

LEGAL

Data processor agreement

Last updated 15 January 2026

THE UNDERSIGNED

1. Customer, whose company and contact details and principal place of business are specified at the signature field below, hereinafter referred to as "Controller"

and

2. VoiceHubs, a private company with limited liability, incorporated and registered under the laws of the Netherlands having its registered office in (2031 ES) Haarlem, at the Tingietersweg 99, registered with the Chamber of Commerce of the Netherlands under number 83680578, in this matter duly represented by Bram Tierie (Head of partnerships), hereinafter referred to as "Processor".

Processor and Controller are hereinafter also referred to individually as "Party" or collectively as "Parties".

WHEREAS

- The Processor provides, for the benefit of the Controller, a cloud-based platform that enables asynchronous voice-driven collaboration within organizations. The platform allows users to create structured voice-based hubs ("VoiceHubs") where participants answer questions using their voice. VoiceHubs facilitates the collection, transcription, and analysis of the audio input, providing actionable insights to support group decision-making, employee engagement, and qualitative feedback processes;
- On signing date of this Processing Agreement document, the Controller and the Processor concluded an agreement regarding the provision of the aforementioned services, of which this Processor's Agreement is a part;
- Where the personal data processing is concerned, the Controller classifies as a controller within the meaning of Section 4(7) of the General Data Protection Regulation (Algemene Verordening Gegevensbescherming) ("GDPR");
- Where the personal data processing is concerned, the Processor qualifies as a processor within the meaning of Section 4(8) GDPR;
- The Parties, partly in implementation of the provisions of Section 28(3) GDPR, wish to document a number of conditions in the present processor's agreement which apply to their relationship in the context of the aforesaid activities on the instructions and for the benefit of the Controller.

DECLARE THAT THEY HAVE AGREED AS FOLLOWS

§1 Definitions

1.1 In this Processor's Agreement, capitalized words and expressions, whether in single or plural, have the meaning specified as set out below:

Annex	appendix to this Processor's Agreement which forms an integral part of it;
Agreement	the agreement concluded between the Controller and the Processor with regarding the provision of services by Processor;
Personal Data	all information relating to an identified or identifiable natural person as referred to in Section 4(1) GDPR;
Process	as well as conjugations of this verb: the processing of Personal Data as referred to in Section 4(2) GDPR;
Processor's Agreement	the present agreement;
Sub Processor	the sub-contractor hired by Processor, that Processes Personal Data in the context of this Processor's Agreement on behalf of the Controller, as referred to in Section 28(4) GDPR;
Terms	the terms of use of Processor, which form an integral part of the Agreement.

1.2 The provisions of the Agreement apply in full to this Processor's Agreement. In case provisions with regard to the Processing of Personal Data are included in the Agreement, the provisions of this Processor's Agreement prevail.

§ 2 Purpose of the personal data processing

2.1 The Controller and the Processor have concluded the present Processing Agreement for the Processing of Personal Data in the context of the Agreement. An overview of the type of Personal Data, categories of data subjects and the purposes of Processing, is included in Annex 1.

2.2 The Controller is responsible and liable for the processing of Personal Data in relation to the Agreement and guarantees that Processing is in compliance with all applicable legislation. Controller will indemnify and hold harmless Processor against any and all claims of third parties, those of the data protection authority in particular, resulting in any way from not complying with this guarantee.

2.3 The Processor undertakes to Process Personal Data only for the purpose of the activities referred to in this Processor's Agreement. The Processor guarantees that it will not use the Personal Data which it Processes in the context of this Processor's Agreement for its own or third-party purposes without the Controller's express written consent, unless a legal provision requires the Processor to do so. In such a case, the Processor shall immediately inform the Controller of that legal requirement before Processing, unless that law prohibits such information on important grounds of public interest. The Processor shall only process the minimum amount of Personal Data necessary for the specific purposes as set out in this Agreement.

2.4 The Processor shall not process Personal Data beyond the scope defined in this agreement unless required by law. In such cases, the Processor must inform the Controller without undue delay unless prohibited by legal obligations.

- 2.5** The Processor confirms that Personal Data will not be used to train, fine-tune, or improve underlying machine learning models of third parties (e.g. Whisper, OpenAI), unless explicitly agreed upon in writing by the Controller and compliant with applicable data protection laws.
- 2.6** Where the Controller or a User connects a Google account to the Service, the Processor will Process Google Calendar personal data (including event titles, times, descriptions, locations (if present), and attendee information) solely for the purposes of (i) creating VoiceHubs based on scheduled meetings, (ii) identifying meeting participants for invitations, and (iii) syncing meeting updates with the relevant VoiceHubs, as further specified in Annex 1.

§ 3 Technical and organizational provisions

- 3.1** The Processor will, taking into account the nature of the Processing and insofar as this is reasonably possible, assist the Controller in ensuring compliance with the obligations pursuant to the GDPR to take appropriate technical and organizational measures to ensure a level of security appropriate to the risk. These measures will guarantee an appropriate level of security, taking into account the state of the art and the costs of implementation, in view of the risks entailed by Personal Data Processing and the nature of the data to be protected. The Processor will in any case take measures to protect Personal Data against accidental or unlawful destruction, accidental or deliberate loss, forgery, unauthorized distribution or access, or any other form of unlawful Processing.

§ 4 Confidentiality

- 4.1** The Processor will require the employees that are involved in the execution of the Agreement to sign a confidentiality statement, whether or not included in the employment agreement with those employees, which in any case states that these employees must keep strict confidentiality regarding the Personal Data.

§ 5 Personal data processing outside Europe

- 5.1** The Processor will process certain Personal Data (described in Annex 2) in locations outside the European Economic Area (EEA), limited to the United Kingdom (UK).
- 5.2** The Processor ensures that such data transfers comply with the requirements of the General Data Protection Regulation (GDPR), specifically Chapter V, regarding transfers of personal data to third countries or international organizations.
- 5.3** The Processor will ensure that adequate safeguards are in place for the protection of Personal Data transferred outside the EEA. These safeguards may include, but are not limited to:
- The use of Standard Contractual Clauses (SCCs) as adopted by the European Commission.
 - The implementation of additional technical and organizational measures to secure the data.
- 5.4** The Processor will inform the Controller of any legal framework changes that may affect the legality of the data transfer and will cooperate with the Controller to implement appropriate measures to maintain compliance.

- 5.5** If changes in international data transfer laws impact compliance, the Processor will work with the Controller to update agreements and implement alternative safeguards within 90 days.

§ 6 Sub-processors

- 6.1** The Processor may engage Sub-Processors listed in Annex 2. If the Processor intends to change, add, or replace a Sub-Processor, it must notify the Controller at least 10 days in advance. The Controller will have 5 calendar days to object. If not resolved within 15 days, the Controller may terminate the Agreement.
- 6.2** The Controller has 5 working days to object. If the Processor does not resolve the objection within 30 days, the Controller may terminate the agreement with no penalty.
- 6.3** The Processor requires all Sub-Processors to adhere to at least the same level of data protection and security commitments outlined in this Processing Agreement.

§ 7 Liability

- 7.1** With regard to the liability and indemnification obligations of Processor under this Processor's Agreement the stipulation in Article 7 of the Terms regarding the limitation of liability applies.
- 7.2** Without prejudice to article 7.1 of this Processor's Agreement, Processor shall only be liable for damages caused by Processing where it has not complied with its obligations under Article 28–36 GDPR or has acted outside or contrary to the lawful instructions of the Controller.

§ 8 Personal data breach

- 8.1** In the event the Processor becomes aware of any incident that may have a (significant) impact on the protection of Personal Data, (i) it will notify the Controller without undue delay and (ii) will take all reasonable measures to prevent or limit (further) violation of the GDPR.
- 8.2** The Processor will, insofar as reasonable, provide all reasonable cooperation requested by the Controller in order for Controller to comply with its legal obligations relating to the identified incident.
- 8.3** The Processor will, insofar as reasonable, assist the Controller with the Controller's notification obligation relating to the Personal Data to the Data Protection Authority and/or the data subject, as meant in Section 33(3) and 34(1) GDPR. Processor is never held to report a personal data breach with the Data Protection Authority and/or the data subject.
- 8.4** Processor will not be responsible and/or liable for the (timely and correctly) notification obligation to the relevant supervisor and/or data subjects, as meant in Section 33 and 34 GDPR.

§ 9 Cooperation

- 9.1** The Processor will, insofar as reasonably possible, provide all reasonable cooperation to the Controller in fulfilling its obligation pursuant to the GDPR to respond to requests for exercising rights of data subjects, in particular the right of access (Section 15 GDPR), rectification (Section 16 GDPR), erasure (Section 17 GDPR), restriction (Section 18 GDPR), data portability (Section 20 GDPR) and the right to object (Section 21 and 22 GDPR). The Processor will forward a complaint or request from a data subject with regard to the Processing of Personal Data to the Controller as soon as possible, as the Controller is responsible for handling the request. The Processor is entitled to charge any costs associated with the cooperation with the Controller.
- 9.2** The Processor will, insofar as reasonably possible, provide all reasonable cooperation to the Controller in fulfilling its obligation pursuant to the GDPR to carry out a data protection impact assessment (Section 35 and 36 GDPR).
- 9.3** The Processor will provide the Controller with all the information reasonably necessary to demonstrate that the Processor fulfills its obligations under the GDPR. Furthermore, the Processor will, at the request of the Controller, enable and contribute to audits, including inspections by the Controller or an auditor that is authorized by the Controller. In case the Processor is of the opinion that an instruction relating to the provisions of this paragraph infringes the GDPR or other applicable data protection legislation, the Processor will inform the Controller immediately.
- 9.4** The Processor is entitled to charge any possible costs with the Controller.

§10 Termination and miscellaneous

- 10.1** Upon termination of this Processing Agreement, the Processor will either delete or return all Personal Data at the Controller's request, unless retention is legally required.
- 10.2** Upon termination, the Processor will delete or return all Personal Data within 30 days unless legal retention is required. Upon request, the Processor shall provide written confirmation that all Personal Data has been permanently deleted in accordance with this clause.
- 10.3** The Controller may request data export within the 30-day period before deletion. The Processor will facilitate this in a structured format.
- 10.4** Where a User disconnects a connected Google account during the term, Processor will stop collecting Google Calendar data for that account and will delete or de-identify any stored Google Calendar data relating to that connection within a reasonable period, unless retention is required by law or necessary to meet the Controller's documented instructions.

ANNEX 1

Overview personal data

TYPE OF PERSONAL DATA

EMPLOYEE DATA

- First name
- Last name

- Email
- If provided: birthday
- If provided: gender
- If provided: phone number
- If provided: Job role

AUDIO DATA

- Audio recordings (voice responses, contributions)
- Audio file metadata (e.g., device, browser, IP address, timestamps)

TECHNICAL DATA

- Device information
- Browser information
- IP address
- Usage logs (if applicable)

GOOGLE CALENDAR DATA (IF CONNECTED BY USER)

- Calendar event metadata: event title, start/end time, timezone, location (if present), description/agenda (if present)
- Attendee information: names, email addresses, attendee status (accepted/declined/tentative) (if present)
- Event identifiers needed for syncing updates (event ID / recurring series ID, if applicable)

CATEGORIES OF DATA SUBJECTS

The data subject is any individual whose personal data is processed within a VoiceHub by the Processor. This primarily includes employees of the Controller’s organization, or employees of organizations for whom the Controller acts as a mediator. In some cases, the data subject may also include other participants (e.g., external collaborators or consultants) who are invited to contribute to a VoiceHub. In addition, where Google Calendar is connected, data subjects may include meeting attendees listed in calendar events.

ANNEX 2

Overview sub-processors of personal data

VoiceHubs utilizes multiple subcontractors to process personal identifiable data. However, we try to limit the number of subcontractors that process this personal identifiable data to a minimum. The companies listed below process personal identifiable data.

NAME	DATA BEING PROCESSED	COUNTRIES	DATA STORED

NAME	DATA BEING PROCESSED	COUNTRIES	DATA STORED
Supabase Inc. (Database)	All application data (user profiles, voice hub content, contributions, participant data, authentication data, organization data)	Germany (AWS eu-central-1)	Yes, primary database storage
Supabase Inc. (Storage)	File uploads (audio recordings, attachments, organization logos)	Germany (AWS eu-central-1)	Yes, file storage
Amazon Web Services Inc.	File storage, potentially transcoded audio files	Ireland (eu-west-1)	Yes, file storage
Mistral AI	Voice hub goals, participant responses, contribution content for analysis and question generation	France	Temporarily for processing, not for persistent storage
Speechmatics	Audio recordings for speech-to-text transcription	United Kingdom	Temporarily for processing, transcripts returned and audio deleted
Resend Inc.	Email addresses, names, notification content	Ireland (AWS eu-west-1)	Yes, email delivery logs and bounce data
Functional Software Inc. (Sentry)	Error logs, performance data, potentially user identifiers in error contexts	United States (with EU hosting options available)	Yes, for error tracking and debugging
Stripe Inc.	Payment data, billing information, customer details, transaction records	United States, European Union (depending on configuration)	Yes, for payment processing, compliance, and billing management

Google Calendar data (event titles, times, descriptions, attendee information) may be processed by Supabase, Mistral AI, and Resend as described above. We do not sell or share Google user data with any other third parties.