Data Processing Addendum

Thorpe Voice services purchased through Number People

Version 1.0 | 6 November 2026 |

1. Parties and incorporation

This Data Processing Addendum (DPA) forms part of the agreement between the customer purchasing Thorpe Voice through Number People (Customer) and the legal entity identified as the service provider in the Customer's applicable Number People Terms and Conditions (Provider). Under the June 2025 Number People terms, the contracting entity depends on customer location; the parties should confirm that the account/order identifies the correct entity. "Thorpe Labs" is a brand and "Thorpe Voice" is the product, not separate contracting legal entities. This DPA takes effect when the Customer accepts the Thorpe Voice Supplementary Terms or otherwise enters into a binding order incorporating this DPA.

2. Roles and application

For personal data contained in calls and customer-configured workflows that Provider processes on Customer's behalf, Customer is the controller and Provider is the processor, except where Customer is itself a processor acting for another controller, in which case Provider acts as subprocessor. Provider may separately act as an independent controller for account administration, billing, fraud prevention and compliance, as described in the relevant privacy notice. This DPA applies only to Provider's processor/subprocessor activities. Each party shall comply with data protection law applicable to its activities, including UK GDPR and the Data Protection Act 2018 where applicable.

3. Documented instructions

Provider shall process Customer Personal Data only on documented instructions from Customer, including this DPA, the service agreement, configurations in the service portal and authorised support requests, unless applicable law requires otherwise. Where legally permitted, Provider will notify Customer before processing required by law. Provider shall promptly inform Customer if, in its opinion, an instruction infringes applicable data protection law. Customer is responsible for ensuring its instructions and use of Thorpe Voice have a lawful basis and for providing appropriate caller notices.

4. Confidentiality and personnel

Provider shall ensure that persons authorised to process Customer Personal Data are bound by confidentiality obligations or an appropriate statutory duty of confidentiality, and receive appropriate security and privacy training.

5. Security measures

Provider shall implement appropriate technical and organisational measures under Article 32 UK GDPR, taking account of risks, including role-based access, staff authentication, audit logging for access and live monitoring/takeover, private network connections between relevant service components, encryption in transit and at rest where appropriate, backup protection, vulnerability management, incident response, and access reviews. The detailed measures may evolve provided overall protection is not materially reduced. Provider shall make reasonable information available to demonstrate compliance, subject to confidentiality and security restrictions.

6. Subprocessors

Customer gives general written authorisation for Provider to engage subprocessors necessary to provide Thorpe Voice, subject to the list or notice mechanism made available with the service. Provider shall impose written data protection obligations on subprocessors that provide protection substantially equivalent to those in this DPA and remains responsible to Customer for their performance as required by Article 28. Provider shall notify Customer of intended additions or replacements in advance through the agreed customer notice channel and allow Customer a reasonable opportunity to object on data protection grounds before the change takes effect. If the parties cannot resolve a substantiated objection, Customer may discontinue the affected service under the applicable agreement. The published supplier list should identify relevant vendors and processing purposes and be maintained accurately.

7. International transfers

Provider shall not make a restricted transfer of Customer Personal Data outside the UK unless an applicable lawful transfer mechanism is in place, such as UK adequacy regulations, the UK Extension to the EU-US Data Privacy Framework where the recipient and transfer are covered, the UK International Data Transfer Agreement, or EU Standard Contractual Clauses with the UK Addendum, together with any required transfer risk assessment and supplementary measures. Provider shall make available information reasonably needed for Customer to assess relevant transfers. A supplier's location or certification shall not be assumed without verification.

8. Personal data breaches

Provider shall notify Customer without undue delay after becoming aware of a personal data breach affecting Customer Personal Data. Notification shall include available information on the nature of the incident, affected data and individuals, likely consequences and remedial measures, and shall be supplemented as further information becomes available. Provider shall cooperate reasonably with Customer's investigation and regulatory or individual notification obligations. Notification does not constitute an admission of liability.

9. Assistance to Customer

Taking account of the nature of processing and information available, Provider shall assist Customer through appropriate technical and organisational measures with requests to exercise data subject rights and, where reasonably required, with security obligations, personal data breach notifications, data protection impact assessments and prior consultation with regulators. Provider shall not respond substantively to a request about Customer-controlled call content except on Customer's instructions or where legally required. Reasonable charges for extraordinary assistance may be agreed in advance, to the extent permitted by law.

10. Audit and information

Provider shall make available information reasonably necessary to demonstrate compliance with Article 28 and allow for and contribute to audits, including inspections, by Customer or a mandated independent auditor, subject to reasonable advance notice, confidentiality, security safeguards and measures to avoid disruption. Provider may satisfy routine requests initially through relevant third-party assurance reports, policies and written responses, but this shall not remove mandatory audit rights.

11. Retention, return and deletion

Provider shall retain customer-directed AI transcripts and relevant call content for the agreed operational period, normally up to six months unless an applicable service setting or written agreement specifies otherwise. Upon termination or expiry of the service, at Customer's choice and subject to the service agreement, Provider shall return or delete Customer Personal Data and delete existing copies unless applicable law requires storage. Limited residual copies may persist in secured backups until scheduled overwrite and in operational/security logs under documented,

justified retention schedules; already delivered emails and independent telecommunications records may be outside the AI-content deletion process. Provider shall not represent these exceptions as immediate erasure. On request, Provider shall explain the applicable retention arrangements.

12. Liability, precedence and changes

Liability under this DPA is governed by the applicable service agreement to the extent permitted by law, without limiting rights or remedies that cannot lawfully be excluded. If this DPA conflicts with the Number People Terms or Thorpe Voice Supplementary Terms concerning processing of Customer Personal Data, this DPA prevails to the extent of that conflict. Changes to this DPA shall be made in accordance with the agreement and applicable law; changes that materially reduce data protection commitments require appropriate notice and lawful agreement.

Schedule 1 — Description of processing

Subject matter	**Provision of Thorpe Voice AI telephone reception, triage, call routing, summaries and related support.**
Duration	During the service term and applicable retention/deletion periods described in clause 11.
Nature and purpose	Receive and process caller speech; speech-to-text conversion; generate and deliver spoken responses; route or transfer calls; create call summaries, tickets and notifications; optional recordings where enabled; maintain security and operational functionality.
Data subjects	Callers, Customer employees/agents, contacts and other individuals mentioned during calls.
Personal data	Telephone numbers, names, contact details, caller audio, transcriptions, call metadata, appointment or enquiry details, call summaries, routing and ticket information; potentially special category data if callers disclose it.
Controller obligations	Determine lawful basis, transparency notices, recording configuration, purposes, access permissions, retention choices and lawful instructions.
Processor obligations	Process only on instructions, maintain confidentiality and security, manage subprocessors, assist with rights and breaches, and delete/return data as agreed.

Schedule 2 — Subprocessors and security information

The current Thorpe Voice subprocessor list and privacy information are incorporated by reference where identified in the customer order or service documentation. Relevant categories may include DigitalOcean (hosting and AI inference), OpenAI (model inference through DigitalOcean, contractual status subject to supplier confirmation), Deepgram (speech recognition), Google Cloud (text-to-speech and knowledge-base services), AWS SES (transactional email), and Twilio (SMS where enabled). Pinecone is used for knowledge-base information intended not to contain personal data.

Customer acceptance

This DPA is accepted as part of the Customer's Thorpe Voice service agreement.