

Data Processing Agreement (DPA)

pursuant to Art. 28 GDPR

Nixi AI GmbH

Version 2.0 · Last updated: 11 September 2026

This is an English translation of the German „Auftragsverarbeitungsvertrag (AVV)“. Only the German version is legally binding; in case of any discrepancy, the German version prevails.

Contracting Parties

Controller

The customer of Nixi AI within the meaning of the document “General Terms and Conditions (GTC)”

Name of the practice or institution: _____

Address: _____

(hereinafter “Controller”)

Processor

Nixi AI GmbH

Adolfsallee 14, 65185 Wiesbaden

HRB 36529, Amtsgericht Wiesbaden

represented by its Managing Director Mahsa Yarahmadi

Email: hello@nixiai.ai · Data protection: privacy@nixiai.ai

(hereinafter “Nixi AI”)

Preamble

The Controller is a doctor, a practice or a clinic. It uses the Nixi AI platform (hereinafter “Service”) to support its medical documentation. In doing so, Nixi AI processes personal data on its behalf, in particular health data of patients that are subject to medical confidentiality.

This Agreement governs the data protection rights and obligations of the parties. It supplements the agreement on the use of the Service, which is based on Nixi AI's GTC (hereinafter “Main Agreement”). “Users” are the persons who use the Service for the Controller. “Sub-processors” are further Processors within the meaning of Art. 28(2) and (4) GDPR. Otherwise, terms have the meaning given to them by the General Data Protection Regulation (GDPR).

All documents referred to in this Agreement are available in the Service under Settings > Privacy („Einstellungen > Datenschutz“) and can be obtained on request from privacy@nixiai.ai; the DPA, the List of Sub-processors, the GTC, the Privacy Policy for the Service and the Patient Consent Template are also available at www.nixiai.ai/legal.

§ 1 Subject Matter, Duration, Nature and Purpose of the Processing

(1) The subject matter of this Agreement is the processing of personal data by Nixi AI on behalf of the Controller in the provision of the Service under the Main Agreement.

(2) The purpose of the processing is AI-assisted medical documentation. The Service comprises:

- recording and transcription;
- AI drafts (clinical notes, patient letters, referrals, discharge reports, translations);
- ICD-10-GM coding suggestions;
- EBM billing suggestions (beta, if included in the plan);
- the storage of this content until its deletion and its transfer to the Controller's practice management system (PVS), as set up by the doctor.

All outputs are drafts and must be reviewed by a doctor before use (§ 13).

(3) The nature of the processing, the data flow, the categories of data subjects, the data categories and the retention periods are described in Annex 1.

(4) The processing lasts for as long as the Main Agreement. The deletion obligations under § 14 remain unaffected.

(5) Nixi AI processes the data exclusively for the purpose stated in paragraph 2 and not for its own purposes. § 12 (anonymised data) remains unaffected.

§ 2 Instructions

(1) Nixi AI processes personal data only on documented instructions from the Controller, including with regard to transfers to a third country. This does not apply where Nixi AI is required to carry out the processing under Union or Member State law. In such a case, Nixi AI informs the Controller of that legal requirement before the processing, unless that law prohibits such information on important grounds of public interest.

(2) The Controller's instructions follow from this Agreement and the Main Agreement. The Controller issues further instructions via the settings in the Service (e.g. retention period, automatic GDT transfer), by using functions (e.g. transfer to the PVS, sending by email) or in text form, for example by email to privacy@nixiai.ai.

(3) If Nixi AI is of the opinion that an instruction infringes the GDPR or other data protection provisions, Nixi AI informs the Controller thereof without undue delay. Nixi AI may suspend the execution of the instruction until the Controller confirms or amends it.

§ 3 Confidentiality

(1) For the processing, Nixi AI only uses persons who have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality (Art. 28(3)(b) GDPR). This obligation continues to apply after the end of their activity.

(2) Nixi AI's employees are given access to the Controller's personal data only to the extent that this is necessary for the provision of the Service.

§ 4 Professional Secrecy (§ 203 StGB)

(1) The Controller and the persons working for it are, as a rule, subject to the duty of confidentiality under § 203 StGB (German Criminal Code). Nixi AI participates in their professional activity as an other participating person within the meaning of § 203(3) StGB. Nixi AI obtains knowledge of third-party secrets only to the extent that this is necessary for the provision of the Service. Nixi AI undertakes vis-à-vis the Controller to keep secret all secrets that become known to it in this context and has been instructed that unauthorised disclosure is a criminal offence under § 203(4) StGB.

(2) Nixi AI has obliged the employees who may obtain knowledge of patient data in the provision of the Service to maintain confidentiality in text form (e.g. email) and has instructed them that a breach of this obligation is a criminal offence (§ 203(4) StGB). The same applies to employees deployed in the future.

(3) Nixi AI obliges Sub-processors that may obtain knowledge of patient data to maintain confidentiality and to oblige the persons they deploy accordingly. For this purpose, a contractual supplement regarding § 203 StGB (Google Cloud Professional Secrecy Addendum) is in place with Google, and a supplementary agreement for professional secrecy holders (Professional Secrecy Amendment) is in place with Microsoft. The other Sub-processors are bound to confidentiality by their data processing agreements.

(4) The Controller decides which data it discloses to Nixi AI via the Service and remains responsible for the lawfulness of this disclosure. § 203(3) StGB permits disclosure to participating persons to the extent that it is necessary for engaging them.

§ 5 Security of Processing

(1) Nixi AI takes the technical and organisational measures required under Art. 32 GDPR to ensure a level of protection appropriate to the risk. The measures are described in the document “Technical and Organisational Measures (TOMs)”, which is attached to this Agreement as Annex 2.

(2) The measures are subject to technical progress. Nixi AI may develop them further and replace them with equivalent or better measures, provided that the level of protection is not reduced. Nixi AI documents material changes in an updated version of the TOMs.

§ 6 Sub-processors

(1) The Controller approves the use of the Sub-processors listed in the “List of Sub-processors” (Annex 3). In addition, it grants Nixi AI general authorisation within the meaning of Art. 28(2) GDPR to engage further Sub-processors or to replace existing ones in accordance with the procedure set out in paragraphs 2 and 3.

(2) Nixi AI announces any intended engagement or replacement of a Sub-processor at least 30 days in advance by email (text form) to the email address stored in the account.

(3) The Controller may object to the change on data protection grounds within 14 days of receipt of the announcement in text form, for example by email to privacy@nixiai.ai. The parties shall then endeavour to reach an amicable solution. If no agreement is reached, the Controller may terminate the Main Agreement and this Agreement with effect from the date of the change (special right of termination). If the Controller does not object in due time, the change is deemed approved.

(4) Nixi AI contractually imposes on each Sub-processor the same data protection obligations as are set out in this Agreement, in particular sufficient guarantees for appropriate technical and organisational measures (Art. 28(4) sentence 1 GDPR).

(5) If a Sub-processor fails to fulfil its data protection obligations, Nixi AI is liable to the Controller for the performance of that Sub-processor's obligations (Art. 28(4) sentence 2 GDPR).

(6) Nixi AI's own services operated in Nixi AI's own Google Cloud environment, and the Controller's PVS, to which data are transferred at the Controller's initiative, are not Sub-processors within the meaning of this Agreement.

§ 7 Place of Processing and Third Countries

(1) The data are processed in data centres in the European Union (Germany, France, Sweden, Netherlands) and in Switzerland. An adequacy decision of the European Commission exists for Switzerland (Art. 45 GDPR). Which service is provided at which location is set out in Annex 3.

(2) The processing does not take place in data centres in the USA. Individual Sub-processors or their group companies have their registered office in the USA. Insofar as a transfer to a third country cannot

be ruled out in this context, appropriate safeguards under Chapter V GDPR are in place, in particular the EU-US Data Privacy Framework (Art. 45 GDPR) and EU Standard Contractual Clauses (Art. 46(2)(c) GDPR). Annex 3 states the safeguards for each provider.

(3) Processing at other locations outside the EU and the EEA takes place only if the requirements of Art. 44 et seq. GDPR are met, and only in accordance with the procedure under § 6.

§ 8 Assistance with the Rights of Data Subjects

(1) Nixi AI assists the Controller by appropriate technical and organisational measures in responding to requests from data subjects under Chapter III GDPR, for example for access, rectification, erasure or data portability. For this purpose, the Service provides functions for the export and deletion of data that the Controller can use itself. If these functions are not sufficient, Nixi AI provides assistance upon request in text form (e.g. email).

(2) If a data subject contacts Nixi AI directly, Nixi AI forwards the request to the Controller without undue delay, insofar as Nixi AI can attribute it to the Controller. Nixi AI does not respond to the request itself unless the Controller instructs it to do so.

(3) Nixi AI also assists the Controller in complying with its obligations under Art. 32 to 36 GDPR, taking into account the nature of the processing and the information available to Nixi AI.

§ 9 Personal Data Breaches

(1) Nixi AI notifies the Controller of a personal data breach affecting the Controller's data without undue delay, and at the latest within 48 hours after Nixi AI has become aware of it. The notification is made by email to the email address stored in the account.

(2) The notification contains at least the information under Art. 33(3) GDPR:

- a) a description of the nature of the breach, including where possible the categories and approximate number of data subjects and records concerned;
- b) the name and contact details of the data protection officer or other contact point where more information can be obtained;
- c) a description of the likely consequences of the breach;
- d) a description of the measures taken or proposed to address the breach and, where appropriate, to mitigate its possible adverse effects.

Where not all information is available at the same time, Nixi AI provides it in phases without undue further delay.

(3) Nixi AI takes the necessary measures without undue delay to secure the data and to mitigate possible adverse consequences. Nixi AI assists the Controller with its obligations under Art. 33 and 34 GDPR. Notification of the supervisory authority and communication to data subjects are the responsibility of the Controller.

§ 10 Data Protection Impact Assessment and Prior Consultation

Nixi AI assists the Controller with a data protection impact assessment (Art. 35 GDPR) and with any prior consultation of the supervisory authority (Art. 36 GDPR). For this purpose, Nixi AI provides the "DPIA Guidance", in which the information on Nixi AI and the Service has already been filled in, and provides further necessary information upon request.

§ 11 Requests from Authorities and Third Parties

(1) If an authority, a court or any other third party requests information from Nixi AI about the Controller's data or requests their surrender, Nixi AI informs the Controller without undue delay, insofar as this is legally permissible, and where possible refers the requesting party to the Controller. Nixi AI surrenders data only if the Controller instructs it to do so or if Nixi AI is legally obliged to do so.

(2) Nixi AI informs the Controller without undue delay of inspections and measures by a supervisory authority insofar as they relate to this processing.

§ 12 Anonymised Data

The Controller permits Nixi AI to anonymise data and to use exclusively anonymised data to improve the Service; personal data are not used for this purpose. Data are anonymised if they no longer relate to an identified or identifiable natural person (Recital 26 GDPR).

§ 13 AI Outputs Are Drafts

(1) Transcripts, AI drafts, translations, and coding and billing suggestions are generated automatically and may be incorrect or incomplete. All outputs are drafts and must be reviewed by a doctor before use. EBM billing suggestions are a beta feature.

(2) Responsibility for reviewing, correcting and using the outputs, and for the content of the medical documentation, lies with the Controller.

§ 14 Deletion and Return upon Termination of the Agreement

(1) During the term of the Agreement, data are deleted automatically in accordance with the periods specified in Annex 1.

(2) After termination of the Main Agreement, Nixi AI deletes all personal data of the Controller within 30 days, unless there is an obligation to store the data under Union or Member State law. Until then, the data still available can be exported. Backups are automatically overwritten after their retention period of 30 days, at the latest 30 days after the deletion.

(3) Upon request, Nixi AI confirms the deletion in text form (e.g. email).

(4) Data for which Nixi AI itself is the controller, for example account, contract and invoicing data, are not the subject matter of this Agreement. The "Privacy Policy for the Service" applies to them.

§ 15 Evidence and Audits

(1) Nixi AI makes available to the Controller all information necessary to demonstrate compliance with the obligations under Art. 28 GDPR. Nixi AI allows for and contributes to audits, including inspections, conducted by the Controller or by an auditor mandated by the Controller.

(2) Evidence is provided primarily by means of documentation, in particular the TOMs, by means of information, and by means of certificates and audit reports of the providers, for example on the certification of the data centres under ISO/IEC 27001 or under BSI C5.

(3) On-site audits at Nixi AI are possible with prior notice of 30 days and during normal business hours. As a rule, they take place no more than once a year, unless there is a specific reason such as a personal data breach. The costs are borne by the Controller. Nixi AI may reject auditors who are competitors of Nixi AI. Auditors must be obliged to maintain confidentiality; data of other customers and Nixi AI's trade secrets remain protected.

(4) Audits of Sub-processors are generally carried out by means of their certificates and audit reports.

(5) The powers of the supervisory authorities remain unaffected.

§ 16 Obligations of the Controller

(1) The Controller is responsible for the lawfulness of the processing. In particular, it ensures that there is a legal basis under Art. 6 and Art. 9 GDPR for the processing of the patient data.

(2) The Controller informs its patients about the use of the Service in accordance with Art. 13 GDPR.

(3) The Controller records conversations only with the consent of the patient and documents the consent; it informs other participants in the conversation before the recording and does not record if they object. For this purpose, Nixi AI provides the "Patient Consent Template".

(4) The Service is not an archive. The Controller transfers the reviewed documentation to its PVS (Annex 1 No. 3) or to another system of its own before the retention period expires. It fulfils statutory retention obligations, for example under § 630f BGB (German Civil Code), in its own systems.

(5) The Controller chooses the settings in the Service, in particular the retention period (individual period in Pro and Enterprise plans), on its own responsibility. It ensures that each User uses their own account and keeps their access credentials secret, and it observes the recommendations in Section 8 of the TOMs.

(6) If the Controller detects errors or irregularities in the processing, it informs Nixi AI without undue delay.

§ 17 Data Protection Officer

(1) Nixi AI's data protection officer is:

Proliance GmbH, Dominik Fünkner

Leopoldstr. 21, 80802 München

Email: datenschutzbeauftragter@datenschutzexperte.de

Phone: +49 89 250 039 227

(2) The Controller addresses data protection enquiries to privacy@nixiai.ai. If the Controller has appointed a data protection officer, it provides Nixi AI with that officer's contact details upon request.

§ 18 Liability

(1) For damage suffered by a person as a result of processing that does not comply with the GDPR, the parties are liable in accordance with Art. 82 GDPR; Art. 82(2) sentence 2 GDPR applies to Nixi AI's liability.

(2) In all other respects, the liability provisions of the GTC apply.

§ 19 Conclusion of the Agreement

(1) This Agreement is concluded electronically (Art. 28(9) GDPR). It is concluded when the Controller accepts it in the Service and requires no signature – neither by the Controller nor by Nixi AI.

(2) Nixi AI stores the fact that and the time when the Controller accepted this Agreement. Upon request to privacy@nixiai.ai, Nixi AI confirms the acceptance in text form (e.g. email).

(3) The currently valid version of this Agreement is available in the Service under Settings > Privacy. The Controller can download and retain it.

§ 20 Term

(1) This Agreement applies from its acceptance for the term of the Main Agreement. It ends together with the Main Agreement without the need for separate termination.

(2) Obligations which by their nature continue beyond the end of the Agreement, in particular confidentiality (§§ 3 and 4) and deletion (§ 14), continue to apply until they have been fulfilled.

(3) From the time it takes effect, this version replaces earlier versions of the data processing agreement between the parties.

§ 21 Final Provisions

(1) Annexes 1 to 3 form part of this Agreement. In the event of conflicts between this Agreement and the Main Agreement, the provisions of this Agreement take precedence in matters of data protection.

(2) Amendments and supplements to this Agreement require text form (e.g. email); an electronic format is sufficient (Art. 28(9) GDPR). The amendment procedure of the GTC applies to amendments by Nixi AI. Amendments to Annexes 2 and 3 are governed by § 5(2) and § 6.

(3) The law of the Federal Republic of Germany applies. To the extent permitted by law, the place of jurisdiction is Wiesbaden.

(4) Should any provision of this Agreement be or become invalid, the validity of the remaining provisions remains unaffected. The invalid provision is replaced by the statutory provisions, in particular Art. 28 GDPR.

Note on the Conclusion of the Agreement

This Agreement is accepted electronically and not signed (§ 19). It takes effect upon acceptance in the Service.

Annex 1 — Description of the Processing

1. Subject Matter and Purpose

Nixi AI provides the Controller with the Service for AI-assisted medical documentation. The sole purpose of the processing is to support the Controller with the documentation; the functions of the Service are listed in § 1(2). All outputs are drafts and must be reviewed by a doctor before use.

2. Nature of the Processing

Collection (recording in the browser), transmission, storage, transcription, recognition of text in uploaded documents, creation and translation of drafts using AI models, display and editing, transfer (to the PVS or by email, in each case at the User's initiative), export, anonymisation (§ 12) and deletion.

3. Data Flow

1. **Recording:** The doctor starts a session. The browser records the conversation and transmits it to Nixi AI via an encrypted connection.
2. **Transcription:** Microsoft Azure AI Speech (Germany) converts the audio data into text.
3. **Audio:** The audio data are stored temporarily in encrypted form and deleted automatically: on Nixi AI's servers (Google Cloud, Frankfurt) after 72 hours, and the encrypted backup copy in the browser after 4 hours at the latest.

4. **AI drafts:** Microsoft Azure OpenAI (Germany, France, Sweden, Switzerland) generates the AI drafts (clinical notes, patient letters, referrals, discharge reports). On request, Google Vertex AI (Netherlands) generates rewritten versions of patient letters and referral letters, translates them, translates discharge reports and is used for EBM billing suggestions (beta). The Service also generates ICD-10-GM coding suggestions. Text in uploaded documents is recognised by Microsoft Azure Document Intelligence (Germany).
5. **Medical review and transfer:** All outputs are drafts. The doctor reviews and edits them in the Service and transfers them to the PVS via a button. Optionally, the doctor can activate an automatic GDT transfer; it is deactivated by default. At the User's initiative, documents can also be sent by email (Mailgun, EU servers).
6. **Storage:** Transcripts, notes, letters and patient data are stored in Google Cloud SQL (Frankfurt). Nixi AI additionally encrypts sensitive content fields at application level (AES-256-GCM).
7. **Deletion:** Session data are deleted automatically after the retention period set by the Controller (see No. 6 of this Annex).

Nixi AI uses exclusively anonymised data to improve the Service (§ 12).

4. Categories of Data Subjects

- patients of the Controller;
- employees of the Controller and other Users of the Service;
- where applicable, third parties mentioned in the conversation or in documents, for example relatives or co-treating doctors.

5. Categories of Personal Data

Health data and other patient data (special categories of personal data under Art. 9 GDPR):

- audio recordings of the conversations;
- transcripts;
- clinical notes, patient letters, referrals, discharge reports and translations;
- diagnoses and ICD-10-GM coding suggestions and EBM billing suggestions;
- identification data mentioned in the conversation, for example name or date of birth;
- patient data entered by the doctor;
- uploaded documents and the text recognised from them.

User data:

- account data of the Users, for example name, email address and medical specialty;
- assignment of sessions and documents to the respective User account;
- security and audit logs.

§ 14(4) applies to data for which Nixi AI itself is the controller.

6. Retention Periods

Data	Deletion
Audio on Nixi AI's servers (Google Cloud, Frankfurt)	automatically after 72 hours
Encrypted backup copy of the audio in the browser	after 4 hours at the latest
Session data (transcripts, notes, letters)	automatically after the retention period of 1–90 days (default: 30 days; individual period in Pro and Enterprise plans)
Dictation backup in the browser (unencrypted local cache for dictated text)	until successfully saved, for a maximum of 7 days
Other content in the account, unless already deleted together with the session (e.g. entered patient data, uploaded documents)	at the latest upon final deletion of the User account or at the end of the Agreement (see below)
Deleted User account	final deletion after 30 days
Backups (daily, in the EU)	retention for 30 days
Security and audit logs	1 year
All data of the Controller at the end of the Agreement	deletion within 30 days; backups are overwritten at the latest 30 days after the deletion

Annex 2 — Technical and Organisational Measures (TOMs)

Separate document “Technical and Organisational Measures (TOMs)”, Version 2.0 · Last updated: 11 September 2026. The current version in each case is authoritative (§ 5(2)).

Annex 3 — List of Sub-processors

Separate document “List of Sub-processors”, Version 2.0 · Last updated: 11 September 2026, stating the service, the data processed, the place of processing and the safeguards for each provider. Changes are made in accordance with § 6.