Data Processing Agreement

How we process personal data in your media on your behalf, under Article 28 of the GDPR.

Version	Last updated	Applies from
1.0 (draft)	29 September 2026	Acceptance of the Terms of Service

Draft, pending legal review

This is a draft of the agreement we intend to offer. It is not yet in force. Email privacy@subtitle.ai if you need a signed DPA before it is finalised.

---

1. About this agreement

1.1 This Data Processing Agreement ("DPA") is between Quantum Noodle BV, trading as Subtitle AI, with its registered office at Hallaardreef 5, 2580 Beerzel, Belgium ("Subtitle AI", "we", "us"), and the customer that has accepted our Terms of Service ("Customer", "you").

1.2 This DPA forms part of the Terms of Service (together, the "Agreement"). It applies automatically whenever we process personal data on your behalf while providing the Services. You do not need to sign it. If your organisation needs a countersigned copy for its records, email privacy@subtitle.ai and we will send one.

1.3 Where this DPA and the Terms of Service conflict on the processing of personal data, this DPA prevails. Where this DPA and the Standard Contractual Clauses referred to in section 8 conflict, the Standard Contractual Clauses prevail.

2. Definitions

Terms such as “controller”, “processor”, “data subject”, “personal data”, “processing” and “supervisory authority” have the meaning given to them in the GDPR. In addition:

- **Applicable Data Protection Law** means Regulation (EU) 2016/679 (the “GDPR”), the Belgian Act of 30 July 2018 on the protection of natural persons with regard to the processing of personal data, and, where it applies, the UK GDPR and the Swiss Federal Act on Data Protection.
- **Customer Content** means the audio, video, text and other material you or your users upload to the Services, and everything the Services produce from it: transcripts, subtitles, translations, rendered videos and exports.
- **Customer Personal Data** means any personal data in Customer Content, and any personal data about your users that we process on your behalf under the Agreement.
- **Sub-processor** means a third party we engage to process Customer Personal Data.
- **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.

3. Roles and scope

3.1 For Customer Personal Data, you are the controller and we are your processor. If you yourself process the data on behalf of a client (for example, as a subtitling agency working for a broadcaster), you are the processor, we are your sub-processor, and you are responsible for passing on your client’s instructions to us.

3.2 The subject matter, duration, nature and purpose of the processing, and the types of personal data and data subjects concerned, are described in Annex 1.

3.3 This DPA does not cover personal data we process as a controller for our own purposes, such as account administration, billing and website analytics. Our Privacy Policy describes that processing.

3.4 You are responsible for having a lawful basis for the processing, for informing the people who appear in your media where the law requires it, and for holding the rights needed to upload Customer Content to the Services.

---

4. Processing only on your instructions

4.1 We process Customer Personal Data only on your documented instructions. The Agreement, and your use and configuration of the Services' features, are your complete instructions at the date of this DPA. You can give additional written instructions by emailing privacy@subtitle.ai, provided they are consistent with the Agreement.

4.2 We will tell you promptly if, in our opinion, an instruction infringes Applicable Data Protection Law. If Union or Member State law requires us to process Customer Personal Data in any other way, we will inform you before doing so, unless that law prohibits it.

4.3 We do not sell Customer Personal Data, use it for advertising, or combine it with data from other customers or sources.

4.4 We do not use Customer Content to train, fine-tune or evaluate machine-learning models, or to tune prompts, unless the Customer has agreed to it in writing. We do not allow our Sub-processors to do so.

---

5. Confidentiality

5.1 We ensure that everyone we authorise to process Customer Personal Data is bound by a duty of confidentiality, whether contractual or statutory, and has access only to the extent their role requires.

6. Security

6.1 We implement the technical and organisational measures described in Annex 2, which are designed to give a level of security appropriate to the risk, as required by Article 32 GDPR.

6.2 We may update these measures as technology and threats change, provided the update does not lower the overall level of protection.

7. Sub-processors

7.1 You give us general authorisation to engage Sub-processors. The Sub-processors we use at the date of this DPA are listed in Annex 3.

7.2 We will give at least 30 days' notice before a new Sub-processor starts processing Customer Personal Data, by emailing the owner of your account and updating the list on our website.

7.3 You may object to a new Sub-processor on reasonable data protection grounds within that notice period. We will then work with you in good faith to find an alternative. If we cannot offer one, you may terminate the affected Services and we will refund any fees you prepaid for the period after termination. This clause takes precedence over the no-refund clause in the Terms of Service.

7.4 We impose data protection obligations on each Sub-processor that are no less protective than those in this DPA, and we remain liable to you for their performance.

8. International transfers

8.1 Some Sub-processors process Customer Personal Data outside the European Economic Area. Annex 3 states where each one does so. We transfer Customer Personal Data outside the EEA only where one of the following applies:

- the European Commission has decided that the destination country ensures an adequate level of protection, including, for the United States, where the recipient is certified under the EU-U.S. Data Privacy Framework; or
- we have entered into the Standard Contractual Clauses adopted by Commission Implementing Decision (EU) 2021/914 with the recipient, together with any supplementary measures a transfer impact assessment shows to be necessary.

9. Helping you meet your obligations

9.1 You can access, correct, export and delete Customer Content yourself in the Services. Where you cannot answer a data subject's request that way, we will help you as far as reasonably possible.

9.2 If a data subject contacts us directly about Customer Personal Data, we will pass the request on to you without undue delay and will not respond to it ourselves, except to tell them to contact you.

9.3 Taking into account the information available to us, we will give you reasonable help with data protection impact assessments and prior consultations with a supervisory authority, where they relate to the Services.

10. Personal data breaches

10.1 We will notify you without undue delay, and in any event within 48 hours, after becoming aware of a Personal Data Breach affecting your Customer Personal Data.

10.2 Our notice will describe, as far as we know at the time, the nature of the breach, the categories and approximate number of data subjects and records concerned, its likely consequences, and the measures we have taken or propose to take. We will send further information as it becomes available.

10.3 Notifying you of a breach is not an admission of fault or liability.

11. Return and deletion

11.1 While the Agreement is in force, you can download and delete Customer Content at any time in the Services. On your request, we will also delete any copies that remain in our storage, such as preview copies and rendered videos, within 30 days.

11.2 When the Agreement ends, or when you ask us to close your account, we will delete Customer Personal Data within 30 days, unless Union or Member State law requires us to keep it. Before the Agreement ends, you are responsible for downloading anything you want to keep.

11.3 Deleted data can remain in encrypted database backups until those backups expire in the normal course. We do not restore it from a backup except to recover from an incident, and we then delete it again.

12. Information and audits

12.1 We will make available the information you reasonably need to demonstrate compliance with Article 28 GDPR. That includes this DPA and its annexes, and written answers to a reasonable security questionnaire once per year.

12.2 If that information is not enough, or a supervisory authority requires it, you may audit our compliance, yourself or through an independent auditor bound by confidentiality. You must give at least 30 days' written notice, and the audit must take place during business hours and avoid disrupting the Services. Unless the audit finds a material breach of this DPA, you bear its cost, and you may audit no more than once in any twelve months.

13. Liability, term and governing law

13.1 Each party's liability under this DPA is subject to the limitations of liability in the Terms of Service, to the extent Applicable Data Protection Law allows.

13.2 This DPA stays in force for as long as we process Customer Personal Data, including after the Agreement ends.

13.3 This DPA is governed by Belgian law. The courts of the judicial district of Antwerp have exclusive jurisdiction, as set out in the Terms of Service.

13.4 We may update this DPA, for example when the law changes or we add a Sub-processor. We will not reduce the protection it gives Customer Personal Data without your agreement, and we will give you notice of material changes in the same way as for the Terms of Service.

Annex 1: Details of the processing

Subject matter

Providing the Services: transcribing, subtitling, translating, editing, rendering and exporting audio and video.

Duration

The term of the Agreement, followed by deletion as described in section 11.

Nature of the processing

Storage; automated speech recognition; machine translation and other language-model processing of transcripts; editing; video rendering; transmission to Sub-processors; deletion.

Purpose

Solely to provide the Services to you, including support you ask for and keeping the Services secure.

Data subjects

People whose voice, image or name appears in Customer Content; people mentioned in it; and your authorised users.

Categories of personal data

Voice recordings; images and likeness in video; spoken words as transcribed and translated; speaker labels; names in file and project names; and, for your users, names, email addresses, IP addresses and usage logs.

Special categories of data

The Services do not require them, but Customer Content may contain them, for example health information discussed in a documentary. They are processed only as part of Customer Content, under the same measures. Voices are not used to identify people: speakers are labelled, not recognised.

Frequency

Continuous, for as long as you use the Services.

Retention

Until you delete the content, or as described in section 11.

Annex 2: Security measures

Hosting in the EU

File storage, the database, application servers and processing jobs run in Paris, France, on Amazon Web Services, MongoDB Atlas and Vercel. Speech recognition runs in the EU with Soniox, Reson8 and Speechmatics; the backup provider ElevenLabs is being moved to its EU environment (see Annex 3).

Encryption

All connections use TLS, and HTTPS is enforced with HTTP Strict Transport Security. Stored files and the database are encrypted at rest with AES-256.

Access control

Apart from sign-in, sign-up and callbacks from our providers, every page and API request of the application requires an authenticated session, and access to projects is restricted by project and folder roles. Media files are delivered through our content delivery network by unlisted links, which the application shows only to users with access to the project; a link gives access to that file without signing in.

Authentication

Passwords are stored as bcrypt hashes. Email addresses are verified before password sign-in, and sign-up is protected against automated abuse.

Staff access

Production access is limited to the engineers who operate the Services. They open Customer Content only when you ask for help with it, or when security or the law requires it.

Application security

Uploads of file types a browser could execute are refused. A Content Security Policy and anti-framing headers are applied to every page. Database identifiers are validated before use.

Deletion

Deleting a project in the application removes its records from the database straight away. On request, we delete any stored files that remain, such as preview copies and rendered videos, within 30 days (section 11).

Data minimisation

Each Sub-processor receives only what its task needs: speech recognition receives the media file, and language models receive transcript text, never audio or video.

Sub-processor management

Every Sub-processor processes Customer Personal Data under data protection terms, and the terms or account settings of each AI provider exclude using Customer Content to train its models.

Annex 3: Sub-processors

We use the following Sub-processors at the date of this DPA.

Amazon Web Services

Amazon Web Services EMEA SARL, Luxembourg

Stores your files and runs our processing: preview copies, waveforms, thumbnails, transcription and subtitle jobs, and video rendering. Delivers files to your browser through Amazon CloudFront.

What it receives

Your uploaded media and everything produced from it.

Where

EU (Paris, France). CloudFront can briefly cache a file at the edge location nearest the person viewing it.

Transfer safeguard

AWS Data Processing Addendum, including the Standard Contractual Clauses, for edge caching outside the EEA.

MongoDB Atlas

MongoDB Limited, Ireland

Our database.

What it receives

Transcripts, subtitles, translations, project and file names, and account details.

Where

EU (Paris, France)

Vercel

Vercel Inc., United States

Hosts the web application. Its server functions handle every request the editor makes.

What it receives

Content passing through the application while you use it, account details and IP addresses.

Where

EU (Paris, France) for server functions. Static pages are served from Vercel's global network.

Transfer safeguard

Standard Contractual Clauses

Soniox

Soniox, Inc., United States

Speech recognition: turns the audio in your file into a transcript. Our primary provider, except for files uploaded as Dutch – dialect.

What it receives

Your audio or video file, which it fetches from our storage, and your custom vocabulary.

Where

EU, through Soniox's EU endpoint: audio and transcripts are processed and stored in the EU.

Transfer safeguard

Standard Contractual Clauses, for the service metadata Soniox may process outside the EEA

Reson8

Resonate Labs B.V., the Netherlands

Speech recognition for files uploaded as Dutch – dialect. When it is unavailable, those files go to Soniox.

What it receives

Your audio or video file and your custom vocabulary.

Where

EU (the Netherlands), on servers Reson8 runs itself.

ElevenLabs

Eleven Labs Inc., United States

Backup speech recognition, used only when Soniox is unavailable and the file is under 1 GB.

What it receives

Your audio or video file and your custom vocabulary.

Where

United States for now. We are moving it to ElevenLabs' EU data residency environment.

Transfer safeguard

EU-U.S. Data Privacy Framework

Speechmatics

Cantab Research Limited, United Kingdom

Backup speech recognition for files of 1 GB or more, used only when Soniox is unavailable.

What it receives

Your audio or video file and your custom vocabulary.

Where

EU

Transfer safeguard

UK adequacy decision, for access from the United Kingdom

Google Gemini API

Google LLC, United States

Language models that lay out subtitles, translate them, and write chapters and highlights.

What it receives

Transcript text with timings and speaker labels, and any instructions you add, such as tone of voice. Never your audio or video.

Where

Not fixed: Google may process requests in any of its data centres.

Transfer safeguard

EU-U.S. Data Privacy Framework, and Google's data processing terms with the Standard Contractual Clauses

Resend

Plus Five Five, Inc., United States

Sends account and notification emails.

What it receives

Your email address, and the project names and links in notification emails.

Where

United States

Transfer safeguard

Standard Contractual Clauses

PostHog — PostHog Inc., United States

Product analytics: which features are used, linked to a pseudonymous user ID.

What it receives

Usage events from the application, which can include the text of on-screen elements you click, such as a line of a transcript.

Where

EU (Frankfurt, Germany)

Transfer safeguard

Standard Contractual Clauses, for access from the United States