

Data Processing Agreement (DPA)

pursuant to Art. 28(3) of the General Data Protection Regulation (GDPR)

Melo Designer GmbH · Alter Schützenweg 14 · 49688 Lastrup · Version: September 2026

between

_____ (hereinafter the “**Controller**”)

and

Melo Designer GmbH, Alter Schützenweg 14, 49688 Lastrup, Germany
represented by its Managing Director Guilherme Alexandre Gonçalves de Melo
(hereinafter the “**Processor**”)

– together the “Parties”, individually a “Party” –

Recital: The Controller uses **Sprecho**, GDPR-compliant voice-dictation software provided by Melo Designer GmbH. In the course of this use the Processor processes personal data on behalf of the Controller. This agreement governs the Parties' rights and obligations pursuant to Art. 28 GDPR and supplements Sprecho's Terms of Service and Privacy Policy.

§ 1 Subject Matter and Duration of Processing

- 1.1** The subject matter of this agreement is the provision of the cloud-based voice-dictation software “Sprecho” as a desktop application (macOS, Windows, Linux) and mobile app (iOS, Android), including speech recognition, AI-assisted text formatting, storage and synchronisation of transcriptions, and associated user management.
- 1.2** The duration of the processing corresponds to the term of the main contract (subscription). It begins upon creation of a user account and ends with the complete deletion of all personal data following termination pursuant to § 16 of this agreement.
- 1.3** Processing takes place exclusively within the European Union / European Economic Area (EU/EEA). The content (audio data and transcriptions) is stored exclusively in Germany; transient speech recognition may run on servers in Germany and/or the Netherlands (further regulated in § 11).
- 1.4** A business customer within the meaning of this agreement is any Controller that uses Sprecho in the course of its commercial, freelance or other independent professional activity (entrepreneur within the meaning of § 14 BGB), irrespective of the selected tariff. This includes sole traders, freelancers as well as non-profit and public bodies.

§ 2 Nature and Purpose of Processing

The Processor processes personal data on behalf of the Controller exclusively for the purposes exhaustively listed below. No processing beyond these purposes takes place.

- 2.1 Speech recognition and transcription:** audio data is transmitted from the user's device to the Processor's servers, converted to text using speech-recognition technology (Whisper) and formatted by a self-hosted AI language model. Processing takes place exclusively within the EU/EEA.
- 2.2 Storage and synchronisation:** transcribed text is stored in a database in Germany and synchronised across devices. Audio data is stored temporarily (14 days by default) or, in privacy mode, deleted immediately after

Melo Designer GmbH

Alter Schützenweg 14, 49688 Lastrup
USt-ID: DE331465335
Handelsregister: HRB 216834
Registergericht: Amtsgericht Oldenburg

Bankverbindung

VR-BANK: DE85280615010030682700
BIC: GENODEF1CLP
Sparkasse IBAN: DE412665 0001 1091 0847 54
BIC: NOLADE21EMS

Kontakt

Tel: +49 (0) 4475 929 6293
Mobil: +49 (0) 173 2304 748
info@melodesigner.de
www.melodesigner.de

transcription.

- 2.3 User management:** management of user accounts, authentication, session management and settings.
- 2.4 Dictionary and auto-corrections:** storage of user-defined word corrections to improve transcription quality.
- 2.5 Billing:** management of subscriptions, invoicing and payment processing via external payment service providers.
- 2.6 Email communication:** sending of transactional emails (verification, password reset, billing notifications).
- 2.7 Optional training data:** only where the user's consent is enabled, anonymised transcriptions are used to improve the model (further regulated in § 4). Without consent no processing takes place for this purpose.

§ 3 Categories of Personal Data

The following categories of personal data are processed:

- 3.1 Voice and audio data:** users' voice recordings, which may contain any kind of personal content (e.g. medical, legal or business dictation).
- 3.2 Transcription data:** raw, formatted and user-edited text.
- 3.3 Account data:** email address, name, password hash, language preference, profession, preferred dictation languages.
- 3.4 Session and device data:** IP address, user agent, device ID, session tokens.
- 3.5 Application context:** name and identifier of the active application (always captured, required for formatting); window title and URL (transient only, on the device and during processing, not stored); visible text excerpt (~500 characters, optional and deactivatable, § 5).
- 3.6 Billing data:** billing name, company, address, VAT ID. Card/IBAN data is processed exclusively by the payment service provider.
- 3.7 Usage data:** timestamps, recording duration, insertion method.
- 3.8 Communication data:** email addresses for transactional notifications.

§ 4 Special Categories of Personal Data (Art. 9 GDPR) and AI Training

- 4.1** The Processor is aware that dictated content may contain special categories of personal data within the meaning of Art. 9(1) GDPR (in particular health data). All dictation content is treated as potentially containing Art. 9 data and protected accordingly.
- 4.2 No use of Controller data for AI training:** personal data of the Controller and its users is not used to train AI models. The optional training-data collection can be disabled by the user at any time in the settings; from that point on, and in privacy mode, no processing of transcription data for training purposes takes place whatsoever. For Enterprise customers, training-data collection is **disabled by default** and locked centrally via team policy; towards Enterprise customers this constitutes a binding assurance.
- 4.3** Special categories of personal data from dictation are never used to train AI models. Even where consent is given (outside Enterprise customer accounts), all personal data is replaced with realistic placeholders on the user's device before any transmission (on-device anonymisation).
- 4.4** Privacy mode enables immediate deletion of all data right after the text is inserted. Alternatively, individual retention periods can be configured (immediate, 1 day, 1 week, 1 month, 3 months).

Melo Designer GmbH

Alter Schützenweg 14, 49688 Lastrup
USt-ID: DE331465335
Handelsregister: HRB 216834
Registergericht: Amtsgericht Oldenburg

Bankverbindung

VR-BANK: DE85280615010030682700
BIC: GENODEF1CLP
Sparkasse IBAN: DE412665 0001 1091 0847 54
BIC: NOLADE21EMS

Kontakt

Tel: +49 (0) 4475 929 6293
Mobil: +49 (0) 173 2304 748
info@melodesigner.de
www.melodesigner.de

§ 5 Application-Context Data

- 5.1 Purpose:** to improve transcription accuracy the service optionally captures contextual metadata during dictation.
- 5.2 Screen content:** a text excerpt (~500 characters) of the active window may be captured. This feature can be fully disabled in settings; once disabled, no screen content is captured or transmitted.
- 5.3 Base metadata:** application name and application identifier are captured to detect the formatting style and are subject to the same configurable retention periods as the transcription. Window title and URL are used exclusively transiently, on the device and during processing, and are not stored.
- 5.4 No use for AI training:** application-context data is never used to train AI models.
- 5.5 Recommendation for healthcare and social services:** for medical practices, medical institutions and providers of social services, child and youth welfare, the Processor recommends disabling context awareness and enabling privacy mode or a short retention period.

§ 6 Categories of Data Subjects

The processing concerns in particular the following sector-specific categories of data subjects. The categories actually relevant depend on the Controller's intended use and its staff's use of the service:

- **Active users:** employees and staff of the Controller who use Sprecho for dictation and productivity purposes (log-in, configuration, usage behaviour);
- **Freelancers and external contractors authorised by the Controller** who are permitted to use the service in the context of their work for the Controller;
- **Patients** and their relatives whose data (including health data, diagnoses, findings, medication, treatment history) appears in medical dictation (particularly relevant for practices, MVZs, hospitals, expert witnesses);
- **Clients** and parties to proceedings, witnesses, opposing parties and other third parties named in the mandate whose data appears in legal dictation (particularly relevant for law firms, notaries' offices, tax consultancies);
- **Staff and applicants of third parties**, in particular in staffing services and temporary work (AÜG): applicant master data, qualifications, residence permits, social-security data, deployment reports, time recording, payroll and settlement data (particularly relevant for staffing service providers; cf. § 26 BDSG and Art. 88 GDPR);
- **Customer and prospect contacts** of the Controller whose name, contact data or role assignment is dictated in business correspondence, offers, order confirmations or memos;
- **Supplier and partner contacts** whose data appears in orders, complaints or negotiation records;
- **Children, adolescents and members of specially protected groups**, where their data is dictated (e.g. in reports of youth welfare services, school and educational contexts or social counselling);
- **Other third parties** whose personal data is mentioned in dictated content of the Controller (e.g. witnesses, experts, publicly acting persons, other natural persons named in memos).

Clarification: the above categories are named on a sector-typical basis and are not collected by the Processor itself. Which categories are actually processed depends solely on the dictation content of the Controller's users and lies within the Controller's sphere of responsibility.

§ 7 Right to Issue Instructions and Scope of Instructions

- 7.1** The Processor processes personal data only on documented instructions from the Controller, unless required to process by Union or Member-State law; in that case it informs the Controller of that legal requirement before processing, unless the law prohibits this on important grounds of public interest.
- 7.2** Instructions are issued in text form as a rule (email is sufficient). Oral instructions must be confirmed in text form without delay. The Processor documents the instructions issued to it.

Melo Designer GmbH

Alter Schützenweg 14, 49688 Lastrup
USt-ID: DE331465335
Handelsregister: HRB 216834
Registergericht: Amtsgericht Oldenburg

Bankverbindung

VR-BANK: DE85280615010030682700
BIC: GENODEF1CLP
Sparkasse IBAN: DE412665 0001 1091 0847 54
BIC: NOLADE21EMS

Kontakt

Tel: +49 (0) 4475 929 6293
Mobil: +49 (0) 173 2304 748
info@melodesigner.de
www.melodesigner.de

- 7.3 Only the persons named in **Annex G** are authorised to issue instructions (Controller side) and to receive them (Processor side). Changes must be notified to the other Party in text form.
- 7.4 The content of instructions is determined by this agreement, the main contract and the Controller's documented configuration settings (e.g. retention periods, privacy mode, training-data consent). The Controller may supplement the processing by individual instructions within the scope of the service description.
- 7.5 **Notice of unlawful instructions:** the Processor informs the Controller without delay if, in its opinion, an instruction infringes the GDPR or other Union or Member-State data-protection provisions. The Processor is entitled to suspend the execution of that instruction until it is confirmed or amended.
- 7.6 Extraordinary instructions not covered by the service description may be remunerated separately.

§ 8 Obligations of the Processor

- 8.1 The Processor implements all technical and organisational measures (TOMs) required under Art. 32 GDPR, described in detail in **Annex D**.
- 8.2 The Processor complies with the conditions for engaging further processors pursuant to § 10.
- 8.3 The Processor assists the Controller in responding to data-subject requests (Chapter III GDPR) pursuant to § 14 and in complying with Art. 32–36 GDPR pursuant to § 13.
- 8.4 Upon completion of the processing the Processor deletes or returns all personal data pursuant to § 16, unless a statutory retention obligation applies.
- 8.5 The Processor makes available to the Controller all information necessary to demonstrate compliance with Art. 28 GDPR and allows for reviews pursuant to § 17.
- 8.6 The Processor does not process the data for its own purposes (see § 4 regarding anonymised, consented training data outside Enterprise customer accounts).

§ 9 Confidentiality Obligation of Authorised Persons

- 9.1 The Processor ensures that all persons authorised to process the personal data (employees, temporary workers, freelancers and other contributors) have committed themselves **personally and in text form, before commencing their activity**, to confidentiality or are under an equivalent statutory confidentiality obligation.
- 9.2 The confidentiality obligation expressly covers observance of data secrecy under § 53 BDSG, compliance with special confidentiality duties (including § 203 StGB where applicable) and the prohibition on processing personal data for purposes other than those contractually agreed.
- 9.3 The confidentiality obligation continues **after the end of the activity** of the respective person and after termination of this agreement. Upon a bound person's departure, their access rights to the Controller's personal data are revoked without delay.
- 9.4 All persons involved in the processing are instructed and trained on the relevant data-protection provisions before commencing their activity and at regular intervals (at least annually). Training completion is documented.
- 9.5 Access to the Controller's personal data is limited exclusively to those persons who require it to provide the contractual services (need-to-know principle). Access roles and permissions are documented and reviewed as part of the annual audits.
- 9.6 **Duty of proof:** upon written request from the Controller, the Processor shall provide within a reasonable period an anonymised, aggregated confirmation of the confidentiality obligations in place (number of bound persons, date of each undertaking, date of last data-protection training). Upon request, the Processor shall additionally provide a template of the confidentiality declaration used.

Melo Designer GmbH

Alter Schützenweg 14, 49688 Lastrup
USt-ID: DE331465335
Handelsregister: HRB 216834
Registergericht: Amtsgericht Oldenburg

Bankverbindung

VR-BANK: DE85280615010030682700
BIC: GENODEF1CLP
Sparkasse IBAN: DE412665 0001 1091 0847 54
BIC: NOLADE21EMS

Kontakt

Tel: +49 (0) 4475 929 6293
Mobil: +49 (0) 173 2304 748
info@melodesigner.de
www.melodesigner.de

§ 10 Sub-processors

10.1 The engagement of sub-processors follows the authorisation option selected below. The option ticked in the cover sheet or in **Annex B** applies:

10.2 ☐ **General authorisation with right to object:** the Controller grants a general written authorisation. The Processor informs of any intended change; the Controller may object within **30 calendar days**. Where a justified objection cannot be resolved amicably, the Controller has a right to extraordinary termination.

10.3 ☐ **Specific prior authorisation:** each addition or replacement of a sub-processor requires the Controller's prior authorisation in text form.

10.4 By contract, the Processor imposes on each sub-processor the same data-protection obligations as in this agreement and remains responsible to the Controller for their compliance.

Current list of sub-processors (as of September 2026) – see also Annex B:

Sub-processor	Location	Purpose	Data processed
STRATO GmbH	Germany	server hosting, application server, PostgreSQL database, file and audio storage	all stored service data (audio, transcriptions, user, billing data)
Media Trooper GmbH (Trooper.ai)	Germany and Netherlands (EU)	GPU servers for transient speech recognition (Whisper) and AI text formatting; no persistent storage	audio and transcription data (transient during processing)
Hetzner Online GmbH	Germany (Nuremberg)	Off-site database backups (daily, object storage, TLS-encrypted transfer); not in the request path	database backups (all stored service data)
Mollie B.V.	Netherlands (EU)	payment processing	email, billing address, payment tokens
PayPal (Europe) S.à r.l. et Cie, S.C.A.	Luxembourg (EU)	payment processing	email, billing agreement ID
Brevo (Sendinblue)	France (EU)	transactional emails	email address, name, language preference
Haufe-Lexware GmbH & Co. KG (LexOffice)	Germany	invoice generation	name, address, VAT ID, invoice items

Note: all sub-processors that process the Controller's personal data are established within, or process exclusively within, the EU/EEA. No transfer of contract data to a third country takes place (§ 11). Marketing/analytics services on the sprecho.ai website (e.g. Google Analytics, Meta Pixel) are **not the subject of this agreement**; they process no contract data and are addressed in the website privacy policy.

§ 11 Third-Country Transfers

11.1 Processing of the Controller's personal data takes place exclusively within the EU/EEA. **No transfer of contract data to a third country (outside the EU/EEA) takes place.**

11.2 The content (audio data, transcriptions) is stored exclusively on servers in Germany. Transient speech recognition (audio-to-text) may run on servers in Germany and/or the Netherlands (Media Trooper GmbH, German or Dutch data centre, EU/EEA). The content never leaves the EU/EEA.

Melo Designer GmbH

Alter Schützenweg 14, 49688 Lastrup
USt-ID: DE331465335
Handelsregister: HRB 216834
Registergericht: Amtsgericht Oldenburg

Bankverbindung

VR-BANK: DE85280615010030682700
BIC: GENODEF1CLP
Sparkasse IBAN: DE412665 0001 1091 0847 54
BIC: NOLADE21EMS

Kontakt

Tel: +49 (0) 4475 929 6293
Mobil: +49 (0) 173 2304 748
info@melodesigner.de
www.melodesigner.de

11.3 Should a transfer to a third country be intended in future, it requires the **Controller's prior consent in text form** and is subject to appropriate safeguards pursuant to Art. 44 et seq. GDPR. Without such consent no transfer takes place.

11.4 As no transfer to a third country takes place, standard contractual clauses under Art. 46(2)(c) GDPR or other transfer mechanisms under Art. 44 et seq. GDPR are not required.

No tracking components in the apps: the desktop and mobile apps contain no tracking, analytics or telemetry components whatsoever. Any data transmission from the apps goes exclusively to Sprecho's own servers in the EU/EEA to provide the service.

§ 12 Technical and Organisational Measures (TOMs)

12.1 The Processor has implemented the technical and organisational measures pursuant to Art. 32 GDPR described in **Annex D** and maintains them throughout the term of the agreement.

12.2 The measures are subject to technical progress; the Processor reviews them for effectiveness and adequacy **at least once a year** and on an ad-hoc basis (e.g. after a personal-data breach) and adapts them where necessary. Material changes that would reduce the level of protection are not permitted; improvements are documented.

12.3 The Controller was able to satisfy itself of compliance with the TOMs before processing began; the result is documented in this Annex D. Ongoing compliance may be verified pursuant to § 17.

§ 13 Assistance with Obligations under Art. 32–36 GDPR

Taking into account the nature of the processing and the information available to it, the Processor assists the Controller in complying with the following obligations:

13.1 Security of processing (Art. 32): through the TOMs described in Annex D and their regular review (§ 12).

13.2 Breach notification (Art. 33, 34): through prompt notification and assistance pursuant to § 15.

13.3 Data-protection impact assessment (Art. 35): on request, the Processor provides the information about the processing operations necessary for the Controller to carry out a DPIA. A DPIA may be required in particular when processing special categories of data (e.g. health data).

13.4 Prior consultation (Art. 36): where a DPIA indicates that the processing would result in a high risk, the Processor assists the Controller in any prior consultation of the competent supervisory authority and provides the information required for this.

§ 14 Rights of Data Subjects

14.1 The Processor assists the Controller in fulfilling data-subject rights pursuant to Art. 15–22 GDPR:

- a) **Access (Art. 15):** user data is viewable in account settings; on request the Processor provides a full data export.
- b) **Rectification (Art. 16):** users can edit profile data, transcriptions and dictionary entries themselves.
- c) **Erasure (Art. 17):** individual transcriptions and the entire account can be deleted (cascading deletion).
- d) **Restriction (Art. 18):** accounts can be suspended on request.
- e) **Portability (Art. 20):** export in a structured, commonly used, machine-readable format.
- f) **Objection (Art. 21):** privacy mode disables optional data collection; any training-data consent can be withdrawn at any time.

Melo Designer GmbH

Alter Schützenweg 14, 49688 Lastrup
USt-ID: DE331465335
Handelsregister: HRB 216834
Registergericht: Amtsgericht Oldenburg

Bankverbindung

VR-BANK: DE85280615010030682700
BIC: GENODEF1CLP
Sparkasse IBAN: DE412665 0001 1091 0847 54
BIC: NOLADE21EMS

Kontakt

Tel: +49 (0) 4475 929 6293
Mobil: +49 (0) 173 2304 748
info@melodesigner.de
www.melodesigner.de

14.2 The Processor assists the Controller within **72 hours** of receiving a forwarded data-subject request. If a data subject contacts the Processor directly, the Processor refers them to the Controller and informs the Controller without delay.

§ 15 Personal-Data-Breach Notification

15.1 The Processor reports any personal-data breach to the Controller without undue delay, and at the latest within **24 hours** of becoming aware of it.

15.2 The notification includes at least:

- a) a description of the nature of the breach, including the categories and approximate number of data subjects and records concerned;
- b) the name and contact details of the point of contact;
- c) the likely consequences of the breach;
- d) the measures taken or proposed to address the breach.

15.3 The Processor documents all breaches and assists the Controller with its notification duties towards the supervisory authority (Art. 33) and the communication to data subjects (Art. 34).

§ 16 Deletion and Return of Data

16.1 Upon termination of the main contract the Processor deletes all of the Controller's personal data within **30 calendar days**, unless a statutory retention obligation applies. Backup copies are deleted within the same period.

16.2 Before termination the Controller may request a full data export in a structured, commonly used, machine-readable format.

16.3 Anonymised training data (where consent was given outside Enterprise customer accounts) may be retained as it no longer constitutes personal data.

16.4 Statutory retention periods remain unaffected (in particular invoices: 10 years pursuant to § 147 AO). Category-specific retention periods are set out in **Annex E**.

16.5 The Processor confirms complete deletion in text form on request.

§ 17 Audit Rights of the Controller

17.1 The Controller has the right to verify compliance with this agreement through audits and may engage an independent auditor for this purpose.

17.2 Audits may be conducted once a year and on an ad-hoc basis (upon a breach or specific suspicion). The Processor provides relevant documentation and certifications (e.g. Annex C), answers questionnaires and enables on-site or remote audits with reasonable notice (14 calendar days).

17.3 The Controller bears the costs unless the audit reveals a breach of this agreement by the Processor.

§ 18 Liability

18.1 The Parties' liability is governed by Art. 82 GDPR. The internal allocation of liability follows the main contract and the provisions of the GDPR.

18.2 The Processor is liable for damage caused by processing that does not comply with the GDPR or this agreement.

18.3 The Processor is not liable for damage resulting from the Controller's instructions that infringe the GDPR, provided it informed the Controller of the infringement pursuant to § 7(5).

Melo Designer GmbH

Alter Schützenweg 14, 49688 Lastrup
USt-ID: DE331465335
Handelsregister: HRB 216834
Registergericht: Amtsgericht Oldenburg

Bankverbindung

VR-BANK: DE85280615010030682700
BIC: GENODEF1CLP
Sparkasse IBAN: DE412665 0001 1091 0847 54
BIC: NOLADE21EMS

Kontakt

Tel: +49 (0) 4475 929 6293
Mobil: +49 (0) 173 2304 748
info@melodesigner.de
www.melodesigner.de

§ 19 Reference to Statutory Sanctions

The Parties have been informed of the applicability of the fines and penalties under Art. 83 and 84 GDPR and §§ 42 and 43 BDSG. Infringements of data-protection provisions may be sanctioned with significant fines and criminal consequences.

§ 20 Final Provisions

20.1 This agreement forms part of the main contract. In the event of conflicts on data-protection matters, this agreement prevails.

20.2 Amendments and supplements require text form (email is sufficient).

20.3 The law of the Federal Republic of Germany applies. The place of jurisdiction is Oldenburg (Oldb.), provided the Controller is a merchant, a legal entity under public law or a special fund under public law.

20.4 Should individual provisions be invalid, the validity of the remaining provisions remains unaffected; the invalid provision is replaced by a valid one that comes closest to its economic purpose.

20.5 This agreement enters into force upon signature by both Parties. The Controller sends the version signed by it to dpo@sprecho.ai; the Processor returns the countersigned version as a PDF by email within five working days.

Lastrup, _____

Processor

Melo Designer GmbH



Guilherme Alexandre Gonçalves de Melo
Managing Director

Controller

Name, function
Date, signature

Annex A: Contacts for Data-Protection Inquiries

Processor	Melo Designer GmbH
Data-protection contact	Guilherme Alexandre Gonçalves de Melo (TÜV SÜD certified data-protection officer)
Address	Alter Schützenweg 14, 49688 Lastrup
Phone	+49 4475 9296 293
E-Mail	dpo@sprecho.ai
Website	https://sprecho.ai

Annex B: Sub-processor List

Selected authorisation option (§ 10): ☐ General with right to object ☐ Specific prior authorisation

Melo Designer GmbH

Alter Schützenweg 14, 49688 Lastrup
USt-ID: DE331465335
Handelsregister: HRB 216834
Registergericht: Amtsgericht Oldenburg

Bankverbindung

VR-BANK: DE85280615010030682700
BIC: GENODEF1CLP
Sparkasse IBAN: DE412665 0001 1091 0847 54
BIC: NOLADE21EMS

Kontakt

Tel: +49 (0) 4475 929 6293
Mobil: +49 (0) 173 2304 748
info@melodesigner.de
www.melodesigner.de

Sub-processor	Location	Purpose	Data processed
STRATO GmbH	Germany	server hosting, application server, PostgreSQL database, file and audio storage	all stored service data (audio, transcriptions, user, billing data)
Media Trooper GmbH (Trooper.ai)	Germany and Netherlands (EU)	GPU servers for transient speech recognition (Whisper) and AI text formatting; no persistent storage	audio and transcription data (transient during processing)
Hetzner Online GmbH	Germany (Nuremberg)	Off-site database backups (daily, object storage, TLS-encrypted transfer); not in the request path	database backups (all stored service data)
Mollie B.V.	Netherlands (EU)	payment processing	email, billing address, payment tokens
PayPal (Europe) S.à r.l. et Cie, S.C.A.	Luxembourg (EU)	payment processing	email, billing agreement ID
Brevo (Sendinblue)	France (EU)	transactional emails	email address, name, language preference
Haufe-Lexware GmbH & Co. KG (LexOffice)	Germany	invoice generation	name, address, VAT ID, invoice items

The current list is available at <https://sprecho.ai/trust/subprocessors>. Changes are notified pursuant to § 10.

Annex C: Certifications and Evidence

- **STRATO GmbH:** ISO/IEC 27001-certified data centres in Germany; GDPR-compliant
- **Hetzner Online GmbH:** ISO/IEC 27001-certified data centres in Germany
- **Media Trooper GmbH (Trooper.ai):** ISO/IEC 27001-certified data centre in Germany; Netherlands facility meets equivalent Tier III standards
- **Mollie B.V.:** PCI-DSS Level 1
- **Melo Designer GmbH:** Managing Director is a TÜV SÜD certified data-protection officer
- **SSL/TLS:** all connections encrypted (HTTPS/WSS)

Current certification evidence is provided on request.

Annex D: Technical and Organisational Measures (Art. 32 GDPR)

The following measures are documented specifically for the Sprecho service and reviewed regularly pursuant to § 12.

D.1 Physical access control

- ✓ hosting in ISO 27001-certified data centres (STRATO, Media Trooper; off-site backups at Hetzner Online GmbH, Germany) with 24/7 security staff, biometric access control and video surveillance
- ✓ no physical server access by the Processor's staff (managed hosting)

D.2 System access control

- ✓ JWT-based authentication with token expiry (60-min access, 30-day refresh tokens)
- ✓ password hashing with bcrypt/Argon2; OAuth 2.0 (Google, Microsoft, Apple)
- ✓ session management with device detection; admin area restricted to super admins

Melo Designer GmbH

Alter Schützenweg 14, 49688 Lastrup
USt-ID: DE331465335
Handelsregister: HRB 216834
Registergericht: Amtsgericht Oldenburg

Bankverbindung

VR-BANK: DE85280615010030682700
BIC: GENODEF1CLP
Sparkasse IBAN: DE412665 0001 1091 0847 54
BIC: NOLADE21EMS

Kontakt

Tel: +49 (0) 4475 929 6293
Mobil: +49 (0) 173 2304 748
info@melodesigner.de
www.melodesigner.de

D.3 Data access control

- ✓ role-based permission model (user, team admin, team owner, super admin)
- ✓ users access only their own transcriptions; per-user API authorisation on every request

D.4 Transmission control

- ✓ all transmission via TLS/HTTPS; WebSockets via WSS
- ✓ CORS restricted to known domains; secrets as environment variables

D.5 Input control

- ✓ audit trail for training-data review; logging of audio deletions; session tracking with timestamps

D.6 Processing control

- ✓ processing only on documented instructions (§ 7); sub-processors bound by contract

D.7 Availability control

- ✓ redundant power and network; automated PostgreSQL backups; daily off-site backups at Hetzner Online GmbH (Germany, TLS-encrypted transfer); Docker orchestration; health checks

D.8 Separation

- ✓ logical separation by user and team ID; multi-tenant architecture; training data anonymised and stored separately

D.9 Resilience & recoverability

- ✓ regular backups and restore tests; restoration of availability after a physical or technical incident

Annex E: Retention Periods by Data Category

Data category	Retention period
Audio data	14 days by default; configurable (immediate/1 day/1 week/1 month/3 months); privacy mode: immediate deletion
Transcriptions (content)	user-configurable; until deleted by the user or upon account deletion
Application-context metadata	application name/identifier: identical to the associated transcription; window title and URL: not stored
Account data	for the lifetime of the account; deleted within 30 days of account deletion / contract end
Session/usage data (telemetry)	session tokens until expiry (max. 30 days); usage timestamps stored with the transcription
Server log files	14 days
Billing/invoice data	10 years (§ 147 AO)

Annex F: Description of Processing (Art. 28(3) GDPR)

Subject matter	provision of the Sprecho voice-dictation software (§ 1)
Duration	term of the main contract until deletion pursuant to § 16
Nature and purpose	speech recognition, transcription, AI formatting, storage/synchronisation, user management, billing (§ 2)

Melo Designer GmbH

Alter Schützenweg 14, 49688 Lastrup
USt-ID: DE331465335
Handelsregister: HRB 216834
Registergericht: Amtsgericht Oldenburg

Bankverbindung

VR-BANK: DE85280615010030682700
BIC: GENODEF1CLP
Sparkasse IBAN: DE412665 0001 1091 0847 54
BIC: NOLADE21EMS

Kontakt

Tel: +49 (0) 4475 929 6293
Mobil: +49 (0) 173 2304 748
info@melodesigner.de
www.melodesigner.de

Types of data	see § 3; special categories under Art. 9 possible (§ 4)
Categories of data subjects	see § 6 (incl. users, patients, clients, third parties)
Place of processing	EU/EEA; storage in Germany, transient inference Germany/Netherlands (§ 11)

Annex G: Persons Authorised to Issue / Receive Instructions

Controller (authorised to instruct)	Processor (authorised to receive)
Name: _____	Name: Guilherme A. G. de Melo
Function: _____	Function: Managing Director / DPO
E-Mail: _____	E-Mail: dpo@sprecho.ai
Name: _____	
Function: _____	
E-Mail: _____	



Melo Designer GmbH

Alter Schützenweg 14, 49688 Lastrup
USt-ID: DE331465335
Handelsregister: HRB 216834
Registergericht: Amtsgericht Oldenburg

Bankverbindung

VR-BANK: DE85280615010030682700
BIC: GENODEF1CLP
Sparkasse IBAN: DE412665 0001 1091 0847 54
BIC: NOLADE21EMS

Kontakt

Tel: +49 (0) 4475 929 6293
Mobil: +49 (0) 173 2304 748
info@melodesigner.de
www.melodesigner.de