

DATA PROCESSING AGREEMENT

Standard Terms - Incorporated into the Master Services Agreement

Version 2.1 | 6 October 2026

No separate customer signature is required. This DPA becomes binding through incorporation into the Agreement.

Data Processing Agreement

This Data Processing Agreement (DPA) forms part of the Agreement between the Company and TeleFlow and applies automatically where TeleFlow Processes Company Personal Data on behalf of the Company in connection with the Services.

The Company is the entity identified as the Company in the Agreement.

TeleFlow is TeleFlow Ltd, a company incorporated in England and Wales with company number 09027630 and registered office at Unit J1, 6 Vantage Way, Poole, Dorset, England, BH12 4NU.

This DPA takes effect on the Effective Date and forms part of the Agreement without requiring separate execution.

Background

- A. The parties have entered into an Agreement under which TeleFlow provides telecommunications, call handling, recording, transcription and/or related services to the Company.
- B. In providing the Services, TeleFlow may process Personal Data on behalf of the Company. Depending on the Company's role in relation to that Personal Data, TeleFlow will act as a Processor or as a Sub-processor.
- C. The parties enter into this DPA to satisfy the requirements applying to controller-processor and processor-sub-processor arrangements under Applicable Data Protection Law, including Article 28 of the UK GDPR and, where applicable, Article 28 of the EU GDPR.
- D. TeleFlow undertakes its own processing of Company Personal Data in-house in the United Kingdom, except that TeleFlow may use any of the Approved Sub-processors listed in Schedule 2 for automated speech-to-text transcription and related processing in accordance with clauses 10 and 11.

Contents

- 1. Definitions and interpretation
- 2. Scope, roles and precedence
- 3. Company instructions and responsibilities
- 4. TeleFlow processing obligations
- 5. Confidentiality and personnel
- 6. Security of processing
- 7. Personal Data Breaches
- 8. Data subject rights
- 9. DPIAs, consultations and regulatory assistance
- 10. Sub-processors
- 11. International transfers and data location
- 12. Records, information and audits
- 13. Return and deletion
- 14. Liability
- 15. Term and termination
- 16. General
- Schedule 1 - Details of Processing
- Schedule 2 - Approved Sub-processors
- Schedule 3 - Technical and Organisational Measures

1. Definitions and interpretation

- 1.1 Agreement means the Master Services Agreement between TeleFlow and the Company, together with each applicable Sales Contract, Order Form or Schedule and any other document expressly incorporated into them, as amended from time to time.
- 1.2 Applicable Data Protection Law means all laws and regulations relating to privacy, data protection and the processing of Personal Data that apply to a party or the Processing under this DPA, including, as applicable: (a) the UK GDPR; (b) the Data Protection Act 2018; (c) the Privacy and Electronic Communications (EC Directive) Regulations 2003; (d) the EU GDPR; and (e) any legislation amending, replacing or supplementing the foregoing.
- 1.3 Controller, Data Subject, Personal Data, Personal Data Breach, Processing (and Process), Processor, Special Category Data and Supervisory Authority have the meanings given in Applicable Data Protection Law.
- 1.4 Company means the Company as defined in the Master Services Agreement.
- 1.5 Company Personal Data means Personal Data processed by TeleFlow on behalf of the Company in connection with the Services.
- 1.6 Effective Date means the date on which the Agreement becomes binding on the Company or, if later, the date on which TeleFlow first Processes Company Personal Data on behalf of the Company.
- 1.7 EU GDPR means Regulation (EU) 2016/679 as it applies in the European Economic Area.
- 1.8 Restricted Transfer means a transfer of Personal Data to a country or recipient where Applicable Data Protection Law requires a transfer mechanism or additional safeguard.
- 1.9 Services means the services provided by TeleFlow under the Agreement, including any enabled call recording or speech-to-text functionality.
- 1.10 Sub-processor means any third party appointed by or on behalf of TeleFlow to Process Company Personal Data on behalf of the Company, excluding TeleFlow personnel.
- 1.11 UK GDPR has the meaning given in section 3(10) of the Data Protection Act 2018, as amended from time to time.
- 1.12 References to a law include amendments, re-enactments and subordinate legislation made under it. If there is a conflict between this DPA and the Agreement on a matter concerning the protection or Processing of Company Personal Data, this DPA prevails to the extent of that conflict.

2. Scope, roles and precedence

- 2.1 This DPA applies to all Processing of Company Personal Data by TeleFlow in connection with the Services.
- 2.2 Where the Company is a Controller, the Company is the Controller and TeleFlow is the Processor. Where the Company is itself a Processor acting for one or more underlying Controllers, TeleFlow is a Sub-processor and references in this DPA to the Company's rights or instructions include rights or instructions validly passed down from the relevant underlying Controller.
- 2.3 Schedule 1 describes the subject matter, nature, purpose and duration of the Processing, the types of Personal Data and the categories of Data Subject.
- 2.4 This DPA forms part of the Agreement. Except as expressly modified by this DPA, the Agreement remains in force.

3. Company instructions and responsibilities

- 3.1 The Company instructs TeleFlow to Process Company Personal Data only as necessary to provide, secure, support and maintain the Services in accordance with the Agreement, the Company's

configuration of the Services, this DPA and any further documented instructions that are consistent with the Agreement.

- 3.2 The Company is responsible for ensuring that its instructions are lawful and that it has all necessary rights, permissions and lawful bases to disclose Company Personal Data to TeleFlow and to instruct the Processing.
- 3.3 Without limiting clause 3.2, the Company is responsible for satisfying any transparency, notification, consent or other legal requirements applicable to the recording, monitoring and transcription of telephone or other communications, including any requirements applicable to employees, agents, callers and call recipients.
- 3.4 Where Company Personal Data includes Special Category Data or criminal offence data, the Company is responsible for identifying and satisfying any additional condition or safeguard required by Applicable Data Protection Law.
- 3.5 Where the Company acts as a Processor, it warrants that: (a) it is authorised by each relevant Controller to appoint TeleFlow as a Sub-processor; (b) its instructions to TeleFlow are consistent with the Controller's instructions; and (c) it may grant the general authorisation for Sub-processors set out in clause 10.
- 3.6 The Company shall not instruct TeleFlow to Process Personal Data in a way that would cause TeleFlow to breach Applicable Data Protection Law. If TeleFlow reasonably believes an instruction infringes Applicable Data Protection Law, TeleFlow shall inform the Company without undue delay and may suspend the affected Processing until the instruction is clarified, amended or confirmed to be lawful.

4. TeleFlow processing obligations

- 4.1 TeleFlow shall Process Company Personal Data only on the Company's documented instructions, including in relation to transfers, unless TeleFlow is required to Process the data by applicable law. Where legally permitted, TeleFlow shall inform the Company of that legal requirement before Processing.
- 4.2 TeleFlow shall not sell Company Personal Data or use it for advertising. TeleFlow shall not use Company Personal Data to train or improve third-party or shared artificial intelligence or machine-learning models unless the Company has expressly authorised that use in writing.
- 4.3 TeleFlow shall Process only the Company Personal Data reasonably necessary for the Services and shall take reasonable steps to ensure that Personal Data is accurate to the extent relevant to TeleFlow's role.
- 4.4 TeleFlow shall promptly notify the Company if it receives a legally binding request from a public authority for disclosure of Company Personal Data, unless prohibited by law. Where appropriate and lawful, TeleFlow shall take reasonable steps to challenge a request that it reasonably considers unlawful, overbroad or inconsistent with applicable transfer safeguards.

5. Confidentiality and personnel

- 5.1 TeleFlow shall ensure that persons authorised to Process Company Personal Data are bound by appropriate contractual or statutory duties of confidentiality and receive access only to the extent necessary for their duties.
- 5.2 TeleFlow shall take reasonable steps to ensure that personnel with access to Company Personal Data receive appropriate data protection and information security awareness training.
- 5.3 Access to Company Personal Data shall be removed or adjusted when it is no longer required for an individual's role.

6. Security of processing

- 6.1 Taking into account the state of the art, implementation costs, the nature, scope, context and purposes of Processing and the risk to Data Subjects, TeleFlow shall implement and maintain appropriate technical

and organisational measures designed to protect Company Personal Data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Company Personal Data.

- 6.2 The measures shall include, as appropriate to the risk, controls relating to confidentiality, integrity, availability and resilience; access control; secure transmission; system maintenance and patching; backup and recovery; incident management; and regular review of the effectiveness of relevant controls.
- 6.3 The minimum categories of measures currently committed to by TeleFlow are set out in Schedule 3. TeleFlow may update those measures where the update does not materially reduce the overall level of protection for Company Personal Data.
- 6.4 The Company acknowledges that security is a shared responsibility and shall use the Services in accordance with reasonable security instructions provided by TeleFlow, including maintaining the security of its own credentials, endpoints, integrations and administrator accounts.

7. Personal Data Breaches

- 7.1 TeleFlow shall notify the Company without undue delay after becoming aware of a Personal Data Breach affecting Company Personal Data and, so far as reasonably practicable, within 24 hours of becoming aware.
- 7.2 The initial notice shall contain information then reasonably available to TeleFlow, which may include: (a) the nature of the breach; (b) the categories and approximate number of affected Data Subjects and records, where known; (c) likely consequences; and (d) measures taken or proposed to contain, investigate and remediate the breach. TeleFlow may provide information in phases as it becomes available.
- 7.3 TeleFlow shall take reasonable steps to contain and remediate the breach and shall provide reasonable assistance to enable the Company to meet its breach notification obligations.
- 7.4 Notification or assistance under this clause does not constitute an admission of fault or liability by TeleFlow.

8. Data subject rights

- 8.1 Taking into account the nature of the Processing, TeleFlow shall provide reasonable assistance through appropriate technical and organisational measures to enable the Company to respond to requests by Data Subjects exercising rights under Applicable Data Protection Law.
- 8.2 If TeleFlow receives a request from a Data Subject relating to Company Personal Data, TeleFlow shall not respond substantively except on the Company's documented instruction or where required by law, and shall forward or otherwise notify the Company of the request without undue delay where it can reasonably identify the relevant Company.

9. DPIAs, consultations and regulatory assistance

- 9.1 Taking into account the nature of the Processing and information available to TeleFlow, TeleFlow shall provide reasonable assistance to the Company with: (a) security obligations; (b) Personal Data Breach assessments and notifications; (c) data protection impact assessments; and (d) prior consultation with a Supervisory Authority, in each case to the extent required by Applicable Data Protection Law.
- 9.2 Unless the assistance is required because of TeleFlow's breach of this DPA or Applicable Data Protection Law, the parties may agree reasonable charges for substantial assistance that goes beyond TeleFlow's standard compliance information and support.

10. Sub-processors

- 10.1 The Company gives TeleFlow general written authorisation to engage the direct Sub-processors listed in Schedule 2 (the Approved Sub-processors). The Company expressly authorises TeleFlow to select,

switch between and use any one or more of the Approved Sub-processors for any individual call, transcription request, batch or workload at TeleFlow's reasonable discretion, including for reasons of transcription quality, language support, latency, availability, resilience, technical compatibility or cost. No additional case-by-case notice or consent is required for TeleFlow to route Processing between Approved Sub-processors already listed in Schedule 2.

- 10.2** TeleFlow shall ensure that each Approved Sub-processor is engaged under written terms that impose data protection obligations appropriate to the delegated Processing and that satisfy the requirements applicable to TeleFlow's appointment of a Sub-processor under Applicable Data Protection Law.
- 10.3** TeleFlow remains responsible to the Company for the performance of its Sub-processors' data protection obligations to the extent required by Applicable Data Protection Law.
- 10.4** TeleFlow shall give the Company at least 30 days' prior notice of any intended addition or replacement of a direct Sub-processor that is not already an Approved Sub-processor listed in Schedule 2 and that will Process Company Personal Data, unless an urgent change is reasonably necessary to address a security, legal or service-continuity issue, in which case notice shall be given as soon as reasonably practicable.
- 10.5** The Company may object to a proposed new direct Sub-processor on reasonable, documented data protection grounds by notifying TeleFlow before the proposed appointment takes effect. This objection right does not apply to TeleFlow's selection or switching between Approved Sub-processors already listed in Schedule 2. The parties shall work in good faith to address a valid objection to a new Sub-processor. If no reasonable solution is available, TeleFlow may permit the Company to discontinue the materially affected feature or Service without penalty for the discontinued element, or either party may exercise any applicable termination right under the Agreement.
- 10.6** An Approved Sub-processor may itself use downstream processors where permitted under its contract with TeleFlow and Applicable Data Protection Law. TeleFlow shall maintain appropriate contractual flow-down protections for such Processing and shall rely on the applicable provider's published or contractually maintained downstream sub-processor arrangements.

11. International transfers and data location

- 11.1** TeleFlow's own Processing of Company Personal Data is undertaken in-house in the United Kingdom. For automated transcription and related speech processing, TeleFlow may route Company Personal Data to any Approved Sub-processor listed in Schedule 2 in accordance with clause 10. The Company acknowledges that, depending on the provider selected by TeleFlow for a particular workload, such Processing may occur in the European Union or in the United States as specified in Schedule 2.
- 11.2** The parties acknowledge that the United Kingdom is outside the EEA. Where the EU GDPR applies to a transfer from the EEA to TeleFlow in the United Kingdom, the parties may rely on an applicable European Commission adequacy decision for the United Kingdom for so long as that decision remains valid and applicable, or otherwise on an appropriate transfer mechanism required by Applicable Data Protection Law.
- 11.3** Where TeleFlow selects Google Cloud Speech-to-Text, TeleFlow shall configure the service to use the EU regional or EU multi-regional Speech-to-Text endpoint for Company audio and transcript Processing and shall keep Google's optional Speech-to-Text data-logging/model-improvement programme disabled unless the Company has expressly authorised otherwise in writing.
- 11.4** Where TeleFlow selects OpenAI or ElevenLabs and the relevant Processing occurs in the United States, TeleFlow shall ensure that the Restricted Transfer is covered by a lawful transfer mechanism applicable to the relevant data and relationship. Such mechanism may include an applicable adequacy regulation or data-bridge arrangement, the EU Standard Contractual Clauses, the UK Addendum to the EU Standard Contractual Clauses, or another lawful safeguard incorporated into or entered under the relevant provider's data processing terms. TeleFlow shall complete any transfer risk assessment, data protection test or equivalent assessment required of it by Applicable Data Protection Law.

- 11.5 TeleFlow shall not opt Company Personal Data into optional provider programmes that use such data to train or improve shared or third-party artificial intelligence or machine-learning models unless the Company has expressly authorised that use in writing. In particular, TeleFlow shall keep Google Speech-to-Text data logging/model improvement disabled, shall not opt OpenAI API Customer Data into model training, and shall maintain ElevenLabs' available account-level model-improvement opt-out for Company Personal Data. Provider retention will otherwise be governed by the applicable provider terms and the retention controls available for the service and account used by TeleFlow.
- 11.6 TeleFlow shall not otherwise make a Restricted Transfer of Company Personal Data unless the transfer is permitted under Applicable Data Protection Law. If a transfer mechanism relied upon by TeleFlow or an Approved Sub-processor ceases to be valid or applicable, TeleFlow shall take reasonable steps to implement a lawful replacement mechanism or cease the affected transfer, and the parties shall cooperate in good faith where additional documentation is reasonably required.

12. Records, information and audits

- 12.1 TeleFlow shall maintain records of its Processing activities to the extent required by Applicable Data Protection Law and shall make available to the Company information reasonably necessary to demonstrate compliance with the obligations applicable to TeleFlow under Article 28 of the UK GDPR and, where applicable, Article 28 of the EU GDPR.
- 12.2 TeleFlow shall allow for and contribute to reasonable audits or inspections by the Company or an independent auditor mandated by the Company, subject to the safeguards in this clause.
- 12.3 Except where an audit is required by a Supervisory Authority, follows a material Personal Data Breach, or is reasonably necessary because the Company has credible evidence of material non-compliance, audits shall: (a) occur no more than once in any 12-month period; (b) be conducted on at least 20 business days' prior written notice; (c) take place during normal business hours; (d) avoid unreasonable disruption to TeleFlow's business; and (e) be limited to systems, records and facilities relevant to the Company's Processing.
- 12.4 The Company and its auditor shall protect TeleFlow's confidential information, security information and information concerning other customers. Auditors must be suitably qualified and not be direct competitors of TeleFlow.
- 12.5 The Company shall bear its own audit costs and TeleFlow's reasonable costs of providing exceptional audit assistance, unless the audit identifies a material breach by TeleFlow, in which case TeleFlow shall bear its own reasonable costs relating to remediation and verification of that breach.
- 12.6 Nothing in this clause limits the powers of a competent Supervisory Authority.
- 12.7 TeleFlow may maintain internal data protection impact assessments, transfer risk assessments, data protection tests and similar accountability records relating to the Services. Such internal assessments do not form part of the Agreement and do not require execution by the Company. On reasonable request, TeleFlow shall provide information reasonably necessary to demonstrate compliance, subject to appropriate confidentiality, security and legal restrictions.

13. Return and deletion

- 13.1 At the end of the provision of Services involving Processing, and at the Company's choice, TeleFlow shall delete or return Company Personal Data and delete existing copies, unless applicable law requires continued storage.
- 13.2 Where immediate deletion from backups or immutable archives is not reasonably practicable, TeleFlow may retain such copies until they are overwritten or deleted in the ordinary backup cycle, provided they remain protected, are put beyond normal operational use and are not Processed for any other purpose.
- 13.3 During the term of the Agreement, deletion and retention of Company Personal Data shall follow the Company's documented configuration or instructions and any retention functionality described in the Services, subject to legal retention requirements.

14. Liability

- 14.1** Each party remains responsible for its own compliance with Applicable Data Protection Law and for any liability directly imposed on it by law.
- 14.2** To the extent permitted by law, any liability arising under or in connection with this DPA is subject to the exclusions and limitations of liability in the Agreement as if references there to the Agreement included this DPA.
- 14.3** Nothing in this DPA excludes or limits liability to the extent that such exclusion or limitation is prohibited by Applicable Data Protection Law or other applicable law.

15. Term and termination

- 15.1** This DPA takes effect on the Effective Date and continues for so long as TeleFlow Processes Company Personal Data on behalf of the Company.
- 15.2** Clauses that by their nature are intended to survive termination, including confidentiality, international transfer safeguards, return and deletion, audit rights relating to the term, and liability provisions, shall survive to the extent necessary to give them effect.

16. General

- 16.1** TeleFlow may amend this DPA in accordance with the amendment provisions of the Agreement. TeleFlow shall not make an amendment that materially reduces the overall protection afforded to Company Personal Data during the applicable term without providing the notice required under the Agreement. Changes to Approved Sub-processors are additionally governed by clause 10 of this DPA.
- 16.2** If any provision of this DPA is held invalid or unenforceable, it shall be modified to the minimum extent necessary to make it valid and enforceable, and the remaining provisions continue in effect.
- 16.3** Notices under this DPA shall be given in accordance with the notice provisions of the Agreement, including any provisions permitting electronic legal or data-protection notices.
- 16.4** This DPA is governed by the law and jurisdiction specified in the Agreement. If the Agreement does not specify governing law and jurisdiction, this DPA is governed by the laws of England and Wales and the courts of England and Wales have exclusive jurisdiction, subject always to the powers and jurisdiction of competent Supervisory Authorities under Applicable Data Protection Law.

Schedule 1 - Details of Processing

Subject matter	Provision of TeleFlow telecommunications, call handling, recording, transcription and related services to the Company.
Duration	For the term of the Agreement and any period required to complete return, deletion, backup expiry or legally required retention in accordance with this DPA and the Company's documented configuration or instructions.
Nature of Processing	Receipt, collection, recording, organisation, structuring, transmission, routing, storage, retrieval, consultation, analysis necessary for service operation, automated speech-to-text transcription, support, security, backup, deletion and other Processing necessary to provide the Services.
Purpose	To provide and operate the Services on the Company's behalf, including call routing and handling, any enabled call recording, automated speech-to-text transcription, service administration, security, support and troubleshooting.
Frequency	As initiated by the Company and its users or end customers; potentially continuous while the Services are in active use.

Categories of Data Subjects

- The Company's and underlying controllers' customers, subscribers, clients and prospects.
- Callers, call recipients and other participants in telephone or voice communications.
- Employees, workers, contractors, agents and representatives of the Company, underlying controllers and their counterparties.
- Users and administrators of the Services.
- Other individuals whose Personal Data is contained in call audio, transcripts, notes or related service data.

Types of Personal Data

- Voice and audio data, including call recordings where recording is enabled.
- Speech-to-text transcripts and other text derived from call audio.
- Telephone numbers, caller line identification, dialled numbers and related contact identifiers.
- Names, usernames, account identifiers and organisational details where supplied through the Services or contained in communications.
- Call metadata, such as timestamps, duration, routing or queue information, call identifiers, extension numbers and service events.
- The free-form contents of communications, which may include any Personal Data disclosed during a call.
- Technical and security data reasonably necessary to provide, administer and protect the Services, such as authentication, audit and diagnostic records.

Special Category / Sensitive Data

TeleFlow does not require Special Category Data as a condition of providing standard call transcription services. However, because telephone conversations are free-form, Company Personal Data may incidentally or foreseeably include health information, biometric information in the ordinary sense of voice characteristics (without TeleFlow using voice data for unique biometric identification), racial or ethnic origin, religious or philosophical beliefs, political opinions, trade union information, sex life or sexual orientation, or criminal

offence information. Such data will be Processed only as part of the Company's instructed use of the Services and subject to the additional requirements of Applicable Data Protection Law.

Company obligations and rights

The Company retains all rights and obligations of a Controller under Applicable Data Protection Law where it acts as Controller. Where the Company acts as a Processor, it shall exercise rights and provide instructions only to the extent authorised by the relevant underlying Controller.

Schedule 2 - Approved Sub-processors

Pre-authorised direct transcription Sub-processors

Provider	Processing details and safeguards
Google Cloud Platform	Service / purpose: Cloud Speech-to-Text for automated transcription of call audio. Data: Call audio/voice submitted for transcription; returned transcript; request and technical metadata necessary to provide the service. Processing location: European Union for Speech-to-Text Company Personal Data submitted through Google's EU regional or EU multi-regional endpoint. Ancillary account, support, security and service data is handled under Google's applicable Cloud data processing terms. Transfer / safeguards: UK-to-EU transfers may rely on applicable UK adequacy regulations. TeleFlow requires the EU Speech-to-Text endpoint and keeps the optional Speech-to-Text data-logging/model-improvement programme disabled unless expressly authorised by the Company.
OpenAI (OpenAI OpCo, LLC and applicable affiliates / downstream sub-processors under the OpenAI DPA)	Service / purpose: OpenAI API speech-to-text / audio transcription services. Data: Call audio/voice; transcription output; request and technical metadata. Because calls are unstructured, content may include Personal Data and Special Category Data described in Schedule 1. Processing location: United States when TeleFlow uses the US OpenAI API processing configuration; OpenAI downstream processing may also occur in locations identified in OpenAI's applicable sub-processor list and DPA. Transfer / safeguards: OpenAI's applicable DPA and transfer clauses, including for UK Data the EU Standard Contractual Clauses as amended by the UK Addendum where applicable; Module Three applies where TeleFlow acts as Processor and OpenAI acts as Sub-processor. TeleFlow will not opt Company Personal Data into OpenAI model training or improvement. Retention: Governed by the OpenAI service/endpoints and data controls used by TeleFlow. This DPA does not represent that Zero Data Retention applies unless TeleFlow has actually enabled and is eligible for that control.

Provider	Processing details and safeguards
ElevenLabs (Eleven Labs Inc. and applicable affiliates / downstream sub-processors under the ElevenLabs DPA)	Service / purpose: ElevenLabs Speech-to-Text / Scribe transcription services. Data: Call audio/voice; transcription output; request and technical metadata. Because calls are unstructured, content may include Personal Data and Special Category Data described in Schedule 1. Processing location: United States for the US-hosted transcription service used by TeleFlow; downstream processing may also occur in locations identified in ElevenLabs' applicable sub-processor arrangements. Transfer / safeguards: ElevenLabs' applicable DPA permits relevant transfers using applicable adequacy arrangements, the EU Standard Contractual Clauses and/or the UK Addendum or other lawful safeguards. Where TeleFlow acts as Processor, the processor-to-processor / processor-to-sub-processor transfer module applies as appropriate. TeleFlow will maintain the available account-level opt-out so new Company Personal Data is not used to improve ElevenLabs shared models. Retention: Governed by the ElevenLabs plan and applicable provider terms. This DPA does not represent that ElevenLabs Zero Retention Mode applies unless TeleFlow has separately enabled and is eligible for that feature.
IQ Mobile Ltd and applicable affiliates / downstream sub-processors under the IQ Mobile DPA)	Service / purpose: Voice connectivity Data: Call audio/voice and technical metadata necessary to provide the service. Processing location: UK Retention: Governed by UK Data Retention regulations

Provider selection and downstream processors. The Company authorises TeleFlow to use and switch between any Approved Sub-processor listed above without further case-by-case notice. Each provider may use authorised downstream processors under its applicable data processing terms.

Provider configuration. TeleFlow will maintain the safeguards stated in this Schedule. TeleFlow may change models or transcription endpoints within an Approved Sub-processor where the change does not materially reduce those safeguards.

Schedule 3 - Technical and Organisational Measures

TeleFlow shall maintain technical and organisational measures appropriate to the risk of the Processing. The following describes the minimum control categories committed to under this DPA. Specific technologies may change over time, provided the overall level of protection is not materially reduced.

1. Governance and confidentiality

Documented responsibility for data protection and information security; confidentiality obligations for personnel; access limited to personnel with a business need; appropriate staff awareness and training.

2. Identity and access management

Use of individual or otherwise accountable access credentials for administrative access; least-privilege principles; timely removal or adjustment of access; strengthened authentication for privileged access where appropriate to the risk and technically available.

3. Network and transmission security

Use of appropriate secure protocols and encryption for transmission of Company Personal Data over public networks; network controls designed to reduce unauthorised access to systems used to provide the Services.

4. Storage access controls

Appropriate logical and, where relevant, physical access controls for systems storing Company Personal Data, designed to restrict access to authorised personnel and protect against unauthorised access, alteration, loss or deletion, proportionate to the risk and system architecture.

5. System security and maintenance

Reasonable hardening, vulnerability management, anti-malware or equivalent protective controls where appropriate, security updates and patching processes for relevant systems and software.

6. Logging and monitoring

Logging and monitoring appropriate to the relevant systems and risk, including the ability to investigate material security events and unauthorised access where reasonably practicable.

7. Availability, resilience and recovery

Backup, recovery and continuity measures appropriate to the Services and the risk, with the objective of restoring availability and access following a material technical or physical incident.

8. Data segregation and minimisation

Logical controls appropriate to the architecture to reduce unauthorised cross-customer access; collection and Processing limited to data reasonably necessary for the Services and the Company's configuration.

9. Secure development and change management

Reasonable processes for managing material system changes and addressing security issues in software and configurations used to provide the Services.

10. Incident response

Processes to identify, investigate, contain, remediate and document suspected or confirmed security incidents and Personal Data Breaches, including escalation and Company notification in accordance with clause 7.

11. Retention and disposal

Retention and deletion mechanisms designed to follow the Company's documented settings or instructions and the end-of-contract requirements in clause 13; secure disposal appropriate to the media and sensitivity of the data.

12. Physical security

Reasonable controls to restrict unauthorised physical access to in-house systems, equipment and locations used by TeleFlow to Process Company Personal Data.

13. Approved third-party transcription services

Use only of the Approved Sub-processors listed in Schedule 2 for outsourced transcription processing. TeleFlow maintains provider-specific configuration controls appropriate to the service used, including Google EU endpoint enforcement and data-logging/model-improvement opt-out, OpenAI business/API use without opt-in model training, ElevenLabs model-improvement opt-out, restricted service credentials, and lawful international-transfer safeguards where Processing occurs outside the UK or EEA. Retention controls are applied where available and consistent with the relevant provider plan and TeleFlow's contractual commitments.

14. Review of measures

Periodic review of relevant security measures and adjustment where reasonably necessary in light of material changes to technology, threats, the Services or Applicable Data Protection Law.