Data processing agreement

Version: 2026-10-01

Effective date: 2026-10-01

This Data Processing Agreement ("**DPA**") is concluded between:

Quantum Noodle BV, a private limited liability company (*besloten vennootschap*) organised under the laws of Belgium, with its registered office at Hallaardreef 5, 2580 Beerzel, Belgium, registered with the Crossroads Bank for Enterprises under number 1003.622.970, trading as Scribewave ("**Scribewave**"); and

the natural or legal person that uses the Scribewave services under the Scribewave Terms of Service, published at https://app.scribewave.com/policy/terms-of-service, or under another written agreement with Scribewave (the "**Customer**").

This DPA forms part of the Terms of Service and of any other agreement between Scribewave and the Customer for the Services (together, the "**Agreement**"). It applies without signature from the moment the Customer accepts the Terms of Service or starts using the Services, and governs all processing of Customer Personal Data by Scribewave in providing the Services. Customers who need other terms can contact Scribewave at hello@scribewave.com.

1. Definitions

1.1. "**GDPR**" means Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

1.2. "**Data Protection Laws**" means the GDPR, the Belgian Act of 30 July 2018 on the protection of natural persons with regard to the processing of personal data, and any other data protection law of the European Union or its Member States that applies to the processing under this DPA.

1.3. "**Customer Personal Data**" means the personal data that Scribewave processes on behalf of the Customer in providing the Services, as described in Annex 1.

1.4. "**Services**" means the Scribewave transcription, subtitling, translation, meeting recording and related services, including the web application, the API and integrations, as described in the Agreement.

1.5. "**Subprocessor**" means any third party that Scribewave engages to process Customer Personal Data.

1.6. "**Personal Data Breach**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Customer Personal Data.

1.7. "**EEA**" means the European Economic Area.

1.8. Terms such as "controller", "processor", "personal data", "processing", "data subject" and "supervisory authority" have the meaning given to them in the GDPR.

2. Scope, roles and duration

2.1. With respect to Customer Personal Data, the Customer acts as controller and Scribewave acts as processor. Where the Customer itself acts as a processor on behalf of a third party, the Customer warrants that its instructions to Scribewave, including the engagement of Scribewave as a subprocessor, are authorised by that third party, and Scribewave acts as the Customer's subprocessor.

2.2. Scribewave processes certain personal data for its own purposes, such as account administration, billing, security, fraud prevention and compliance with legal obligations. For that processing Scribewave is a controller, and it is governed by the Scribewave Privacy Policy, not by this DPA.

2.3. The subject matter, nature and purpose of the processing, the types of personal data and the categories of data subjects are set out in Annex 1.

2.4. This DPA remains in force for as long as Scribewave processes Customer Personal Data, including after the Agreement ends until the deletion described in clause 12 is complete.

3. Instructions

3.1. Scribewave processes Customer Personal Data only on the Customer's documented instructions, unless required to do so by Union or Member State law to which Scribewave is subject. In that case Scribewave informs the Customer of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest.

3.2. The Customer's instructions are set out in the Agreement and this DPA, and are given through the Customer's use and configuration of the Services, including the features, settings and options that the Customer's users choose. Additional instructions require Scribewave's written agreement.

3.3. Scribewave informs the Customer without undue delay if, in its opinion, an instruction infringes Data Protection Laws. Scribewave may suspend carrying out that instruction until the Customer confirms or changes it.

3.4. Scribewave does not process Customer Personal Data for any purpose other than providing the Services to the Customer, does not sell it, and does not take decisions about its use, its disclosure to third parties or its retention period other than on the Customer's instructions.

3.5. Scribewave does not use Customer Personal Data, including audio and video recordings, transcripts and any content derived from them, to train, retrain, fine-tune or otherwise improve any artificial intelligence, machine learning or speech recognition model, whether its own or a third party's, and does not permit its Subprocessors to do so.

3.6. Customer Personal Data remains the property of the Customer or of the data subjects concerned. Scribewave acquires no rights in it other than those needed to provide the Services.

4. Obligations of the Customer

4.1. The Customer is responsible for the lawfulness of the processing of Customer Personal Data, including having a valid legal basis under Article 6 GDPR and, where special categories of personal data are processed, under Article 9 GDPR, and for informing data subjects and obtaining any consent that is required. This includes informing people that a conversation or meeting is being recorded and transcribed.

4.2. The Customer warrants that the content it uploads, records or otherwise provides to the Services is lawful and does not infringe the rights of third parties.

4.3. The Customer decides which personal data it provides to the Services, and whether this includes special categories of personal data. Scribewave applies the measures in Annex 2 to all Customer Personal Data, whatever its category.

4.4. The Customer is responsible for managing its users' access to the Services, keeping their credentials confidential, and for the sharing settings it chooses, including making transcripts available through public or shared links.

5. Confidentiality

5.1. Scribewave treats Customer Personal Data as confidential. It ensures that any person acting under its authority who has access to Customer Personal Data is bound by an appropriate obligation of confidentiality and has access only to the extent needed to provide the Services.

5.2. Scribewave does not disclose Customer Personal Data to third parties, except to Subprocessors in accordance with clause 7, where the Customer has authorised the disclosure, or where Union or Member State law requires it.

5.3. If a public authority requests access to Customer Personal Data, Scribewave informs the Customer of the request without undue delay, unless the law prohibits this, and discloses no more than the law requires.

6. Security

6.1. Scribewave implements appropriate technical and organisational measures to ensure a level of security appropriate to the risk, as required by Article 32 GDPR, taking into account in particular the risks of processing special categories of personal data. The measures in place are described in Annex 2.

6.2. Scribewave may update these measures as technology and threats evolve, provided that the overall level of security is not reduced.

7. Subprocessors

7.1. The Customer gives Scribewave general authorisation to engage Subprocessors. The Subprocessors currently engaged, what they are used for and where they process Customer Personal Data are listed at https://app.scribewave.com/legal/subprocessors (Annex 3).

7.2. Some Subprocessors are used only when the Customer's users use a specific feature, as indicated in the list. Those Subprocessors do not receive Customer Personal Data unless that feature is used. Enterprise customers can, on request to privacy@scribewave.com, opt out of the Subprocessors that the list marks as open to an opt-out. Scribewave then stops using those Subprocessors for the Customer's organisation, which may limit the features or languages available to it.

7.3. Scribewave engages each Subprocessor under a written contract that imposes data protection obligations no less protective than those in this DPA, including the restriction in clause 3.5.

7.4. Scribewave gives at least thirty (30) days' notice before adding or replacing a Subprocessor. It does so by publishing the change and the date it takes effect on the page referred to in clause 7.1, and by emailing the administrators of the Customer's organisation in the Services and anyone who has subscribed to change notifications on that page.

7.5. The Customer may object to a new Subprocessor on reasonable grounds relating to data protection, by writing to privacy@scribewave.com within fifteen (15) days of the notice. The parties will then discuss the objection in good faith; Scribewave may, for example, propose a way to use the Services without that Subprocessor. If no solution is found before the change takes effect, the Customer may terminate the Agreement, or the use of the Services affected by the change, by written notice before that date, without penalty.

7.6. Scribewave remains responsible to the Customer for the performance of its Subprocessors' data protection obligations, subject to clause 14.

8. International transfers

8.1. Scribewave hosts and stores Customer Personal Data in the European Union. Some Subprocessors process Customer Personal Data outside the EEA; the list referred to in clause 7.1 shows where each of them processes it.

8.2. Scribewave transfers Customer Personal Data outside the EEA only in accordance with Chapter V GDPR: to a country covered by an adequacy decision of the European Commission, or subject to appropriate safeguards such as the standard contractual clauses adopted by Commission Implementing Decision (EU) 2021/914, together with supplementary measures where needed.

8.3. On request, Scribewave informs the Customer of the transfer mechanism that applies to a given Subprocessor.

9. Personal Data Breaches

9.1. Scribewave notifies the Customer of a Personal Data Breach without undue delay, and in any event within seventy-two (72) hours after becoming aware of it, so that the Customer can meet its obligations under Articles 33 and 34 GDPR.

9.2. The notification describes, as far as the information is available: the nature of the Personal Data Breach, including where possible the categories and approximate number of data subjects and records concerned; its likely cause and consequences; the measures taken or proposed to address it and to mitigate its effects; and a contact point for further information. Where not all information is available at once, Scribewave provides it in phases without undue further delay.

9.3. Scribewave takes reasonable steps to contain the Personal Data Breach and limit its consequences, and cooperates with the Customer. The Customer remains responsible for any notification to supervisory authorities and data subjects.

9.4. The Customer notifies Scribewave without undue delay of any Personal Data Breach, or suspected breach, that it becomes aware of, including incidents on its own systems or the misuse of its users' credentials, and cooperates reasonably so that Scribewave can investigate and contain it.

9.5. Notifying or responding to a Personal Data Breach is not an acknowledgement of fault or liability by Scribewave.

10. Requests from data subjects

10.1. If Scribewave receives a request from a data subject to exercise their rights under Articles 15 to 22 GDPR regarding Customer Personal Data, it forwards the request to the Customer without undue delay and does not respond to it itself, unless the Customer instructs it to.

10.2. Taking into account the nature of the processing, Scribewave assists the Customer by appropriate technical and organisational measures, insofar as possible, in responding to such requests. The Services let the Customer access, correct, export and delete Customer Personal Data.

11. Assistance

Taking into account the nature of the processing and the information available to it, Scribewave assists the Customer in ensuring compliance with its obligations under Articles 32 to 36 GDPR, including data protection impact assessments and prior consultation of a supervisory authority.

12. Deletion and return

12.1. When the Customer deletes a project or file in the Services, Scribewave deletes the corresponding recordings and transcripts from its production systems without undue delay. Deleted data may remain in encrypted backups for up to fourteen (14) days, after which it is permanently deleted.

12.2. When a user deletes their account, the account is deleted after a short grace period (currently ten (10) days) during which the deletion can be cancelled.

12.3. The Customer can export Customer Personal Data through the Services at any time before the Agreement ends. Within thirty (30) days after the Agreement ends, Scribewave deletes all Customer Personal Data, unless Union or Member State law requires it to be stored. The backup period in clause 12.1 applies.

12.4. On written request, Scribewave confirms the deletion in writing.

13. Information and audits

13.1. Scribewave makes available to the Customer, on request, the information necessary to demonstrate compliance with Article 28 GDPR, such as this DPA, a description of its security measures, the list of Subprocessors and reasonable answers to security questionnaires.

13.2. Where that information is not sufficient to demonstrate compliance, where a supervisory authority requires it, or after a Personal Data Breach, the Customer may have an audit carried out, including an inspection, by an independent auditor bound by an obligation of confidentiality. The Customer gives at least thirty (30) days' written notice, and audits take place no more than once in any twelve (12) month period, except where required by a supervisory authority or following a Personal Data Breach. Audits take place during normal business hours, follow Scribewave's reasonable security requirements and do not unreasonably interfere with its business.

13.3. Scribewave may meet its obligations under this clause by providing relevant third-party certifications or audit reports, including those of its Subprocessors, where these cover the processing concerned.

13.4. The Customer bears the costs of an audit, unless the audit reveals a material breach of this DPA by Scribewave, in which case Scribewave bears its own costs and reimburses the Customer's reasonable audit costs. The parties discuss the findings of an audit and agree on any measures to be taken.

14. Liability

14.1. Each party's liability under or in connection with this DPA, including for any claim by a data subject under Article 82 GDPR, is subject to the limitations and exclusions of liability in the Agreement.

14.2. Scribewave is not liable for a Personal Data Breach caused by an attack, including zero-day vulnerabilities, advanced persistent threats or state-sponsored attacks, that could not reasonably have been prevented by measures that were state of the art at the time, provided that Scribewave had implemented the measures in Annex 2 in good faith and acted without undue delay to contain and mitigate the incident.

14.3. The Customer indemnifies Scribewave against all claims, fines, damages, losses and costs, including reasonable legal fees, arising from (i) the absence of a valid legal basis for the processing of the personal data provided to the Services, (ii) unlawful content uploaded or recorded by or for the Customer, (iii) the misuse of credentials of the Customer's users or of persons acting under the Customer's authority, (iv) instructions of the Customer that infringe Data Protection Laws, or (v) any other breach of the Customer's obligations under this DPA.

15. Changes to this DPA

15.1. Scribewave may amend this DPA by publishing a new version, with its version number and effective date, at https://app.scribewave.com/legal/dpa.

15.2. Scribewave gives at least thirty (30) days' notice by email to the administrators of the Customer's organisation in the Services of any amendment that reduces the protection of Customer Personal Data. If the Customer objects, it may terminate the Agreement by written notice before the amendment takes effect. Amendments required by law or by a supervisory authority may take effect sooner.

15.3. Changes to the list of Subprocessors follow clause 7, not this clause.

16. Miscellaneous

16.1. In case of conflict between this DPA and any other part of the Agreement, this DPA prevails with respect to the processing of Customer Personal Data.

16.2. If a provision of this DPA is invalid or unenforceable, the other provisions remain in force, and the parties replace the provision with a valid one that comes as close as possible to its purpose.

16.3. This DPA is governed by Belgian law, without prejudice to the mandatory provisions of the GDPR. Any dispute arising from or in connection with this DPA is submitted to the competent courts of the judicial district of Antwerp, Belgium, without prejudice to the powers of supervisory authorities.

16.4. Logs and measurements kept by Scribewave are deemed authentic, unless the Customer provides convincing proof to the contrary.

16.5. This DPA is drawn up in English. If it is translated, the English version prevails.

16.6. Notices under this DPA are sent to Scribewave at privacy@scribewave.com, and to the Customer at the email address of the administrators of its organisation in the Services.

Annex 1: Description of the processing

Subject matter. Providing the Services to the Customer: automated transcription, subtitling and translation of audio and video recordings, recording meetings, AI-assisted editing and analysis, and storing, sharing and exporting the results.

Duration. The term of the Agreement, and afterwards until deletion in accordance with clause 12.

Nature and purpose. Receiving and storing audio and video files and recordings; automated speech-to-text transcription; translation; editing and review of transcripts and subtitles by the Customer's users; AI-assisted features when the Customer's users use them; joining, recording and transcribing meetings when the Customer uses the meeting notetaker; sharing and exporting results; support at the Customer's request; and security and abuse prevention.

Types of personal data. Audio and video recordings and whatever they contain; transcripts, subtitles, translations, summaries and notes derived from them; speaker names and labels; names and email addresses of meeting participants; custom vocabulary; names and email addresses of the Customer's users; phone numbers used for uploads over WhatsApp; and technical data such as IP addresses and logs.

Special categories of personal data. Depending on what the Customer records or uploads, recordings and transcripts may contain special categories of personal data within the meaning of Article 9 GDPR, such as data concerning health. The Customer decides whether to provide such data (clause 4.3).

Categories of data subjects. The Customer's users; people whose voice, image or words appear in recordings, such as interviewees, patients, clients and meeting participants; and other people mentioned in recordings or transcripts.

Frequency. Continuous, for as long as the Customer uses the Services.

Retention. Until the Customer deletes the data, and at the latest in accordance with clause 12.

Annex 2: Technical and organisational measures

Encryption. TLS 1.2 or higher for data in transit between users, the Services and Subprocessors. AES-256 encryption at rest for stored recordings, transcripts and database content, provided by Amazon S3 and MongoDB Atlas. Encrypted backups, kept for at most fourteen (14) days after deletion. Passwords are stored only as bcrypt hashes.

Hosting. The Services are hosted in the European Union: Amazon Web Services in its Paris and Ireland regions, and MongoDB Atlas in the EU. Recordings are uploaded directly from the user's browser to storage in the EU through short-lived signed URLs.

Access control. Role-based access control within the Services, with each customer's data isolated under its

own organisation. Access by Scribewave personnel to production data is limited to a small number of named people on a need-to-know basis, and administrative access requires multi-factor authentication. Access is logged.

Infrastructure security. Separate production, staging and development environments. Regular updates and vulnerability patching. Rate limiting and bot protection on sensitive endpoints.

Minimisation. Internal monitoring and analytics use aggregated or non-identifying data where possible. Customer Personal Data is not used to train AI models (clause 3.5).

Resilience. Automated, encrypted backups, and recovery procedures that are tested periodically.

Organisational measures. Confidentiality undertakings for everyone with access to Customer Personal Data. Security and data protection training. A documented incident response procedure. Due diligence on Subprocessors and contractual flow-down of data protection obligations.

Annex 3: Subprocessors

The Subprocessors that Scribewave engages, what they are used for, where they process Customer Personal Data, which of them are used only for a specific feature, and which of them enterprise customers can opt out of are listed at https://app.scribewave.com/legal/subprocessors, together with the changes made to the list. The list as it stood on the date shown is appended to the PDF version of this DPA.

Subprocessor list

As of: 2026-10-01

Amazon Web Services EMEA SARL

Part of: Amazon.com, Inc.

Purpose: Hosting, file storage and media processing; machine translation when the AI translation fails

Processing region: European Union

Use: Always used

MongoDB Limited

Part of: MongoDB, Inc.

Purpose: Application database

Processing region: European Union

Use: Always used

Vercel Inc.

Purpose: Hosting of the web application and page analytics

Processing region: European Union

Use: Always used

Twilio Inc.

Purpose: Sending service emails

Processing region: United States

Use: Always used

Upstash, Inc.

Purpose: Rate limiting (user and organization IDs, IP addresses)

Processing region: European Union
Use: Always used

Eleven Labs Inc.

Purpose: Speech-to-text (default engine)
Processing region: United States
Use: Always used
Opt-out: Possible for enterprise customers, on request

Cantab Research Limited (Speechmatics)

Purpose: Speech-to-text (custom vocabulary, multiple languages, very long files)
Processing region: European Union
Use: Always used
Opt-out: Possible for enterprise customers, on request

AssemblyAI, Inc.

Purpose: Speech-to-text (some languages, and fallback when another engine fails)
Processing region: European Union
Use: Always used
Opt-out: Possible for enterprise customers, on request

Deepgram, Inc.

Purpose: Speech-to-text (enhanced privacy mode and some models)
Processing region: European Union
Use: Always used
Opt-out: Possible for enterprise customers, on request

Soniox, Inc.

Purpose: Speech-to-text (beta model)
Processing region: United States
Use: Used only when you use a beta transcription model
Opt-out: Possible for enterprise customers, on request

Replicate, Inc.

Purpose: Speech-to-text (beta model)
Processing region: United States
Use: Used only when you use a beta transcription model
Opt-out: Possible for enterprise customers, on request

Salad Technologies, Inc.

Purpose: Speech-to-text (beta model, through the API only)
Processing region: Worldwide
Use: Used only when you use a beta transcription model
Opt-out: Possible for enterprise customers, on request

Hyperdoc Inc. (Recall.ai)

Purpose: Joining, recording and transcribing meetings

Processing region: European Union

Use: Used only when you use the meeting notetaker

Opt-out: Possible for enterprise customers, on request

Google Cloud EMEA Limited

Part of: Google LLC

Purpose: Calendar invitations to the meeting notetaker and meeting summary emails

Processing region: Worldwide

Use: Used only when you use the meeting notetaker

Opt-out: Possible for enterprise customers, on request

Google Cloud EMEA Limited

Part of: Google LLC

Purpose: AI features in the app: chat, AI edits, translation, pseudonymisation and export AI prompts

Processing region: European Union

Use: Used only when you use AI features, including the AI meeting notes the meeting notetaker makes by default

Opt-out: Possible for enterprise customers, on request

Google LLC

Purpose: AI meeting notes and AI-enhanced bulk exports

Processing region: Worldwide

Use: Used only when you use AI features, including the AI meeting notes the meeting notetaker makes by default

Opt-out: Possible for enterprise customers, on request

WhatsApp Ireland Limited

Part of: Meta Platforms, Inc.

Purpose: Receiving audio sent over WhatsApp and replying with a link to the transcript

Processing region: Worldwide

Use: Used only when you use WhatsApp uploads

SHA-256 of the text: 3106f0bc2035dc7ec68ed672a1fc6d10c1f17e131f056f8d672a65fef4c411da