

DATA PROCESSING AGREEMENT

Between

<<CLIENT NAME>>

and

Localscript Ltd

For

Provision of transcription and anonymisation services by Localscript Ltd for <<CLIENT NAME>>.

DATA PROCESSING AGREEMENT

This Agreement is between

(1) <<CLIENT NAME>>, [incorporated and registered in England and Wales with company number <<NUMBER>>] / [an institution established at] whose registered office is at <<ADDRESS>> ("**the Data Controller**"); and

(2) **Localscript Ltd**, incorporated and registered in England and Wales with company number 17388152, whose registered office is at 13 The Terrace, Barnes, London, SW13 0NP ("**the Data Processor**").

BACKGROUND

A. The Data Processor has agreed to provide the Services (defined in the Schedule) to the Data Controller and in doing so shall process the Shared Personal Data (defined in the Schedule) for or on behalf of the Data Controller; and

B. The Data Controller has agreed to provide the Data Processor with access to the Shared Personal Data and the Data Processor has agreed to process the Shared Personal Data in accordance with the terms and conditions set out in this Agreement.

AGREED TERMS

1. The following definitions apply in this Agreement. Any capitalised terms not defined below shall have the meaning ascribed to them in the Schedule.

Agreed Purpose	means the purpose(s) for which Shared Personal Data can be processed by the Data Processor under this Agreement, which are to transcribe, attribute speakers within, anonymise and format audio and audiovisual recordings sent from <<CLIENT NAME>>
Commencement Date	<<DATE>>, notwithstanding the last date of signature of this Agreement
<<CLIENT NAME>> Single Point of Contact (SPoC)	Name: <<NAME>> Position: <<POSITION>> T: <<TELEPHONE>> E: <<EMAIL>>
Localscript Ltd Single Point of Contact (SPoC)	Montagu Franks, Director E: monty@localscript.co.uk

2. The Data Processor agrees to process the Shared Personal Data on behalf of the Data Controller for the Term and on the terms and conditions of this Agreement.

3. The Data Processor does not transfer Shared Personal Data outside the United Kingdom. The provisions of **Annex C** apply.

4. In the event of a conflict between the terms of the Annexes, the remainder of the Agreement and the Services Agreement (as defined in the Schedule), the order of precedence shall be as follows:

1. Annex (if applicable)
2. The remainder of this Agreement
3. The Services Agreement

In witness whereof, this page together with the page preceding it and the Schedule and Annexes are executed as follows:

SIGNED FOR AND ON BEHALF OF <<CLIENT NAME>>

Signed for and on behalf of

at

on 20

by (print name)

Position

Signature

Witness Signature

Name (print)

Address

.....

SIGNED FOR AND ON BEHALF OF LOCALSCRIPT LTD

Signed for and on behalf of Localscript Ltd

at

on 20

by (print name) **Montagu Franks**

Position **Director**

Signature

Witness Signature

Name (print)

Address

.....

THE SCHEDULE

**THIS IS THE SCHEDULE REFERRED TO IN THE DATA PROCESSING AGREEMENT
BETWEEN <<CLIENT NAME>> AND LOCALSCRIPT LTD**

1. GENERAL TERMS AND CONDITIONS

1.1 In addition to those defined terms set out elsewhere in the Agreement, the following definitions and rules of interpretation apply in this Agreement.

Agreement: means the front section together with the terms set out in this Schedule and any Annexes, all of which are attached and signed as relative hereto;

Business Day: any day other than a Saturday, Sunday or public holiday in England and Wales;

Data Security Breach: a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to the Shared Personal Data;

Data Subject: has the meaning set out in the UK GDPR and includes those categories of data subjects set out in Annex B, Part (i);

Data Protection Legislation: the UK General Data Protection Regulation (UK GDPR) as defined in section 3(10) of the Data Protection Act 2018, the Data Protection Act 2018, the Privacy and Electronic Communications (EC Directive) Regulations 2003, and any other laws and regulations relating to the processing of personal data and privacy which apply to a party, together with the guidance and codes of practice issued by the Information Commissioner's Office, in each case as amended, extended or re-enacted from time to time;

Deliverables: transcripts, anonymisation logs and re-identification keys produced by the Data Processor;

Personal Data: has the meaning set out in the UK GDPR;

Recordings: audio or audiovisual files supplied by the Data Controller to the Data Processor;

Sample Transcript: a transcript of a short extract of a Recording, produced by the Data Processor free of charge and without obligation on either party, to allow the Data Controller to assess the quality of the Services before entering into a paid engagement;

Services: the provision of the services to be provided by the Data Processor to the Data Controller under the Services Agreement and as detailed in Annex A (Part i) of this Schedule;

Services Agreement: the agreement between the Data Controller and the Data Processor for the provision of Services, being the Localscript Ltd Terms and Conditions unless the parties agree otherwise in writing, and if in written form as attached at Annex A (Part ii);

Shared Personal Data: the Personal Data and Special Categories of Personal Data to be shared by the Data Controller with the Data Processor and processed by the Data Processor for the Agreed Purpose as part of the Services, described within Annex B, Part (ii) to this Schedule;

Special Categories of Personal Data: the type of Personal Data referred to in Article 9(1) of the UK GDPR;

Term: has the meaning set out in Clause 2 of this Schedule.

1.2 The Schedule and the Annexes form part of this Agreement and shall have the same force and effect as if set out in full in the body of this Agreement, and any reference to this Agreement includes the Schedule and Annexes.

1.3 The headings in this Agreement are included for convenience only and shall be ignored in construing this Agreement.

1.4 A reference to a company shall include any company, corporation or other body corporate, wherever and however incorporated or established, and any university, institution or other body.

1.5 Unless the context otherwise requires, words in the singular shall include the plural and in the plural shall include the singular.

1.6 Unless the context otherwise requires, a reference to one gender shall include a reference to the other genders.

1.7 A reference to any party shall include that party's personal representatives, successors and permitted assigns.

1.8 A reference to a statute or statutory provision is a reference to it as amended, extended or re-enacted from time to time.

1.9 A reference to a statute or statutory provision shall include all subordinate legislation made from time to time under that statute or statutory provision.

1.10 A reference to writing or written includes email.

1.11 Any obligation on a party not to do something includes an obligation not to allow that thing to be done.

1.12 References to Clauses, Schedule and Annexes are to the clauses, schedule and annexes of this Agreement.

1.13 Any words following the terms including, include, in particular, for example or any similar expression shall be construed as illustrative and shall not limit the sense of the words, description, definition, phrase or term preceding those terms.

1.14 This Agreement applies to all processing of Shared Personal Data by the Data Processor on behalf of the Data Controller, including the production of any Sample Transcript, whether or not a paid engagement follows.

2. COMMENCEMENT AND DURATION

2.1 This Agreement shall commence on the Commencement Date and, subject to earlier termination, continue in force until expiry or termination of the Services Agreement and the deletion of all Shared Personal Data in accordance with Clause 3.2(n).

3. THE DATA PROCESSOR'S RESPONSIBILITIES

3.1 The Data Processor undertakes and warrants to the Data Controller to process the Shared Personal Data during the Term (i) only for the Agreed Purpose and (ii) unless otherwise obliged by applicable law, act only in accordance with the lawful written instructions reasonably given by the Data Controller to the Data Processor under this Agreement. In the event the Data Processor is obliged by applicable law to act outside the scope of, or contrary to, the instructions of the Data Controller, it agrees to inform the Data Controller as soon as reasonably practicable and prior to the processing activity, of such legal requirement, unless such law prohibits such information being notified to the Data Controller on important grounds of public interest.

3.2 In addition to the provision of Clause 3.1, the Data Processor shall:

(a) comply with the requirements set out in Annex D;

(b) take appropriate technical and organisational measures (in addition to those specified in Annex D) against unauthorised or unlawful processing of Shared Personal Data and against accidental loss or destruction of, or damage to, Shared Personal Data, including adequate backup and recovery procedures, to ensure a level of security appropriate to the risk which satisfies the requirements of Article 32 of the UK GDPR as a minimum;

(c) ensure that the individual named in Clause 3.3 is subject to a binding obligation of confidentiality in respect of the Shared Personal Data;

(d) (i) make available to the Data Controller all information necessary, and allow its data processing arrangements, procedures and documentation to be inspected by the Data Controller or its representatives, in order to ascertain compliance with the terms of this Agreement; and (ii) inform the Data Controller if, in its opinion, a request under this Clause 3.2(d) infringes the Data Protection Legislation. Inspections shall be on not less than 14 days' written notice, no more than once in any 12-month period unless a Data Security Breach has occurred, and shall be conducted remotely where reasonably practicable;

(e) (i) promptly, and **within 24 hours** of becoming aware of a Data Security Breach, inform the Data Controller of that breach and/or if any Shared Personal Data is lost, destroyed, damaged, corrupted or unusable, or is processed in a manner not expressly authorised by the Data Controller; and (ii) in the event any of the occurrences referred to in Clause 3.2(e)(i) arise, promptly provide such assistance to the Data Controller as is reasonably required and requested by the Data Controller to allow the Data Controller to manage such event and meet its obligations under the Data Protection Legislation, including taking steps to minimise loss or damage arising, notifying the breach to the supervisory authority and communicating the breach to Data Subjects. Notification under this Clause shall include, so far as known, the nature of the breach, the categories and approximate number of Data Subjects and records affected, the likely consequences, and the measures taken or proposed;

(f) send notification of Data Security Breaches, as per Clause 3.2(e), to the SPoC identified on the front section of this Agreement.

For Localscript Ltd, breach notifications should be sent to: monty@localscript.co.uk

For <<CLIENT NAME>>, breach notifications should be sent to: <<EMAIL ADDRESS>>;

(g) not process or transfer the Shared Personal Data outside the United Kingdom under any circumstances. All processing, storage and backup of Shared Personal Data takes place within the United Kingdom. Where the Data Controller wishes to vary this position, the variation must be recorded in writing and an appropriate transfer mechanism under Chapter V of the UK GDPR put in place before any transfer occurs;

(h) notify the Data Controller of any request or complaint received from Data Subjects and provide relevant copies within 48 hours of receipt to the appropriate address specified in Clause 3.2(f), and shall not respond to such requests unless authorised to do so by the Data Controller;

(i) promptly provide such assistance to the Data Controller as is reasonably required to allow the Data Controller to fulfil its obligations under the Data Protection Legislation with regard to all requests and complaints received from Data Subjects in the exercise of their rights under Chapter III of the UK GDPR, including the right of access to their Shared Personal Data held by, or on behalf of, the Data Controller;

(j) provide such assistance as is reasonably required to the Data Controller to ensure the Data Controller meets its obligations pursuant to Articles 32 to 36 of the UK GDPR, including data protection impact assessments and prior consultation with the Information Commissioner's Office;

(k) subject to any obligation to comply with applicable law, court or regulatory body, not divulge any Shared Personal Data, whether directly or indirectly, to any other application, system or third party without the express, explicit and informed consent of the Data Controller;

(l) keep a record of any processing of personal data it carries out on behalf of the Data Controller in accordance with Article 30(2) of the UK GDPR, and make that record available to the Data Controller on request;

(m) engage no sub-processor. The Data Processor confirms that no sub-processor is engaged in the performance of the Services. The Data Processor shall not engage any sub-processor without the prior specific written authorisation of the Data Controller. General authorisation is not sought or accepted. Where specific authorisation is given, the Data Processor shall impose on the sub-processor data protection obligations no less onerous than those set out in this Agreement and shall remain fully liable to the Data Controller for the sub-processor's performance;

(n) retain the Shared Personal Data and Deliverables for no longer than **30 days** following delivery of the Deliverables to the Data Controller, and on expiry of that period securely and permanently delete all copies, including from backups, confirming deletion in writing if requested. The Data Processor shall delete earlier on the Data Controller's written request, save where retention is required by law. The re-identification key shall be delivered to the Data Controller with the Deliverables and deleted at the same time as the Recordings, unless the Data Controller instructs otherwise in writing;

(o) not use the Shared Personal Data or Deliverables, or any part of them, to train, fine-tune, evaluate or improve any machine learning model, nor for any research, benchmarking, marketing or portfolio purpose;

(p) where the Data Controller requires a Disclosure and Barring Service (DBS) check in respect of the individual named in Clause 3.3, obtain one at the appropriate level and provide evidence of it before processing begins. The Data Processor does not represent that such a check is currently held;

(q) inform the Data Controller without undue delay if, in its opinion, an instruction from the Data Controller infringes the Data Protection Legislation, and may suspend performance of that instruction.

3.3 Named individual. The Data Processor confirms that **the Services are performed solely by Montagu Franks** (known as Monty Franks), a director of the Data Processor. No employee, contractor, freelancer, agency or transcription pool has access to the Shared Personal Data or Deliverables. The Data Processor shall not permit any other person to access the Shared Personal Data or Deliverables, or engage any additional person to perform the Services, without the Data Controller's prior written authorisation, and shall in that event comply with Clause 3.2(m).

3.4 Continuity and incapacity. Where the individual named in Clause 3.3 becomes unable to perform the Services by reason of illness, incapacity or death, the Data Processor shall notify the Data Controller as soon as reasonably practicable and shall, at the Data Controller's election, either (i) return all Shared Personal Data and Deliverables to the Data Controller by a route the Data Controller specifies, or (ii) securely and permanently delete them and certify that deletion in writing. No other person shall be given access to the Shared Personal Data in order to complete the Services without the Data Controller's prior written authorisation under Clause 3.3. The Data Processor maintains standing written instructions sufficient to give effect to this Clause.

3.5 During the Term, the Data Processor warrants and undertakes to comply with the Data Protection Legislation in so far as it is applicable to the Data Processor when processing the Shared Personal Data.

3.6 Roles. The parties acknowledge that in respect of the Shared Personal Data the Data Controller is the controller and the Data Processor is a processor. The Data Processor acts as a controller only in respect of its own business records — client contact details, correspondence, invoicing and accounting data. That processing falls outside this Agreement and is governed by the Data Processor's privacy notice.

4. THE DATA CONTROLLER'S RESPONSIBILITIES

4.1 The Data Controller acknowledges that the Data Processor is reliant on the Data Controller for direction as to the extent to which the Data Processor is entitled to use and process the Shared Personal Data. The Data Controller warrants that the processing of the Shared Personal

Data by the Data Processor under, or in relation to, this Agreement will not breach the Data Protection Legislation. The Data Controller further warrants and undertakes that it shall comply with all Data Protection Legislation for so long as the Data Controller is in receipt of the Services.

4.2 The Data Controller warrants that it has:

(a) a lawful basis under Article 6 of the UK GDPR for the processing it instructs;

(b) where Special Categories of Personal Data are or may be present in the Recordings, a condition under Article 9 of the UK GDPR (which, for academic research, will commonly be Article 9(2)(j) together with Schedule 1 Part 1 of the Data Protection Act 2018);

(c) obtained all necessary consents or approvals, including research ethics approval where applicable, and provided all necessary information to Data Subjects, including that transcription may be carried out by an external provider.

4.3 The Data Controller shall promptly provide such assistance to the Data Processor as is reasonably required to allow the Data Processor to fulfil its obligations under the Data Protection Legislation.

4.4 The Data Controller shall provide the Data Processor with details of the Data Controller's data retention requirements for Shared Personal Data processed under, or in relation to, this Agreement, and the Data Processor shall take reasonable steps to hold all Shared Personal Data processed on the Data Controller's behalf for the time periods specified, subject to Clause 3.2(n).

4.5 The Data Controller is responsible for selecting the mechanism by which Recordings are transferred to the Data Processor, in accordance with Annex D. The Data Controller shall retain its own copy of every Recording.

5. TERMINATION

5.1 Either party ("the First Party") may terminate this Agreement with immediate effect by serving written notice on the other party ("the Second Party") in the event:

(a) the Second Party is in breach of a material term of this Agreement which, in the case of a breach capable of remedy, shall not have been remedied within twenty-one (21) days from the date of receipt by the Second Party of a notice from the First Party identifying the breach and requiring its remedy; or

(b) the Second Party becomes insolvent, has a receiver, administrator, or administrative receiver appointed over the whole or any part of its assets, enters into any compound with creditors, or has an order made or resolution passed for it to be wound up (otherwise than in furtherance of a scheme for solvent amalgamation or reconstruction).

6. CONSEQUENCES OF TERMINATION

6.1 On termination or expiry of this Agreement for any reason, the Data Processor shall on the instructions of the Data Controller immediately delete or deliver to the Data Controller all Shared Personal Data and all copies of information and data provided by the Data Controller to the Data Processor in connection with the Services, and certify to the Data Controller that it has not retained any copies of Shared Personal Data or other information or data, unless law requires storage of the personal data. In either case any remaining copies shall be deleted within 30 days.

6.2 On termination or expiry of this Agreement, the following clauses shall continue in force: Clauses 6, 7, 8 and 13.

6.3 Termination or expiry of this Agreement shall not affect any rights, remedies, obligations or liabilities of the parties that have accrued up to the date of termination or expiry, including the right to claim damages in respect of any breach of the Agreement which existed at or before the date of termination or expiry.

7. LIABILITY

7.1 Neither party excludes or limits liability to the other party for death or personal injury caused by negligence, fraud or breach of statutory duty, and/or any matter for which it would be unlawful for the parties to exclude liability, including any matter for which limitation is prohibited by the Data Protection Legislation.

7.2 Subject to Clause 7.1, neither party shall in any circumstances be liable, whether in contract, tort (including for negligence and/or breach of statutory duty howsoever arising), misrepresentation (whether innocent or negligent), restitution or otherwise, for:

(a) any loss (whether direct or indirect) of profits, business, business opportunities, revenue, turnover, reputation or goodwill; or

(b) loss (whether direct or indirect) of anticipated savings or wasted expenditure (including management time).

7.3 Clause 7.2 shall not prevent claims for:

(a) direct financial loss that is not excluded under any of the categories set out in Clause 7.2(a), which shall include any penalties or fines issued by a Data Protection Authority; or

(b) tangible property or physical damage.

7.4 Except as expressly stated in this Agreement, all warranties, conditions and terms relating to the subject matter of this Agreement, whether express or implied by statute, common law or otherwise, are hereby excluded to the extent permitted by law.

7.5 Subject to Clause 7.1, each party's aggregate liability for loss arising (whether directly or indirectly) from its acts or omissions under or in relation to this Agreement shall in no event exceed **twice the value of sums actually received by the Data Processor under the Services Agreement, or £2,000, whichever is the greater**. The cap of liability expressed in this Clause 7.5 shall not apply to any regulatory fine imposed by a Supervisory Authority.

7.6 Where the Data Processor produces a Sample Transcript free of charge and no paid engagement has yet been agreed, the cap in Clause 7.5 applies as if the Sample Transcript had been produced under the Services Agreement.

7.7 For the avoidance of doubt, the provisions of this Clause 7 shall only apply to matters arising under this Agreement. Any liability arising from or in relation to the Services generally shall be in accordance with the terms of the Services Agreement.

7.8 Insurance. The Data Processor shall maintain professional indemnity and cyber liability insurance appropriate to the Services from the commencement of the first paid engagement under the Services Agreement, and shall provide details of cover on request. The Data Processor does not represent that such insurance is in force before that date.

8. FORCE MAJEURE

Neither party shall be deemed to be in breach of this Agreement if it is unable to carry out any provision of it for any reason beyond its control, including (without limiting the generality of the foregoing) acts of God, legislation, war, fire, flood, failure of power supply, loss of internet connectivity, equipment failure, serious illness, civil commotion and industrial action.

9. ASSIGNATION

9.1 Except as expressly provided for in this Agreement, the Data Processor shall not be entitled to:

(a) assign or transfer any or all of its rights and/or obligations under this Agreement (or purport to do so); or

(b) sub-license or sub-contract any or all of its obligations under this Agreement (or purport to do so);

save, in either case, with the prior written consent of the Data Controller.

10. GENERAL

10.1 Except as otherwise expressly provided in this Agreement, none of the terms and conditions of this Agreement shall be enforceable by any person who is not a party to it.

10.2 Each provision of this Agreement shall be construed separately and, save as otherwise expressly provided herein, none of the provisions hereof shall limit or govern the extent, application or construction of any other of them, and the remaining provisions of this Agreement shall continue in full force and effect.

10.3 No waiver by either party of any of the requirements hereof or of any of its rights hereunder shall be effective unless given in writing and signed by or on behalf of that party, and no forbearance, delay or indulgence by either party in enforcing the provisions of this Agreement shall prejudice or restrict the rights of that party, nor shall any waiver by either party of any of the requirements hereof or any of its rights hereunder release the other from full performance of its obligations stated herein.

10.4 This Agreement and any documents referred to herein constitutes the entire understanding between the parties and supersedes and extinguishes all (if any) prior drafts, agreements, understandings, undertakings, representations, warranties and/or arrangements of any nature whatsoever (whether or not in writing) between the parties in connection therewith.

10.5 Nothing in this Agreement shall be construed as establishing or implying any partnership or joint venture between the parties, and nothing in this Agreement shall be deemed to constitute one of the parties as the agent of the other.

10.6 Subject to Clause 6, the parties shall be entitled to amend any details of this Agreement at any time provided that any such amendment is recorded in writing by both parties.

10.7 The rights and remedies provided under this Agreement are in addition to, and not exclusive of, any rights or remedies provided by law.

10.8 The Data Processor shall provide all other reasonable assistance at all times during the term of this Agreement for the purposes of carrying out an audit of all confidentiality, activities, performance, security and integrity in connection with this Agreement.

10.9 If any provision of this Agreement conflicts with the Data Protection Legislation, the Data Protection Legislation prevails.

11. COUNTERPARTS

This Agreement may be executed in two counterparts which, taken together, shall constitute one and the same document. Either party may enter into this Agreement by signing either of such counterparts.

12. NOTICES

A notice given to a party under or in connection with this Agreement, other than a request in relation to Data Security Breaches (Clause 3.2(e)–(f)) and Data Subjects' rights (Clause 3.2(h)), shall be in writing and signed by or on behalf of the party giving it and addressed to the registered office of a party or to the email address of the <<CLIENT NAME>> SPoC or the Localscript Ltd SPoC (as appropriate).

Delivery methods and deemed delivery times are as set out below:

Delivery method	Deemed delivery date and time
Delivery by hand	At time of delivery
Pre-paid first class recorded delivery post	9.00 am on the second Business Day after posting, or at the time recorded by the delivery service
Email	From receipt of delivery confirmation

13. GOVERNING LAW AND JURISDICTION

This Agreement shall be governed and construed in all respects in accordance with the laws of England and Wales, and the Courts of England and Wales shall have exclusive jurisdiction to settle any dispute or claim that arises out of or in connection with this Agreement, or its subject matter or formation.

ANNEXES

THESE ARE THE ANNEXES REFERRED TO IN THE FOREGOING DATA PROCESSING AGREEMENT BETWEEN <<CLIENT NAME>> AND LOCALSCRIPT LTD

ANNEX A

Part (i) — Description of the Services

<<Description of the project and the recordings>>.

Localscript Ltd is to transcribe these recordings into a written format and, in doing so, to:

- convert speech to text and attribute speech to individual speakers;
- review the full transcript against the audio and correct it;
- pseudonymise personal names, place names, organisations and other identifying details, consistently across every transcript in the project;
- produce an anonymisation log recording what was changed and to what;
- produce a re-identification key linking pseudonyms to the original identifiers, delivered to the Data Controller and held separately from the transcripts;
- format the transcript for direct import into NVivo, ATLAS.ti or MAXQDA, or to the Data Controller's own template where supplied;
- apply timestamps and mark passages that cannot be reliably determined from the audio as unclear rather than inferring them;
- deliver the completed Deliverables and securely delete all copies in accordance with Clause 3.2(n).

Part (ii) — Services Agreement

Services are provided under the **Localscript Ltd Terms and Conditions**, published at localscript.co.uk, unless the parties agree otherwise in writing.

Where the Data Controller requires Services to be provided under its own conditions of contract for the purchase of goods and services, those conditions shall be attached here and shall constitute the Services Agreement.

<<Attach where applicable>>

ANNEX B

Part (i) — Categories of Data Subjects

The Data Subjects are:

- research participants recorded in the Recordings — <<describe who the interviewees are>>;
- interviewers, moderators and researchers present in the Recordings;
- third parties incidentally named or described by speakers.

Part (ii) — Shared Personal Data

The content of the interviews recorded is dependent on the Data Subject who is answering the questions. Although information such as surname, address, date of birth, religion and ethnicity will not be directly requested in audio format, the Data Subject may include such information in their responses.

Recordings of interviews conducted by <<CLIENT NAME>> will be sent to Localscript Ltd for transcription. File names will not include any personal information. However, personal information may be mentioned throughout an interview and therefore be present on the audio files.

Shared Personal Data may therefore include:

- voice recordings;
- names of participants, interviewers and third parties;
- names of relatives;
- place names, employers, institutions and other identifying details spoken aloud;
- details of hospital admissions, medical treatments and health conditions;
- any personal information disclosed by a speaker in the course of the recording.

Special Categories of Personal Data. The Recordings may contain, without the Data Processor's prior knowledge, data revealing health conditions, racial or ethnic origin, religious or

philosophical beliefs, political opinions, trade union membership, sex life or sexual orientation. The Data Processor processes such data only to the extent necessary to provide the Services.

ANNEX C

Transfers outside the United Kingdom

Not applicable.

Localscript Ltd does not transfer Shared Personal Data outside the United Kingdom. All processing, storage and backup takes place on equipment located within the United Kingdom.

No part of the processing, storage or backup of Shared Personal Data is provided by, routed through, or hosted on infrastructure operated by any third party, whether within or outside the United Kingdom.

Where the Data Controller selects a file transfer service to deliver Recordings to the Data Processor, or to receive Deliverables, that service is chosen and controlled by the Data Controller in accordance with Annex D, paragraph 1. Such a service is not a sub-processor of the Data Processor and does not form part of the processing described in Annex A.

ANNEX D

Technical and Organisational Security Measures

This is Annex D referred to in the foregoing Data Processing Agreement between <<CLIENT NAME>> and Localscript Ltd.

1. Transfer to Localscript. Recordings are transferred using the Data Controller's own secure file transfer service — ordinarily the institutional service the Data Controller is already approved to use, for example Jisc FileSender or an institutional cloud service with UK data residency. The Data Controller selects the transfer mechanism; Localscript Ltd does not introduce one. Recordings are never sent as email attachments or via consumer file-sharing services. Where the Data Controller has no suitable transfer service available, an encrypted transfer route will be agreed in writing between the parties before any Shared Personal Data is transferred, and Localscript Ltd will identify any third party involved in that route so that the Data Controller can assess it.

2. Processing location. All processing is carried out on a single machine owned and controlled by Localscript Ltd, located in the United Kingdom. Shared Personal Data is not stored on a server, and is not synchronised to any cloud storage service.

3. Automated tooling. Speech-to-text conversion, speaker segmentation, and the initial detection of identifying details are performed by open-source models installed and executed locally on that machine. **No audio, transcript or metadata is transmitted to any external service, application programming interface, or third-party provider at any stage of processing.**

4. Human review. Automated output is not delivered unreviewed. The individual named in Clause 3.3 reviews the full transcript against the audio, corrects speaker attribution, and confirms or amends every identifying detail flagged for pseudonymisation before delivery. Passages that cannot be reliably determined from the audio are marked as unclear rather than inferred.

5. Encryption at rest. Full-disk encryption on the processing machine. Backups are encrypted and held on removable media within the United Kingdom.

6. Access control. Device-level authentication. Sole access by the individual named in Clause 3.3. No shared accounts. No cloud synchronisation of working directories.

7. Return of Deliverables. Deliverables are returned by the same route used for transfer to Localscript Ltd, or by another route the Data Controller specifies in writing. Deliverables are not sent as unencrypted email attachments.

8. Deletion. Secure erasure of Recordings, Deliverables and backup copies within 30 days of delivery, or earlier on the Data Controller's written request. Written confirmation of deletion provided on request.

9. Organisational measures. Written retention and deletion schedule. Registered with the Information Commissioner's Office, registration reference ZC217301. Record of processing activities maintained under Article 30(2) UK GDPR. DBS check obtained on request where an engagement requires it. Binding confidentiality obligation on the named individual.

10. Supporting documentation. The Data Processor's Information Security Policy and Retention and Deletion Policy are provided on request and may be attached to this Annex where the Data Controller's procurement process requires it.

11. Certifications not held. Localscript Ltd **does not** hold ISO 27001, Cyber Essentials or Cyber Essentials Plus certification as at the Commencement Date, and makes no representation to that effect. Professional indemnity and cyber liability insurance is put in place from the commencement of the first paid engagement, in accordance with Clause 7.8.

Localscript Ltd is registered in England and Wales, company no. 17388152. Registered with the Information Commissioner's Office, reference ZC217301. monty@localscript.co.uk