.3.3 keep complete and accurate records and information concerning all processing activities carried out on Client Personal Data in order to demonstrate its compliance with this DPA; and

3.3.4 immediately inform the Client if instructions given by the Client pursuant to Clause 3.3.1, in the opinion of the Service Provider, contravene the Data Protection Legislation.

3.4 In the event that Client Personal Data is subject to the provisions of Article 71 of the Withdrawal Agreement, the Service Provider shall apply the WA GDPR to the processing of any such Client Personal Data provided that the Client has informed the Service Provider of such requirements.

3.5 Subject to Clause 3.6, where the Client is established in the EEA:

3.5.1 The Standard Contractual Clauses in Annex A apply to the processing of Client Personal Data.

3.5.2 To the extent that the Standard Contractual Clauses apply to the processing of Client Personal Data, in the event of conflict between the Standard Contractual Clauses and any other provision of this DPA, the Standard Contractual Clauses take precedence.

3.5.3 Notwithstanding Clause 3.5.1, where the European Commission has determined that the United Kingdom provides an adequate level of protection, for the purposes of Article 45 of the GDPR, the Standard

Contractual Clauses will not apply to the processing of Client Personal Data for as long as such an adequacy decision remains in force.

3.6 Clause 3.5 becomes effective on the first day after the end of the Data Transfer Bridge Period.

4. Data Processor Personnel

The Service Provider shall take reasonable steps to ensure the reliability of any employee, agent or contractor of any Contracted Processor who may have access to the Client Personal Data, ensuring in each case that access is strictly limited to those individuals who need to access the relevant Client Personal Data, as strictly necessary for the purposes of the Principal Agreement, and to comply with the Data Protection Legislation in the context of that individual's duties to the Contracted Processor, ensuring that all such individuals are subject to confidentiality undertakings or professional or statutory obligations 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 Service Provider shall in relation to Client Personal Data implement appropriate technical and organisational measures, as set out in Schedule 3, to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1) of the UK GDPR.

5.2 In assessing the appropriate level of security, the Service Provider shall take account of the risks that are presented by processing, in particular from a personal data breach.

6. Sub-processing

6.1 By virtue of this DPA, the Service Provider has the Client's general written authorisation for the engagement of Sub-processors. The list of Sub-processors already authorised by the Client can be found in Schedule 1. The Service Provider shall inform the Client of any intended changes concerning the addition or replacement of Sub-processors at least 30 days in advance, thereby giving the Client the opportunity to object to such changes prior to the engagement of the concerned Sub-processor(s).

6.2 The Service Provider shall comply with the requirements of Article 28(2) and (4) of the UK GDPR when engaging a Sub-processor.

7. Data Subject Rights

7.1 Taking into account the nature of the processing, and to the extent practicable, the Service Provider shall assist the Client by implementing appropriate technical and organisational measures, for the fulfilment of Client obligations as reasonably understood by the Client, to respond to requests from data subjects to exercise their rights under the Data Protection Legislation.

7.2 The Service Provider shall:

7.2.1 promptly notify the Client if it receives a request from a data subject under any Data Protection Legislation in respect of Client Personal Data; and

7.2.2 ensure that it does not respond to that request except on the documented instructions of the Client or as required by applicable laws to which the Service Provider is subject, in which case the Service Provider shall, to the extent permitted by law, inform the Client of that legal requirement before the responding to the request.

8. Personal Data Breach

8.1 The Service Provider shall notify the Client without undue delay upon becoming aware of a personal data breach affecting Client Personal Data, providing the Client with sufficient information to allow the Client to meet any obligations to report, or inform data subjects of, the personal data breach under the Data Protection Legislation.

8.2 The Service Provider shall cooperate with the Client and take reasonable commercial steps as are directed by Client to assist in the investigation, mitigation and remediation of each such personal data breach.

9. Data Protection Impact Assessment and Prior Consultation

The Service Provider shall provide reasonable assistance to the Client with any data protection impact assessments, and prior consultations with Supervisory Authorities or other competent data privacy authorities, which the Client reasonably considers to be required by Article 35 or 36 of the UK GDPR or equivalent provisions of any other Data Protection Legislation, in each case solely in relation to processing of Client Personal Data by, and taking into account the nature of the processing and information available to, the Contracted Processors

10. Deletion of Client Personal Data

10.1 Unless agreed otherwise by the Parties, following the end of the provision of Services under the Principal Agreement and subject to Clause 10.2, the Service Provider shall delete and procure the deletion of all Client Personal Data, including copies, according to the Data Retention Plan in Schedule 2.

10.2 In the event that retention of Client Personal Data is required by law, the Service Provider shall not delete the Client Personal Data but shall inform the Client of such requirements in writing.

11. Audit Rights

11.1 Subject to this Clause 11, the Service Provider shall make available to the Company upon written request all information necessary to demonstrate compliance with this DPA, and shall allow for and contribute to audits, including inspections, by the Client or an auditor mandated by the Client in relation to the processing of Client Personal Data by the Contracted Processors.

11.2 The information and audit rights of the Client only arise under this Clause 11 to the extent that the DPA does not otherwise give the Client information and audit rights meeting the relevant requirements of the Data Protection Legislation.

12. Data Transfer

12.1 The Service Provider shall not transfer or authorise the transfer of Client Personal Data to countries outside the United Kingdom without the prior written consent of the Client.

12.2 Notwithstanding Clause 12.1, the Client agrees that the Service Provider may transfer Client Personal Data to countries within the EEA.

12.3 In the event that personal data processed under this DPA is transferred to a country outside the United Kingdom, the Parties shall ensure that such personal data is adequately protected according to Chapter V of the UK GDPR.

13. General Terms

13.1 **Confidentiality.** Each Party shall keep this DPA and information it receives about the other Party and its business in connection with this DPA ("Confidential Information") confidential, and shall not use or disclose that Confidential Information without the prior written consent of the other Party except to the extent that:

a) disclosure is required by law to which the disclosing Party is subject; or

b) the relevant information is already in the public domain through no fault of the disclosing Party.

13.2 **Notices.** All notices and communications given under this DPA must be in writing and in accordance with the provisions of Clause 20 of the Principal Agreement.

SCHEDULE 1: Sub-processors

1. **Approved Sub-processors**

The Client agrees that the Service Provider may engage the following sub-processors with respect to the processing of Client Personal Data:

Name	Description of processing	Location	Appropriate safeguards[1]
Amazon Web Services (AWS)	Hosting of the Portal	UK	N/A
MongoDB Atlas	Database services for the Portal	UK	N/A

[1] Pursuant to UK GDPR, Article 46

SCHEDULE 2: Nature and Purpose of Processing

1. **Subject Matter**

1.1 The subject matter of Client Personal Data is determined solely by the Client.

1.2 The source material provided by the Client to the Service Provider will be:

a) in the case of the Service Provider's Live Notetaking service, a live meeting or other similar event captured in real time by the Service Provider; or

b) in the case of any other of the Service Provider's transcription services, recorded audio or video files uploaded to the Portal ("Media Files").

2. **Duration**

The processing of Client Personal Data will continue for the term of the Principal Agreement, subject to the Data Retention Plan set out in Paragraph 7.

3. **Nature of the Processing**

The nature of the processing is as required in order for the Service Provider to provide the Services to the Client, and may include (without limitation):

a) Collection;

b) Recording;

c) Storage;

d) Adaption or alteration;

e) Transcription;

f) Pseudoymisation;

g) Anonymisation;

h) Erasure.

4. **Purpose of the Processing**

The purpose of the processing is to produce typed transcripts ("Transcripts") from the source material described in Paragraph 1.2.

5. **Types of Personal Data**

The types of personal data are determined solely by the Client, and may include (without limitation):

a) Personally identifiable information, such as name, address, telephone number, email address, National Insurance number, or any other identifiers;

b) Information related to data subjects' gender and physical characteristics;

c) Information related to data subjects' employment;

d) Information related to data subjects' activities and interests;

e) Special categories of personal data, including (without limitation):

i. Information related to data subjects' racial or ethnic origin;

ii. Information related to data subjects' health;

iii. Information related to data subjects' political opinions, religious or philosophical beliefs.

6. **Categories of Data Subject**

The categories of data subject are determined solely by the Client, and may include (without limitation):

a) Employees of the Client;

b) Sub-contractors of the Client;

c) Customers of the Client;

d) Interested parties related to the Client's projects or work; and

e) Members of the public involved in the Client's projects or work.

7. **Data Retention Plan**

7.1 The Service Provider shall automatically delete Client Personal Data according to the following schedule:

a) for Media Files, 60 days after upload to the Portal; and

b) for Transcripts, 12 months after the delivery of the completed Transcript.

7.2 Notwithstanding Paragraph 7.1, the Client may delete Client Personal Data manually via the Portal at any time after the delivery of the completed Transcript.

SCHEDULE 3: Technical and Organisational Data Protection Measures

1. The Service Provider shall ensure that, in respect of all Client Personal Data, it maintains security measures to a standard appropriate to:
   1.1 the harm that might result from unlawful or unauthorised processing or accidental loss, damage, or destruction of the Client Personal Data; and
   1.2 the nature of the Client Personal Data.

2. In particular, the Service Provider shall:
   2.1 have in place, and comply with, a security policy which:
      2.1.1 defines security needs based on a risk assessment;
      2.1.2 allocates responsibility for implementing the policy to a specific individual or personnel;
      2.1.3 is provided to the Client on or before the commencement of the Principal Agreement;
      2.1.4 is disseminated to all relevant staff; and
      2.1.5 provides a mechanism for feedback and review.
   2.2 ensure that appropriate security safeguards and virus protection are in place to protect the hardware and software which is used in processing the Client Personal Data in accordance with best industry practice;
   2.3 prevent unauthorised access to the Client Personal Data;
   2.4 protect the Client Personal Data using pseudonymisation, where it is practical to do so;
   2.5 ensure that its storage of Client Personal Data conforms with best industry practice such that the media on which Client Personal Data is recorded (including paper records and records stored electronically) are stored in secure locations and access by personnel to Client Personal Data is strictly monitored and controlled;
   2.6 have secure methods in place for the transfer of Client Personal Data whether in physical form (for example, by using couriers rather than post) or electronic form (for example, by using TLS 1.3 protocols for transfer of Client Personal Data via the Service Provider's Secure Portal);
   2.7 password protect all computers and other devices on which Personal Data is stored, ensuring that all passwords are secure (following the latest guidance issued by the National Cyber Security Centre), and that passwords are not shared under any circumstances;
   2.8 take reasonable steps to ensure the reliability of personnel who have access to the Client Personal Data;
   2.9 have in place methods for detecting and dealing with breaches of security (including loss, damage, or destruction of Client Personal Data) including:
      2.9.1 the ability to identify which individuals have worked with specific Client Personal Data;
      2.9.2 having a proper procedure in place for investigating and remedying breaches of the Data Protection Legislation; and
      2.9.3 notifying the Client as soon as any such security breach occurs.

2.10 have a secure procedure for backing up all electronic Client Personal Data and storing back-ups separately from originals;

2.11 have a secure method of disposal of unwanted Client Personal Data including for back-ups, disks, print-outs, and redundant equipment; and

2.12 adopt such organisational, operational, and technological processes and procedures as are required to comply with the requirements of ISO/IEC 27001:2013, as appropriate to the Services provided to the Client.

ANNEX A: Standard Contractual Clauses (processors)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

The entity identified as "Client" in the DPA
(the "**data exporter**")

and

Take Note Ltd
Three Tuns House, 109 Borough High Street, London, SE1 1NL, United Kingdom
(the "**data importer**")

each a "party"; together "the parties",

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Clause 1

Definitions

For the purposes of the Clauses:

(a) 'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject' and 'supervisory authority' shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;

(b) 'the data exporter' means the controller who transfers the personal data;

(c) 'the data importer' means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) 'the sub-processor' means any processor engaged by the data importer or by any other sub-processor of the data importer who agrees to receive from the data importer or from any other sub-processor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) 'the applicable data protection law' means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) 'technical and organisational security measures' means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves

the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.
2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.
3. The data subject can enforce against the sub-processor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.
4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter[2]

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

[2] Mandatory requirements of the national legislation applicable to the data importer which do not go beyond what is necessary in a democratic society on the basis of one of the interests listed in Article 13(1) of Directive 95/46/EC, that is, if they constitute a necessary measure to safeguard national security, defence, public security, the prevention, investigation, detection and prosecution of criminal offences or of breaches of ethics for the regulated professions, an important economic or financial interest of the State or the protection of the data subject or the rights and freedoms of others, are not in contradiction with the standard contractual clauses. Some examples of such mandatory requirements which do not go beyond what is necessary in a democratic society are, inter alia, internationally recognised sanctions, tax-reporting requirements or anti-money-laundering reporting requirements.

(b) that it has instructed and throughout the duration of the personal data-processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any sub-processor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for sub-processing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of sub-processing, the processing activity is carried out in accordance with Clause 11 by a sub-processor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation;

(ii) any accidental or unauthorised access; and

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data-processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for sub-processing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of sub-processing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the sub-processor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any sub-processor agreement it concludes under the Clauses to the data exporter.

Clause 6

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or sub-processor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his sub-processor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

   The data importer may not rely on a breach by a sub-processor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the sub-processor of any of

their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the sub-processor agrees that the data subject may issue a claim against the data sub-processor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the sub-processor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:
   (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;
   (b) to refer the dispute to the courts in the Member State in which the data exporter is established.
2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.
2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any sub-processor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.
3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any sub-processor preventing the conduct of an audit of the data importer, or any sub-processor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5(b).

Clause 9

Governing law

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clauses.

Clause 11

Sub-processing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the sub-processor which imposes the same obligations on the sub-processor as are imposed on the data importer under the Clauses. Where the sub-processor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the sub-processor's obligations under such agreement.
2. The prior written contract between the data importer and the sub-processor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.
3. The provisions relating to data protection aspects for sub-processing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.
4. The data exporter shall keep a list of sub-processing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5(j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data-processing services

1. The parties agree that on the termination of the provision of data-processing services, the data importer and the sub-processor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.
2. The data importer and the sub-processor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data-processing facilities for an audit of the measures referred to in paragraph 1.

APPENDIX 1 to the Standard Contractual Clauses

Data exporter

The data exporter is engaging the data importer to produce typed transcriptions from recorded media or live meetings, or to provide other services of a similar nature.

Data importer

The data importer is a provider of transcription services and is providing the services described above to the data exporter.

Data subjects

The categories of data subjects are specified in Schedule 2 of the DPA.

Categories of data

The categories of data are specified in Schedule 2 of the DPA.

Special categories of data

The special categories of data are specified in Schedule 2 of the DPA.

Processing operations

The personal data transferred will be subject to the following basic processing activities (please specify):

- Receiving data;
- Holding data;
- Using data to produce typed transcripts or other similar end products;
- Protecting data, including restricting access and encrypting data at rest and in transit;
- Sharing data to facilitate the production of typed transcripts or other similar end products;
- Returning data to the data exporter upon completion of the services; and
- Erasing data.

All processing activities are strictly for the purposes of providing services to the data exporter, as defined in the Principal Agreement and the DPA.

APPENDIX 2 to the Standard Contractual Clauses

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

The technical and organisational security measures implemented by the data importer are specified in Schedule 3 of the DPA.