

Privacy Policy for the Service

Nixi AI GmbH

Version 2.0 · Last updated: 11 September 2026

This is an English translation of the German „Datenschutzerklärung für den Dienst“. Only the German version is legally binding; in case of any discrepancy, the German version prevails.

This Privacy Policy informs you about how Nixi AI GmbH (hereinafter “Nixi AI”) processes your personal data when you use the application at app.nixiai.ai (hereinafter the “Service”). It is addressed to physicians and to staff of practices and clinics who use the Service. A separate privacy policy applies to visits to our website www.nixiai.ai.

Contents

1 Controller · 2 Data Protection Officer · 3 Scope and Patient Data · 4 Processing Operations in Detail · 5 Recipients · 6 Transfers to Third Countries · 7 Retention Period · 8 Cookies and Local Storage · 9 No Automated Decision-Making · 10 Your Rights · 11 Right to Lodge a Complaint · 12 Obligation to Provide Data · 13 Changes

1. Controller

Nixi AI GmbH

Adolfsallee 14, 65185 Wiesbaden

HRB 36529, Amtsgericht Wiesbaden (Local Court of Wiesbaden)

Managing Director: Mahsa Yarahmadi

Email: privacy@nixiai.ai (data protection) · hello@nixiai.ai (general)

www.nixiai.ai

2. Data Protection Officer

You can reach our external data protection officer at:

Proliance GmbH, Dominik Fünkner

Leopoldstr. 21, 80802 München

Email: datenschutzbeauftragter@datenschutzexperte.de

Phone: +49 89 250 039 227

3. Scope and Patient Data

(1) This Privacy Policy concerns the data that Nixi AI, as controller, processes about you as a User of the Service: for your user account, the contract and billing, communication with you, and the security and improvement of the Service.

(2) **Patient Data.** When you use the Service for documentation, Nixi AI processes Patient Data – e.g. audio recordings, transcripts, notes, letters and patient details – on behalf of your practice or clinic. For this data, the practice or clinic is the controller and Nixi AI is the processor pursuant to Art. 28 GDPR. The basis for this is the “Data Processing Agreement (DPA)” with the annexes “Technical and

Organisational Measures (TOMs)” and “List of Sub-processors”. This Privacy Policy does not apply to this processing.

(3) **Requests from patients.** Patients who wish, for example, to obtain information about their data or to have it erased should contact the treating practice or clinic. Nixi AI supports the practice or clinic in this regard in accordance with the DPA. If such a request reaches us directly, we refer the patient to the practice or clinic.

(4) **Anonymised data.** Nixi AI may anonymise data and use exclusively anonymised data to improve the Service. Personal data is not used for this purpose.

4. Processing Operations in Detail

We process your data on the following legal bases under the GDPR:

- **Art. 6(1)(b)** – performance of the contract and pre-contractual measures;
- **Art. 6(1)(c)** – compliance with legal obligations;
- **Art. 6(1)(f)** – legitimate interests, which we specify in each case;
- **Art. 6(1)(a)** – consent, where we obtain it in individual cases. You can withdraw consent at any time with effect for the future.

If you use the Service as a staff member of a practice or clinic that is itself Nixi AI’s contractual partner, we base the processing operations assigned below to Art. 6(1)(b) on Art. 6(1)(f) GDPR: our legitimate interest lies in performing the contract with your practice or clinic.

a) Registration and user account

- **Purpose:** setting up and managing your user account, providing the Service and evidencing that the contractual documents have been accepted.
- **Data:** name, email address, title, medical specialty, practice, language, password (only as a hash, not in plain text) and the time at which the contractual documents were accepted.
- **Registration source:** If you reach registration via a link on our website or from an advertising campaign, we store a pseudonymous identifier contained in that link in order to understand the route by which you found Nixi AI. The legal basis for this is Art. 6(1)(f) GDPR (legitimate interest in evaluating our advertising measures); you can object (Section 10).
- **Legal basis:** Art. 6(1)(b) GDPR.
- **Retention period:** until your user account is deleted. A deleted user account is permanently deleted after 30 days.

b) Login and security

- **Purpose:** secure login, protection of your account and of the Service against unauthorised access and misuse, and traceability of security-relevant and administrative operations. After 5 failed login attempts, the account is locked for 60 minutes.
- **Data:** login times, IP address at login, failed login attempts, account locks, and security and audit logs.
- **Legal basis:** Art. 6(1)(f) GDPR (legitimate interest in a secure Service) and Art. 6(1)(c) GDPR in conjunction with Art. 32 GDPR (obligation to ensure data security).
- **Retention period:** 1 year.

c) Sign-in with Google (optional)

- **Purpose:** Instead of using a password, you can register and log in with your Google account.
- **Provider:** Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland.

- **Data:** Google confirms your login to us. In doing so, we use and store your email address as confirmed by Google and the identifier of your Google account. Signing in with Google itself is subject to Google's privacy policy.
- **Legal basis:** Art. 6(1)(b) GDPR.
- **Retention period:** as for the user account (point a).

d) Usage statistics

- **Purpose:** We evaluate which features of the Service are used and how often, in order to improve the Service and operate it reliably.
- **Data:** information on which features are used and how often, in each case related to your account.
- **Legal basis:** Art. 6(1)(f) GDPR (legitimate interest in improving the Service and ensuring its stability). You can object (Section 10).
- **Retention period:** until your user account is deleted.

e) Error monitoring with Sentry

- **Purpose:** Detecting, tracing and fixing technical errors.
- **Provider:** Functional Software, Inc. (Sentry); storage in Frankfurt.
- **Data:** technical error data; personal data is filtered out in the process. For a proportion of usage sessions and in the event of errors, the sequence of actions in the Service is additionally recorded (session recording). In doing so, all text and inputs are masked and media are blocked.
- **Legal basis:** Art. 6(1)(f) GDPR (legitimate interest in an error-free and stable Service).
- **Retention period:** as long as the data is required for error analysis, for a maximum of 90 days.

f) Emails

- **Service emails:** e.g. confirmation codes, security and account notifications, and information on the contract and invoices. Legal basis: Art. 6(1)(b) GDPR.
- **Product and onboarding emails:** information on getting started with the Service, on its features and on new developments. Legal basis: Art. 6(1)(f) GDPR (legitimate interest in supporting you in using the Service and in informing you about our own similar services) in conjunction with § 7(3) UWG (German Act against Unfair Competition). **You can unsubscribe from these emails at any time**, e.g. by email to privacy@nixiai.ai; this does not incur any costs other than the transmission costs at the basic rates.
- **Data:** name, email address, language, and the content and time of sending.
- **Sending:** via Mailgun (Sinch) on servers in the EU.
- **Retention period:** your contact details for the duration of your user account (point a); emails relating to the contract or invoices, insofar as statutory retention obligations exist.

Emails with which you send documents from the Service are processed by Nixi AI as processor for your practice or clinic in accordance with the DPA (Section 3).

g) Payment processing

- **Purpose:** processing subscriptions, payments and invoices, and complying with tax and commercial law obligations.
- **Provider:** Stripe Payments Europe, Limited, 1 Grand Canal Street Lower, Grand Canal Dock, Dublin, D02 H210, Ireland.
- **Data:** name, email address, billing address, VAT identification number where applicable, plan and Billing Period, payment method, payment and invoice data. You enter card data directly with Stripe; Nixi AI does not store complete card data.

- **Legal basis:** Art. 6(1)(b) GDPR; for the retention of invoices, Art. 6(1)(c) GDPR.
- **Retention period:** invoices 10 years (§ 147 AO (German Fiscal Code), § 14b UStG (German VAT Act)); other payment data until your user account is deleted, unless there is a statutory retention obligation.

h) Customer care

- **Purpose:** support with getting started and with technical problems, handling payment and cancellation queries, and improving our offering, e.g. on the basis of reasons for cancellation.
- **System:** Nixi AI's internally developed customer care system. Nixi AI operates it in its own Google Cloud in Frankfurt. The data is not passed on to third parties; Google Cloud is involved solely as a hosting service provider.
- **Data:** name, email address, medical specialty, practice management system (PVS), country, plan, onboarding status, payment and cancellation status including reason for cancellation, extent of use (e.g. number of Sessions), technical notes on audio quality and the pseudonymous identifier for the registration source (point a).
- **Legal basis:** Art. 6(1)(f) GDPR (legitimate interest in needs-based customer care and in improving the Service).
- **Retention period:** for the duration of the customer relationship; thereafter the data is deleted unless there is a retention obligation.

i) Support requests

- **Purpose:** handling your requests to our support team.
- **Data:** contact email address, your message and the information you provide to us in it. Please do not send us any Patient Data via support.
- **Legal basis:** Art. 6(1)(b) GDPR for requests concerning your contract or account; otherwise Art. 6(1)(f) GDPR (legitimate interest in responding to your request).
- **Retention period:** as long as necessary for handling the request and for traceability, at most for the duration of the customer relationship, unless there is a statutory retention obligation.

5. Recipients

We only pass on your data insofar as this is necessary for the purposes set out in Section 4. The service providers process the data on our behalf (Art. 28 GDPR) or, insofar as they provide services under their own responsibility (e.g. payment processing, sign-in with Google), as controllers in their own right.

Recipient	Task	Location
Google Cloud EMEA Limited	Hosting, database and backups of the Service, including the customer care system	Frankfurt (Germany); backups in the EU
Microsoft Ireland Operations Limited	only within the scope of the DPA (processing of Patient Data on behalf of your practice or clinic)	Germany, France, Sweden, Switzerland
Mailgun (Sinch)	Sending of emails	Servers in the EU
Functional Software, Inc. (Sentry)	Error monitoring and session recordings	Frankfurt (Germany)
Stripe Payments Europe, Limited	Payment processing	Ireland (see Section 6)
Google Ireland Limited	Sign-in with Google (optional)	Ireland (see Section 6)

The sub-processors that process Patient Data are set out in the “List of Sub-processors”. Beyond this, we only pass on data if we are legally obliged to do so, for example to public authorities.

6. Transfers to Third Countries

(1) We store the data covered by this Privacy Policy in the EU. For Patient Data, the Service uses data centres in the EU (Germany, France, Sweden, Netherlands) and in Switzerland (adequacy decision, Art. 45 GDPR); details are governed by the DPA.

(2) Some service providers have links to the USA:

- **Mailgun and Sentry** are US companies that process the data on servers in the EU. Access from the USA nevertheless cannot be ruled out. This is safeguarded by the EU-US Data Privacy Framework (adequacy decision, Art. 45 GDPR) and by standard contractual clauses of the European Commission (Art. 46(2)(c) GDPR).
- **Stripe** may also process data in the USA. The basis for this is the EU-US Data Privacy Framework and standard contractual clauses.
- You can obtain a copy of the standard contractual clauses used in each case on request to privacy@nixiai.ai.
- **Google** processes data under its own responsibility when you sign in with Google; processing outside the EU by Google cannot be ruled out. Further details are provided in Google's privacy policy.

7. Retention Period

Data	Retention period
User account (4 a, c)	until the account is deleted; a deleted user account is permanently deleted after 30 days
Security and audit logs (4 b)	1 year
Usage statistics (4 d)	until the user account is deleted
Error data and session recordings (4 e)	as long as required for error analysis, maximum 90 days
Customer care and support (4 h, i)	for the duration of the customer relationship
Invoices (4 g)	10 years (§ 147 AO, § 14b UStG)
Backups	created daily, retained for 30 days in the EU

When the contract ends, we delete the customer data within 30 days, unless there is a statutory retention obligation. Deleted data remains in the backups for up to 30 days and is then automatically removed. Where a retention obligation exists, we use the data until it expires only for that purpose.

8. Cookies and Local Storage

(1) In the Service, we use exclusively technically necessary cookies and storage technologies. The legal basis for storing and reading them is § 25(2) no. 2 TDDDG (German Telecommunications Digital Services Data Protection Act): they are strictly necessary for us to be able to provide the Service you have requested; consent is not required for this. Insofar as personal data is processed in this context, the legal basis is Art. 6(1)(b) GDPR.

Name / type	Purpose	Duration
Cookie "nx_rt"	keeps you logged in	until logout or until the login expires
Cookie "nx_ws"	authentication of the real-time connection (e.g. for recording and transcription)	until logout or until the login expires
Local browser storage: settings	your settings, e.g. templates, language and favourites	until changed or until you clear the browser storage
Local browser storage: dictation backup	protection against data loss until a dictation has been saved successfully	until successfully saved, maximum 7 days

Name / type	Purpose	Duration
Local browser storage: encrypted audio backup	backup copy of the recording in the event of crashes or connection drops	maximum 4 hours

Both cookies are set as “httpOnly” and “Secure”: they are transmitted only over encrypted connections and cannot be read by scripts in the browser. Dictation and audio backups contain Patient Data; they are processed in accordance with the DPA.

(2) **We do not use any analytics or marketing cookies in the Service.** For the pseudonymous identifier from registration links, see Section 4 a. Error monitoring (Section 4 e) serves exclusively to fix errors; the technical device information collected for this purpose is necessary to provide the Service reliably (§ 25(2) no. 2 TDDDG).

9. No Automated Decision-Making

We do not make any decisions based solely on automated processing that produce legal effects concerning you or similarly significantly affect you (Art. 22 GDPR). The AI features of the Service generate drafts only; these are reviewed, corrected and approved by the physician.

10. Your Rights

(1) Vis-à-vis Nixi AI, you have the right of access (Art. 15 GDPR), rectification (Art. 16 GDPR), erasure (Art. 17 GDPR), restriction of processing (Art. 18 GDPR) and data portability (Art. 20 GDPR). You can withdraw any consent you have given at any time with effect for the future (Art. 7(3) GDPR).

(2) **Data export and account deletion** can be carried out directly in the Service. To protect your account, you confirm both with a code that we send you by email. For all other matters, write to privacy@nixiai.ai or to our data protection officer (Section 2).

Right to object under Art. 21 GDPR

You have the right to object at any time, on grounds relating to your particular situation, to the processing of your data that is based on Art. 6(1)(f) GDPR (e.g. usage statistics, error monitoring, customer care). We will then no longer process the data unless we can demonstrate compelling legitimate grounds that override your interests, rights and freedoms, or the processing serves the establishment, exercise or defence of legal claims.

You can object at any time, without giving reasons, to the use of your email address for product and onboarding emails. We will then no longer use it for this purpose.

You can send your objection informally to privacy@nixiai.ai.

11. Right to Lodge a Complaint

You have the right to lodge a complaint with a data protection supervisory authority (Art. 77 GDPR), in particular in the Member State of your place of residence, your place of work or the place of the alleged infringement. The authority competent for Nixi AI is:

Der Hessische Beauftragte für Datenschutz und Informationsfreiheit (HBDI) (Hessian Commissioner for Data Protection and Freedom of Information)

Gustav-Stresemann-Ring 1, 65189 Wiesbaden

12. Obligation to Provide Data

You are not legally obliged to provide us with data. However, we need the information required for registration and the login and security data (Section 4 a, b) in order to conclude the contract under the document “General Terms and Conditions (GTC)” and to provide the Service securely; for paid plans, this also applies to the payment data (Section 4 g). Without this data, you cannot use the Service or take out a subscription. Sign-in with Google is voluntary.

13. Changes

We adapt this Privacy Policy when the Service or the legal situation changes. We will inform you of material changes by email. The current version is available at www.nixiai.ai/legal and in the Service under Settings > Privacy („Einstellungen > Datenschutz“).