Policy & privacy

Claritalk Data Processing Agreement (DPA)

What does our DPA look like? This agreement governs how Claritalk processes personal data on behalf of the customer in recording, transcribing and analyzing business conversations, in accordance with Article 28 GDPR. The fields in square brackets are completed per customer upon signature.

Parties

1. **[Customer Name]**, with registered office at [address], registered under business number [number], duly represented by [name, title], hereinafter "**Controller**" or "**Customer**";
2. **SalesNote BV**, trading as Claritalk, with registered office at Staatsbaan 305, 9870 Zulte, registered under business number BE 0765.323.961, hereinafter "**Processor**" or "**Claritalk**".

Recitals

- Claritalk provides a conversational intelligence platform (the "**Platform**") that records or receives business conversations (meetings, phone calls, interviews), transcribes them and uses AI to convert them into summaries, tasks, file knowledge and insights.
- The parties have entered into a main agreement or subscription (the "**Main Agreement**"), whereby Claritalk processes personal data on behalf of the Customer.
- This data processing agreement (the "**Agreement**") is an integral part of the Main Agreement. In case of conflict regarding the processing of personal data, this Agreement takes precedence.

Article 1. Definitions

Terms in this Agreement have the meaning from Regulation (EU) 2016/679 (the "**GDPR**"). Additionally, the following applies:

- **Personal Data**: all personal data that Claritalk processes on behalf of the Customer, as described in Annex 1.
- **Customer Content**: audio recordings, transcripts, summaries, tasks, notes, attachments, chat messages with the AI assistant ("Clara") and other content that is placed or generated on the Platform by or for the Customer.

- **Sub-processor**: a third party that Claritalk engages and who gains access to Personal Data (Annex 3).
- **Customer Integration**: a link with a system of the Customer (e.g. CRM, accounting or calendar software) that the Customer activates itself (Annex 4).
- **Breach**: a personal data breach as referred to in Article 4(12) GDPR.
- **EEA**: the European Economic Area.

Article 2. Subject, nature and purpose of processing

1. Claritalk processes Personal Data solely to provide the Platform as agreed in the Main Agreement. The nature, purpose, duration and categories of data and data subjects are set out in Annex 1.
2. Processing includes in particular:
    1. recording or receiving audio via the web and mobile app, a meeting bot (Microsoft Teams, Google Meet, Zoom) or telephony integrations;
    2. transcribing that audio (real-time or afterwards), including speaker recognition and translation;
    3. generating summaries, tasks, conversation analyses and answers by AI language models;
    4. indexing and making Customer Content searchable;
    5. synchronizing data with Customer Integrations at the Customer's request;
    6. sending emails and push notifications related to Platform usage.
3. Claritalk processes Personal Data only on the basis of written instructions from the Customer. The Main Agreement, this Agreement and the configuration that the Customer chooses in the Platform shall be considered such instructions.
4. Claritalk does **not** use Customer Content to train its own AI models or those of Sub-processors, unless the Customer has previously given express written consent.
5. Claritalk may use anonymized or aggregated usage data (e.g. number of meetings, AI token consumption) for billing, capacity planning and product improvement, provided such data is not attributable to individuals.

Article 3. Obligations of the Processor

1. Claritalk processes Personal Data only according to the documented instructions of the Customer, including transfers to third countries, unless a Union or Member State law requires processing. In that case, Claritalk notifies the Customer of that obligation in

advance, unless the law prohibits this.

2. Claritalk shall notify the Customer immediately if an instruction is believed to infringe the GDPR or other privacy legislation.
3. Claritalk ensures that persons authorized to process Personal Data are bound by a confidentiality obligation and only have access to the extent their task requires.
4. Access by Claritalk employees to a customer account (e.g. for support via the "impersonate" feature) occurs only at the request of or with the permission of the Customer and is logged.
5. Claritalk maintains a record of processing activities as referred to in Article 30(2) GDPR.
6. Claritalk provides reasonable assistance to the Customer in conducting data protection impact assessments (DPIA) and prior consultations with the supervisory authority.
7. The Customer remains responsible for the lawfulness of processing, in particular for informing conversation participants of the recording and, where required, obtaining their consent.

Article 4. Sub-processors

1. The Customer gives Claritalk general written permission to engage the Sub-processors listed in Annex 3.
2. Claritalk informs the Customer at least **30 days** in advance of the addition or replacement of a Sub-processor, by email or via the Platform. The Customer may raise a reasoned objection within that period. If a solution cannot be found within a reasonable time, the Customer may terminate the affected part of the service without right to compensation for either party.
3. Claritalk imposes the same data protection obligations on each Sub-processor in writing as set out in this Agreement, in particular appropriate technical and organizational measures.
4. Claritalk remains fully liable to the Customer for the performance of the obligations of its Sub-processors.
5. Providers of Customer Integrations (Annex 4) are not Sub-processors of Claritalk. They are chosen and activated by the Customer itself; the Customer has its own contractual relationship with those parties.

Article 5. Transfers outside the EEA

1. Claritalk processes and stores Personal Data exclusively within the EEA. Hosting and storage are provided by TransIP in the Netherlands; all Sub-processors process data in an EU region (Annex 3).

2. Some Sub-processors are part of a group with headquarters outside the EEA, e.g. in the United States. Should a transfer or access from a third country occur (e.g. for support or maintenance), it shall be done only with an appropriate safeguard according to Chapter V GDPR:
    1. certification under the EU-US Data Privacy Framework; or
    2. the standard contractual clauses of the European Commission (Decision (EU) 2021/914), supplemented by a transfer impact assessment and additional measures where necessary.
3. Claritalk shall not transfer processing outside the EEA without first informing the Customer according to Article 4.2.
4. Upon request, Claritalk shall provide the Customer with a copy of the relevant safeguards.

Article 6. Security

1. Claritalk takes appropriate technical and organizational measures in accordance with Article 32 GDPR, taking into account the state of the art, costs and risks to data subjects. Conversation recordings may contain confidential and sensitive information; the level of security takes this into account.
2. The measures in effect on the date of this Agreement are set out in Annex 2. Claritalk may modify them, provided that the overall level of protection does not decrease.
3. Claritalk regularly tests, evaluates and assesses the effectiveness of those measures.

Article 7. Personal Data Breaches

1. Claritalk shall notify the Customer of a Breach without undue delay and no later than **48 hours** after becoming aware of it, via [Customer email address/contact person].
2. The notification shall contain, to the extent known: the nature of the Breach, the categories and estimated number of data subjects and data records affected, the likely consequences, the measures taken and proposed, and a contact point at Claritalk. Information not yet available shall be provided as soon as possible.
3. Claritalk shall immediately take reasonable measures to contain the Breach and limit the consequences, and shall document every Breach.
4. The Customer shall decide whether the Breach is reported to the supervisory authority and/or to the data subjects. Claritalk shall not do so itself, unless the law requires it.

Article 8. Rights of data subjects and assistance

1. Claritalk shall assist the Customer with appropriate technical and organizational measures to respond to requests from data subjects (access, rectification, erasure, restriction, portability and objection).
2. The Platform provides the Customer with functionality for this purpose, including viewing, editing and deleting meetings, transcripts and files, exporting reports (PDF, Word, Excel) and deleting users.
3. If Claritalk receives a request from a data subject directly, it shall forward it to the Customer without undue delay and shall not respond to it itself, unless instructed to do so by the Customer.
4. Assistance beyond the standard functionality of the Platform may be charged by Claritalk at standard rates, subject to prior agreement from the Customer.

Article 9. Audit

1. Claritalk shall make available to the Customer all information necessary to demonstrate compliance with Article 28 GDPR.
2. The Customer may conduct an audit maximum **once per calendar year**, either itself or by an independent auditor with confidentiality obligation. In case of suspected serious Breach or by order of a supervisory authority, this limitation does not apply.
3. The Customer shall announce an audit in writing at least **30 days** in advance. The audit shall not unreasonably disrupt Claritalk's operations and shall not provide access to data of other customers.
4. The costs of the audit are borne by the Customer, unless the audit reveals a material breach of Claritalk's obligations.
5. Claritalk shall first respond to an audit request in writing, with a completed standard security questionnaire and, if available, recent certifications or audit reports from Claritalk or its Sub-processors. An on-site audit is only possible if that information is reasonably insufficient to demonstrate compliance.

Article 10. Duration, retention and deletion

1. This Agreement runs as long as the Main Agreement runs and as long as Claritalk continues to process the Customer's Personal Data thereafter.
2. During the term, the Customer determines the retention periods. The Platform allows setting a retention period for meetings and a separate retention period for audio recordings per organization; after expiration, a daily task automatically deletes the relevant data.

3. In addition, the following standard retention periods apply:

Data	Retention period
Audio not linked to a meeting or not retrieved	3 days after recording
Incomplete audio upload chunks	until cleanup of outdated chunks
Audit logs (incl. AI audit logs)	90 days active, then archived; deleted after 365 days
AI consumption log (tokens per organization)	5 years (1,825 days), for billing and accounting
Expired access tokens, invitations and shared report links	deleted upon expiration
Back-ups	2 months, at TransIP (Netherlands, EU)

1. After expiration of the Main Agreement, Claritalk shall delete all Personal Data within **30 days**, or at the Customer's request shall first return it in a common format. Copies in back-ups shall be overwritten according to the normal back-up cycle of maximum 2 months and shall not be actively used until then.
2. Claritalk shall confirm deletion in writing upon request. Retention shall remain possible to the extent required by law.

Article 11. Liability and final provisions

1. The liability of the parties under this Agreement shall be governed by the liability provisions of the Main Agreement, without prejudice to Article 82 GDPR.
2. Amendments to this Agreement are only valid if accepted in writing by both parties. An update to Annex 3 according to Article 4 does not require re-signature.
3. If any provision is invalid or unenforceable, the remaining provisions shall remain in force. The parties shall replace the invalid provision with a valid one that comes as close as possible to the intent.
4. This Agreement shall be governed by Belgian law. Disputes shall be submitted to the competent courts of Kortrijk.

Signature

Executed at [location] on [date], in two copies.

	For the Customer	For Claritalk
Name		

Title		
Signature		

Annex 1. Description of processing

Item	Description
Purpose	Recording, transcribing, summarizing and analyzing business conversations; file and task management; AI assistant (Clara); synchronization with Customer systems; support and billing of the Platform
Nature	Collecting, recording, storing, transcribing, translating, analyzing with AI language models, indexing, querying, exporting, transferring to Customer Integrations, deleting
Duration	Term of the Main Agreement, plus the retention periods from Article 10
Frequency	Continuous

Categories of data subjects

- Users of the Platform (employees and administrators of the Customer)
- Conversation participants: customers, prospects, suppliers, candidates, colleagues and other persons participating in or mentioned in recorded conversations
- Contacts and relationships from Customer systems linked to the Platform (CRM, accounting, calendar)

Categories of personal data

- **Account and identity data**: name, email address, profile photo, job title, language, organization and team, role and permissions, login credentials (hashed passwords, 2FA settings, SSO link with Microsoft or Google)
- **Conversation content**: audio recordings, transcripts with speaker labels, summaries, tasks, notes, conversation topics, analyses and evaluations of conversations
- **Calendar and meeting data**: title, time, participants (name, email address), meeting link
- **File and relationship data**: names, contact information and company data of relationships, synchronized from Customer Integrations
- **Attachments**: documents that users attach to meetings or files
- **Chat data**: questions to and answers from the AI assistant
- **Telephony data** (if activated): phone number, time and duration of calls
- **Technical data**: IP address, device and browser data, push notification tokens, log files, error messages, usage statistics

Special categories

The Platform is not designed for special categories of personal data (Article 9 GDPR) or criminal data (Article 10 GDPR). Because conversations flow freely, they may contain such data (e.g. health information during an HR meeting). Additionally, a voice recording is technically a biometric data, but the Platform does not use voices to uniquely identify persons. The Customer assesses whether its use requires a DPIA.

Annex 2. Technical and organizational measures

Area	Measure
Access control	Role-based permissions per organization and team; data strictly separated per organization (multi-tenant)
Authentication	Hashed passwords; two-factor authentication (2FA); SSO via Microsoft Entra ID and Google; email verification; OAuth2 tokens (Passport/Sanctum) with expiration and automatic cleanup
Support access	Logging in as user (impersonation) only by authorized staff, logged
Encryption in transit	TLS for all traffic, including websockets and connections with Sub-processors
Encryption at rest	Integration tokens and secrets encrypted in storage; audio storage in S3-compatible object storage at TransIP (Netherlands) with encryption at rest
Temporary keys	Real-time transcription (Speechmatics, Gladia, Azure Speech) and LiveKit work with short-lived tokens; main keys remain on the server
Attachments	Uploaded attachments scanned for malware (ClamAV)
Webhooks	Incoming webhooks verified with HMAC signature and rate limiting
Logging	Audit logs of user and AI actions; personal data and tokens automatically filtered from application logs (PII denylist and patterns) before going to Datadog or Sentry
Secrets management	Environment variables and keys centrally managed in Infisical; not in source code
AI processing	AI providers via a gateway (Portkey) with fallback; routable per organization; no training on Customer Content
Availability	Multiple nodes for Azure Speech and Azure OpenAI with automatic failover; message queue (AMQP) for asynchronous processing; monitoring and alerting
Data minimization	Customizable retention periods for meetings and audio; automatic deletion of unused audio after 3 days

Development	Code review via pull requests; static analysis (PHPStan), architecture rules (Deptrac) and automated tests in the CI/CD pipeline (Azure Pipelines); separate staging and production environment
Organizational	Confidentiality clauses for employees; security awareness training, incident procedure, backup policy and hosting certification

Annex 3. List of Sub-processors

Claritalk engages the Sub-processors below as of the date of this Agreement. The list is derived from the configuration and dependencies of the Platform. All Sub-processors process Personal Data in an EU region.

Infrastructure and storage

Sub-processor	Service	Data processed	Location
TransIP B.V.	Application servers and database (app.claritalk.com)	All Customer Content and account data	EU (Netherlands)
TransIP B.V.	S3-compatible object storage for audio and attachments; back-ups	Audio recordings, attachments, back-ups	EU (Netherlands)
Typesense	Search index	Meeting titles, summaries	EU

Transcription and speech

Sub-processor	Service	Data processed	Location
Microsoft Ireland Operations Ltd. (Azure)	Azure AI Speech (transcription, batch and real-time), Azure Translator	Audio, transcripts	EU (West Europe)
Speechmatics Ltd.	Real-time transcription	Audio, transcripts	EU
Gladia SAS	Real-time transcription	Audio, transcripts	EU (France)
Recall.ai, Inc.	Meeting bot for Teams, Google Meet and Zoom	Audio, video, participant names, meeting chat	EU (eu-central-1, Frankfurt)
LiveKit, Inc.	Live voice connection (roleplay feature)	User audio	EU

AI language models

Sub-processor	Service	Data processed	Location
Portkey AI, Inc.	AI gateway: routing and failover between language models	Prompts and responses (transcripts, file content, chat questions)	EU
OpenAI Ireland Ltd.	Language models for summaries, analyses and the AI assistant	Prompts and responses	EU (EU data residency)
Microsoft Ireland Operations Ltd. (Azure OpenAI)	Language models (fallback and configurable per organization)	Prompts and responses	EU
Mistral AI SAS	Language models for summaries, keywords and conversation scoring	Prompts and responses	EU (France)

Communication

Sub-processor	Service	Data processed	Location
ActiveCampaign, LLC (Postmark)	Transactional email	Name, email address, notification content	EU
Mailgun Technologies, Inc.	Transactional email	Name, email address, notification content	EU
Google LLC (Firebase)	Push notifications (FCM) and real-time synchronization for the mobile app	Device tokens, notification content	EU

Monitoring, analytics and support

Sub-processor	Service	Data processed	Location
Functional Software, Inc. (Sentry)	Error monitoring	Error messages, user ID, technical data (PII filtered)	EU (Germany)
Datadog, Inc.	Logging and monitoring	Application logs (PII filtered), technical data	EU
Mixpanel, Inc.	Product analytics	User ID, usage events	EU
Product Fruits s.r.o.	In-app onboarding and tours	User ID, name, usage data	EU (Czech Republic)

Google LLC (Tag Manager, reCAPTCHA)	Tag management after cookie consent; bot protection	IP address, browser data	EU
Zoho Corporation B.V.	Billing, subscriptions and Claritalk's CRM	Account, contact and invoice data of the Customer	EU (zoho.eu)

Annex 4. Optional integrations at customer initiative

The Customer may link the Platform to the systems below. Data is only exchanged after the Customer activates and authorizes the link itself (usually via OAuth). These providers are not Sub-processors of Claritalk (Article 4.5).

Integration	Category	Data exchanged
Microsoft 365 (Outlook calendar, Outlook Mail, OneNote, Teams)	Calendar, email, notes	Appointments, participants, reports, notes
Google Calendar	Calendar	Appointments and participants (read-only)
Zoho CRM	CRM	Contacts, companies, reports
Teamleader	CRM	Contacts, companies, reports
Odoo	CRM / ERP	Contacts, companies, reports
AdminPulse	Practice management (accounting)	Relationships, reports, tasks
Silverfin	Accounting (accounting)	Relationships, reports
Brokercloud	Insurance brokerage	Relationships, reports
FID-Manager	Financial services	Relationships, reports
Qaro	Quality and compliance management	Reports
3CX	Telephony	Call recordings, phone numbers, call metadata
Zoho Flow	Automation	Data configured by the Customer in the flow