

Auftragsverarbeitungsvertrag (AVV)

gemäß Art. 28 DSGVO

Nixi AI GmbH

Version 2.0 · Zuletzt aktualisiert: 11. September 2026

Vertragsparteien

Verantwortlicher

Der Kunde von Nixi AI im Sinne des Dokuments „Allgemeine Geschäftsbedingungen (AGB)“

Name der Praxis bzw. Einrichtung: _____

Anschrift: _____

(nachfolgend „Verantwortlicher“)

Auftragsverarbeiter

Nixi AI GmbH

Adolfsallee 14, 65185 Wiesbaden

HRB 36529, Amtsgericht Wiesbaden

vertreten durch die Geschäftsführerin Mahsa Yarahmadi

E-Mail: hello@nixiai.ai · Datenschutz: privacy@nixiai.ai

(nachfolgend „Nixi AI“)

Präambel

Der Verantwortliche ist eine Ärztin oder ein Arzt, eine Praxis oder eine Klinik. Er nutzt die Plattform von Nixi AI (nachfolgend „Dienst“), um seine ärztliche Dokumentation zu unterstützen. Dabei verarbeitet Nixi AI in seinem Auftrag personenbezogene Daten, insbesondere Gesundheitsdaten von Patientinnen und Patienten, die der ärztlichen Schweigepflicht unterliegen.

Dieser Vertrag regelt die datenschutzrechtlichen Rechte und Pflichten der Parteien. Er ergänzt den Vertrag über die Nutzung des Dienstes, dem die AGB von Nixi AI zugrunde liegen (nachfolgend „Hauptvertrag“). „Nutzer“ sind die Personen, die den Dienst für den Verantwortlichen verwenden. „Unterauftragsverarbeiter“ sind weitere Auftragsverarbeiter im Sinne von Art. 28 Abs. 2 und 4 DSGVO. Im Übrigen haben die Begriffe die Bedeutung, die ihnen die Datenschutz-Grundverordnung (DSGVO) gibt.

Alle in diesem Vertrag genannten Dokumente sind im Dienst unter „Einstellungen > Datenschutz“ abrufbar und auf Anfrage an privacy@nixiai.ai erhältlich; AVV, Liste der Unterauftragsverarbeiter, AGB, Datenschutzerklärung und Vorlage Patienteneinwilligung außerdem unter www.nixiai.ai/legal.

§ 1 Gegenstand, Dauer, Art und Zweck der Verarbeitung

(1) Gegenstand dieses Vertrags ist die Verarbeitung personenbezogener Daten durch Nixi AI im Auftrag des Verantwortlichen bei der Erbringung des Dienstes nach dem Hauptvertrag.

(2) Zweck der Verarbeitung ist die KI-gestützte ärztliche Dokumentation. Der Dienst umfasst:

- Aufnahme und Transkription;

- KI-Entwürfe (klinische Notizen, Patientenbriefe, Überweisungen, Entlassberichte, Übersetzungen);
- ICD-10-GM-Kodiervorschläge;
- EBM-Abrechnungsvorschläge (Beta, sofern im Tarif enthalten);
- die Speicherung dieser Inhalte bis zu ihrer Löschung und ihre Übertragung in das Praxisverwaltungssystem (PVS) des Verantwortlichen, so wie der Arzt sie eingerichtet hat.

Alle Ergebnisse sind Entwürfe und vor Verwendung ärztlich zu prüfen (§ 13).

(3) Art der Verarbeitung, Datenfluss, Kategorien betroffener Personen, Datenkategorien und Speicherfristen sind in Anlage 1 beschrieben.

(4) Die Verarbeitung dauert so lange wie der Hauptvertrag. Die Pflichten zur Löschung nach § 14 bleiben unberührt.

(5) Nixi AI verarbeitet die Daten ausschließlich zu dem in Absatz 2 genannten Zweck und nicht für eigene Zwecke. § 12 (anonymisierte Daten) bleibt unberührt.

§ 2 Weisungen

(1) Nixi AI verarbeitet personenbezogene Daten nur auf dokumentierte Weisung des Verantwortlichen, auch in Bezug auf die Übermittlung in ein Drittland. Das gilt nicht, wenn Nixi AI nach dem Recht der Union oder eines Mitgliedstaats zur Verarbeitung verpflichtet ist. In diesem Fall teilt Nixi AI dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

(2) Die Weisungen des Verantwortlichen ergeben sich aus diesem Vertrag und dem Hauptvertrag. Weitere Weisungen erteilt er über die Einstellungen im Dienst (z. B. Aufbewahrungsfrist, automatische GDT-Übertragung), durch die Nutzung von Funktionen (z. B. Übertragung in das PVS, Versand per E-Mail) oder in Textform, etwa per E-Mail an privacy@nixiai.ai.

(3) Ist Nixi AI der Auffassung, dass eine Weisung gegen die DSGVO oder andere Datenschutzvorschriften verstößt, weist Nixi AI den Verantwortlichen unverzüglich darauf hin. Nixi AI darf die Ausführung der Weisung aussetzen, bis der Verantwortliche sie bestätigt oder ändert.

§ 3 Vertraulichkeit

(1) Nixi AI setzt für die Verarbeitung nur Personen ein, die zur Vertraulichkeit verpflichtet sind oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen (Art. 28 Abs. 3 lit. b DSGVO). Diese Pflicht besteht auch nach dem Ende ihrer Tätigkeit fort.

(2) Beschäftigte von Nixi AI erhalten Zugriff auf personenbezogene Daten des Verantwortlichen nur, soweit dies für die Erbringung des Dienstes erforderlich ist.

§ 4 Berufsgeheimnis (§ 203 StGB)

(1) Der Verantwortliche und die bei ihm tätigen Personen unterliegen in der Regel der Schweigepflicht nach § 203 StGB. Nixi AI wirkt an ihrer beruflichen Tätigkeit als sonstige mitwirkende Person im Sinne von § 203 Abs. 3 StGB mit. Nixi AI verschafft sich Kenntnis von fremden Geheimnissen nur, soweit dies für die Erbringung des Dienstes erforderlich ist. Nixi AI verpflichtet sich gegenüber dem Verantwortlichen zur Geheimhaltung aller ihr dabei bekannt werdenden Geheimnisse und ist darüber belehrt, dass eine unbefugte Offenbarung nach § 203 Abs. 4 StGB strafbar ist.

(2) Nixi AI hat die Beschäftigten, die bei der Erbringung des Dienstes Kenntnis von Patientendaten erlangen können, in Textform zur Verschwiegenheit verpflichtet und über die Strafbarkeit einer Verletzung dieser Pflicht belehrt (§ 203 Abs. 4 StGB). Das gilt ebenso für künftig eingesetzte Beschäftigte.

(3) Nixi AI verpflichtet Unterauftragsverarbeiter, die Kenntnis von Patientendaten erlangen können, zur Verschwiegenheit und dazu, die von ihnen eingesetzten Personen entsprechend zu verpflichten. Mit Google besteht hierzu eine Vertragsergänzung zu § 203 StGB (Google Cloud Professional Secrecy Addendum), mit Microsoft eine Zusatzvereinbarung für Berufsgeheimnisträger (Professional Secrecy Amendment). Die übrigen Unterauftragsverarbeiter sind durch ihre Auftragsverarbeitungsverträge zur Vertraulichkeit verpflichtet.

(4) Der Verantwortliche entscheidet, welche Daten er Nixi AI über den Dienst offenbart, und bleibt für die Zulässigkeit dieser Offenbarung verantwortlich. § 203 Abs. 3 StGB erlaubt die Offenbarung gegenüber mitwirkenden Personen, soweit sie für deren Inanspruchnahme erforderlich ist.

§ 5 Sicherheit der Verarbeitung

(1) Nixi AI trifft die nach Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Die Maßnahmen sind im Dokument „Technische und organisatorische Maßnahmen (TOM)“ beschrieben, das diesem Vertrag als Anlage 2 beigelegt ist.

(2) Die Maßnahmen unterliegen dem technischen Fortschritt. Nixi AI darf sie weiterentwickeln und durch gleichwertige oder bessere Maßnahmen ersetzen, sofern das Schutzniveau nicht abgesenkt wird. Wesentliche Änderungen dokumentiert Nixi AI in einer aktualisierten Fassung der TOM.

§ 6 Unterauftragsverarbeiter

(1) Der Verantwortliche genehmigt den Einsatz der Unterauftragsverarbeiter, die in der „Liste der Unterauftragsverarbeiter“ (Anlage 3) aufgeführt sind. Darüber hinaus erteilt er Nixi AI die allgemeine Genehmigung im Sinne von Art. 28 Abs. 2 DSGVO, nach dem Verfahren der Absätze 2 und 3 weitere Unterauftragsverarbeiter hinzuzuziehen oder bestehende zu ersetzen.

(2) Nixi AI kündigt jede beabsichtigte Hinzuziehung oder Ersetzung eines Unterauftragsverarbeiters mindestens 30 Tage vorher per E-Mail (Textform) an die im Konto hinterlegte E-Mail-Adresse an.

(3) Der Verantwortliche kann der Änderung aus datenschutzrechtlichen Gründen innerhalb von 14 Tagen nach Zugang der Ankündigung in Textform widersprechen, zum Beispiel per E-Mail an privacy@nixiai.ai. Die Parteien bemühen sich dann um eine einvernehmliche Lösung. Kommt keine Einigung zustande, kann der Verantwortliche den Hauptvertrag und diesen Vertrag zum Zeitpunkt der Änderung kündigen (Sonderkündigungsrecht). Widerspricht der Verantwortliche nicht fristgerecht, gilt die Änderung als genehmigt.

(4) Nixi AI erlegt jedem Unterauftragsverarbeiter vertraglich dieselben Datenschutzpflichten auf, die in diesem Vertrag festgelegt sind, insbesondere hinreichende Garantien für geeignete technische und organisatorische Maßnahmen (Art. 28 Abs. 4 Satz 1 DSGVO).

(5) Kommt ein Unterauftragsverarbeiter seinen Datenschutzpflichten nicht nach, haftet Nixi AI gegenüber dem Verantwortlichen für die Einhaltung der Pflichten dieses Unterauftragsverarbeiters (Art. 28 Abs. 4 Satz 2 DSGVO).

(6) Keine Unterauftragsverarbeiter im Sinne dieses Vertrags sind eigene Dienste von Nixi AI, die in der eigenen Google-Cloud-Umgebung von Nixi AI betrieben werden, sowie das PVS des Verantwortlichen, in das Daten auf dessen Veranlassung übertragen werden.

§ 7 Ort der Verarbeitung und Drittländer

(1) Die Daten werden in Rechenzentren in der Europäischen Union (Deutschland, Frankreich, Schweden, Niederlande) und in der Schweiz verarbeitet. Für die Schweiz besteht ein Angemessenheitsbeschluss der EU-Kommission (Art. 45 DSGVO). Welche Leistung an welchem Ort erbracht wird, ergibt sich aus Anlage 3.

(2) Die Verarbeitung erfolgt nicht in Rechenzentren in den USA. Einzelne Unterauftragsverarbeiter oder ihre Konzerngesellschaften haben ihren Sitz in den USA. Soweit dabei eine Übermittlung in ein Drittland nicht ausgeschlossen werden kann, bestehen geeignete Garantien nach Kapitel V DSGVO, insbesondere das EU-US Data Privacy Framework (Art. 45 DSGVO) und EU-Standardvertragsklauseln (Art. 46 Abs. 2 lit. c DSGVO). Die Garantien je Anbieter nennt Anlage 3.

(3) Eine Verarbeitung an anderen Orten außerhalb der EU und des EWR erfolgt nur, wenn die Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind, und nur nach dem Verfahren des § 6.

§ 8 Unterstützung bei Rechten betroffener Personen

(1) Nixi AI unterstützt den Verantwortlichen mit geeigneten technischen und organisatorischen Maßnahmen dabei, Anträge betroffener Personen nach Kapitel III DSGVO zu beantworten, etwa auf Auskunft, Berichtigung, Löschung oder Datenübertragbarkeit. Dazu stellt der Dienst Funktionen zum Export und zur Löschung von Daten bereit, die der Verantwortliche selbst nutzen kann. Reichen diese Funktionen nicht aus, unterstützt Nixi AI auf Anfrage in Textform.

(2) Wendet sich eine betroffene Person direkt an Nixi AI, leitet Nixi AI die Anfrage unverzüglich an den Verantwortlichen weiter, soweit Nixi AI sie ihm zuordnen kann. Nixi AI beantwortet die Anfrage nicht selbst, es sei denn, der Verantwortliche weist dies an.

(3) Nixi AI unterstützt den Verantwortlichen außerdem bei der Einhaltung seiner Pflichten nach Art. 32 bis 36 DSGVO, unter Berücksichtigung der Art der Verarbeitung und der Nixi AI vorliegenden Informationen.

§ 9 Datenschutzvorfälle

(1) Nixi AI meldet dem Verantwortlichen eine Verletzung des Schutzes personenbezogener Daten, die Daten des Verantwortlichen betrifft, unverzüglich, spätestens innerhalb von 48 Stunden, nachdem Nixi AI davon Kenntnis erlangt hat. Die Meldung erfolgt per E-Mail an die im Konto hinterlegte E-Mail-Adresse.

(2) Die Meldung enthält mindestens die Angaben nach Art. 33 Abs. 3 DSGVO:

- a) eine Beschreibung der Art der Verletzung, soweit möglich mit den Kategorien und der ungefähren Zahl der betroffenen Personen und Datensätze;
- b) Namen und Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen;
- c) eine Beschreibung der wahrscheinlichen Folgen der Verletzung;
- d) eine Beschreibung der ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung und gegebenenfalls zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Liegen nicht alle Angaben zugleich vor, stellt Nixi AI sie schrittweise und ohne unangemessene weitere Verzögerung zur Verfügung.

(3) Nixi AI ergreift unverzüglich die erforderlichen Maßnahmen, um die Daten zu sichern und mögliche nachteilige Folgen zu mindern. Nixi AI unterstützt den Verantwortlichen bei seinen Pflichten nach Art. 33 und 34 DSGVO. Die Meldung an die Aufsichtsbehörde und die Benachrichtigung betroffener Personen

obliegen dem Verantwortlichen.

§ 10 Datenschutz-Folgenabschätzung und vorherige Konsultation

Nixi AI unterstützt den Verantwortlichen bei einer Datenschutz-Folgenabschätzung (Art. 35 DSGVO) und bei einer etwaigen vorherigen Konsultation der Aufsichtsbehörde (Art. 36 DSGVO). Dazu stellt Nixi AI die „DSFA-Orientierungshilfe“ bereit, in der die Angaben zu Nixi AI und zum Dienst bereits ausgefüllt sind, und erteilt auf Anfrage weitere erforderliche Informationen.

§ 11 Anfragen von Behörden und Dritten

(1) Verlangt eine Behörde, ein Gericht oder ein sonstiger Dritter von Nixi AI Auskunft über Daten des Verantwortlichen oder deren Herausgabe, informiert Nixi AI den Verantwortlichen unverzüglich, soweit dies rechtlich zulässig ist, und verweist den Anfragenden nach Möglichkeit an den Verantwortlichen. Nixi AI gibt Daten nur heraus, wenn der Verantwortliche dies anweist oder Nixi AI rechtlich dazu verpflichtet ist.

(2) Nixi AI informiert den Verantwortlichen unverzüglich über Kontrollen und Maßnahmen einer Aufsichtsbehörde, soweit sie diese Verarbeitung betreffen.

§ 12 Anonymisierte Daten

Der Verantwortliche gestattet Nixi AI, Daten zu anonymisieren und ausschließlich anonymisierte Daten zur Verbesserung des Dienstes zu nutzen; personenbezogene Daten werden hierfür nicht verwendet. Anonymisiert sind Daten, die sich nicht mehr auf eine identifizierte oder identifizierbare natürliche Person beziehen (Erwägungsgrund 26 DSGVO).

§ 13 KI-Ergebnisse sind Entwürfe

(1) Transkripte, KI-Entwürfe, Übersetzungen sowie Kodier- und Abrechnungsvorschläge entstehen automatisiert und können fehlerhaft oder unvollständig sein. Alle Ergebnisse sind Entwürfe und vor Verwendung ärztlich zu prüfen. EBM-Abrechnungsvorschläge sind eine Beta-Funktion.

(2) Die Verantwortung für die Prüfung, Korrektur und Verwendung der Ergebnisse sowie für den Inhalt der ärztlichen Dokumentation liegt beim Verantwortlichen.

§ 14 Löschung und Rückgabe bei Vertragsende

(1) Während der Vertragslaufzeit werden Daten nach den in Anlage 1 genannten Fristen automatisch gelöscht.

(2) Nach Beendigung des Hauptvertrags löscht Nixi AI alle personenbezogenen Daten des Verantwortlichen innerhalb von 30 Tagen, sofern nicht nach dem Recht der Union oder eines Mitgliedstaats eine Pflicht zur Speicherung besteht. Bis dahin ist ein Export der noch vorhandenen Daten möglich. Datensicherungen werden nach ihrer Aufbewahrungsdauer von 30 Tagen automatisch überschrieben, spätestens 30 Tage nach der Löschung.

(3) Auf Anfrage bestätigt Nixi AI die Löschung in Textform.

(4) Daten, für die Nixi AI selbst Verantwortlicher ist, zum Beispiel Konto-, Vertrags- und Rechnungsdaten, sind nicht Gegenstand dieses Vertrags. Für sie gilt die „Datenschutzerklärung für den Dienst“.

§ 15 Nachweise und Kontrollen

- (1) Nixi AI stellt dem Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung der Pflichten nach Art. 28 DSGVO zur Verfügung. Nixi AI ermöglicht Überprüfungen, einschließlich Inspektionen, durch den Verantwortlichen oder einen von ihm beauftragten Prüfer und trägt dazu bei.
- (2) Nachweise erfolgen vorrangig durch Unterlagen, insbesondere die TOM, durch Auskünfte sowie durch Zertifikate und Prüfberichte der Anbieter, etwa zur Zertifizierung der Rechenzentren nach ISO/IEC 27001 oder nach BSI C5.
- (3) Vor-Ort-Kontrollen bei Nixi AI sind mit einer Vorankündigung von 30 Tagen und zu den üblichen Geschäftszeiten möglich. Sie finden grundsätzlich höchstens einmal jährlich statt, es sei denn, es besteht ein konkreter Anlass wie ein Datenschutzvorfall. Die Kosten trägt der Verantwortliche. Nixi AI kann Prüfer ablehnen, die Wettbewerber von Nixi AI sind. Prüfer sind zur Vertraulichkeit zu verpflichten; Daten anderer Kunden und Geschäftsgeheimnisse von Nixi AI bleiben geschützt.
- (4) Kontrollen bei Unterauftragsverarbeitern erfolgen in der Regel über deren Zertifikate und Prüfberichte.
- (5) Die Befugnisse der Aufsichtsbehörden bleiben unberührt.

§ 16 Pflichten des Verantwortlichen

- (1) Der Verantwortliche ist für die Rechtmäßigkeit der Verarbeitung verantwortlich. Er stellt insbesondere sicher, dass für die Verarbeitung der Patientendaten eine Rechtsgrundlage nach Art. 6 und Art. 9 DSGVO besteht.
- (2) Der Verantwortliche informiert seine Patientinnen und Patienten nach Art. 13 DSGVO über den Einsatz des Dienstes.
- (3) Der Verantwortliche nimmt Gespräche nur mit Einwilligung der Patientin oder des Patienten auf und dokumentiert die Einwilligung; weitere Gesprächsbeteiligte informiert er vor der Aufnahme und nimmt nicht auf, wenn diese widersprechen. Hierfür stellt Nixi AI die „Vorlage Patienteneinwilligung“ bereit.
- (4) Der Dienst ist kein Archiv. Der Verantwortliche überträgt die geprüfte Dokumentation vor Ablauf der Aufbewahrungsfrist in sein PVS (Anlage 1 Nr. 3) oder ein anderes eigenes System. Gesetzliche Aufbewahrungspflichten, etwa nach § 630f BGB, erfüllt er in seinen eigenen Systemen.
- (5) Der Verantwortliche wählt die Einstellungen im Dienst, insbesondere die Aufbewahrungsfrist (individuelle Frist in Pro- und Enterprise-Tarifen), in eigener Verantwortung. Er sorgt dafür, dass jeder Nutzer ein eigenes Konto verwendet und seine Zugangsdaten geheim hält, und beachtet die Empfehlungen in Abschnitt 8 der TOM.
- (6) Stellt der Verantwortliche Fehler oder Unregelmäßigkeiten bei der Verarbeitung fest, informiert er Nixi AI unverzüglich.

§ 17 Datenschutzbeauftragter

- (1) Datenschutzbeauftragter von Nixi AI ist:

Proliance GmbH, Dominik Fünkner

Leopoldstr. 21, 80802 München

E-Mail: datenschutzbeauftragter@datenschutzexperte.de

Telefon: +49 89 250 039 227

- (2) Anfragen zum Datenschutz richtet der Verantwortliche an privacy@nixiai.ai. Hat der Verantwortliche einen Datenschutzbeauftragten benannt, teilt er Nixi AI dessen Kontaktdaten auf Anfrage mit.

§ 18 Haftung

(1) Für Schäden, die einer Person wegen einer nicht der DSGVO entsprechenden Verarbeitung entstehen, haften die Parteien nach Art. 82 DSGVO; für die Haftung von Nixi AI gilt Art. 82 Abs. 2 Satz 2 DSGVO.

(2) Im Übrigen gelten die Haftungsregelungen der AGB.

§ 19 Vertragsschluss

(1) Dieser Vertrag wird elektronisch geschlossen (Art. 28 Abs. 9 DSGVO). Er kommt zustande, wenn der Verantwortliche ihn im Dienst annimmt, und bedarf keiner Unterschrift – weder des Verantwortlichen noch von Nixi AI.

(2) Nixi AI speichert, dass und wann der Verantwortliche diesen Vertrag angenommen hat. Auf Anfrage an privacy@nixiai.ai bestätigt Nixi AI die Annahme in Textform.

(3) Die jeweils gültige Fassung dieses Vertrags ist im Dienst unter „Einstellungen > Datenschutz“ abrufbar. Der Verantwortliche kann sie herunterladen und aufbewahren.

§ 20 Laufzeit

(1) Dieser Vertrag gilt ab seiner Annahme für die Laufzeit des Hauptvertrags. Er endet mit dem Hauptvertrag, ohne dass es einer gesonderten Kündigung bedarf.

(2) Pflichten, die ihrer Natur nach über das Vertragsende hinaus bestehen, insbesondere Vertraulichkeit (§§ 3 und 4) und Löschung (§ 14), gelten fort, bis sie erfüllt sind.

(3) Diese Fassung ersetzt ab ihrem Wirksamwerden frühere Fassungen des Auftragsverarbeitungsvertrags zwischen den Parteien.

§ 21 Schlussbestimmungen

(1) Die Anlagen 1 bis 3 sind Bestandteil dieses Vertrags. Bei Widersprüchen zwischen diesem Vertrag und dem Hauptvertrag gehen in Fragen des Datenschutzes die Regelungen dieses Vertrags vor.

(2) Änderungen und Ergänzungen dieses Vertrags bedürfen der Textform; ein elektronisches Format genügt (Art. 28 Abs. 9 DSGVO). Für Änderungen durch Nixi AI gilt das Änderungsverfahren der AGB. Änderungen der Anlagen 2 und 3 richten sich nach § 5 Abs. 2 und § 6.

(3) Es gilt das Recht der Bundesrepublik Deutschland. Gerichtsstand ist, soweit gesetzlich zulässig, Wiesbaden.

(4) Sollte eine Bestimmung dieses Vertrags unwirksam sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt. An die Stelle der unwirksamen Bestimmung tritt die gesetzliche Regelung, insbesondere Art. 28 DSGVO.

Hinweis zum Vertragsschluss

Dieser Vertrag wird elektronisch angenommen und nicht unterschrieben (§ 19). Er ist mit der Annahme im Dienst wirksam.

Anlage 1 — Beschreibung der Verarbeitung

1. Gegenstand und Zweck

Nixi AI stellt dem Verantwortlichen den Dienst zur KI-gestützten ärztlichen Dokumentation bereit. Zweck der Verarbeitung ist ausschließlich, den Verantwortlichen bei der Dokumentation zu unterstützen; die Funktionen des Dienstes sind in § 1 Abs. 2 aufgeführt. Alle Ergebnisse sind Entwürfe und vor Verwendung ärztlich zu prüfen.

2. Art der Verarbeitung

Erheben (Aufnahme im Browser), Übertragen, Speichern, Transkribieren, Erkennen von Text in hochgeladenen Dokumenten, Erstellen und Übersetzen von Entwürfen mithilfe von KI-Modellen, Anzeigen und Bearbeiten, Übermitteln (in das PVS oder per E-Mail, jeweils auf Veranlassung des Nutzers), Exportieren, Anonymisieren (§ 12) und Löschen.

3. Datenfluss

1. **Aufnahme:** Der Arzt startet eine Sitzung. Der Browser nimmt das Gespräch auf und überträgt es über eine verschlüsselte Verbindung an Nixi AI.
2. **Transkription:** Microsoft Azure AI Speech (Deutschland) wandelt die Audiodaten in Text um.
3. **Audio:** Die Audiodaten werden vorübergehend verschlüsselt gespeichert und automatisch gelöscht: auf Servern von Nixi AI (Google Cloud, Frankfurt) nach 72 Stunden, die verschlüsselte Sicherungskopie im Browser nach spätestens 4 Stunden.
4. **KI-Entwürfe:** Microsoft Azure OpenAI (Deutschland, Frankreich, Schweden, Schweiz) erstellt die KI-Entwürfe (klinische Notizen, Patientenbriefe, Überweisungen, Entlassberichte). Google Vertex AI (Niederlande) erstellt auf Anforderung Neufassungen von Patienten- und Überweisungsbriefen, übersetzt diese, übersetzt Entlassberichte und wird für EBM-Abrechnungsvorschläge (Beta) eingesetzt. Der Dienst erzeugt außerdem ICD-10-GM-Kodiervorschläge. Text in hochgeladenen Dokumenten erkennt Microsoft Azure Document Intelligence (Deutschland).
5. **Ärztliche Prüfung und Übertragung:** Alle Ergebnisse sind Entwürfe. Der Arzt prüft und bearbeitet sie im Dienst und überträgt sie über eine Schaltfläche in das PVS. Optional kann der Arzt eine automatische GDT-Übertragung aktivieren; sie ist standardmäßig deaktiviert. Auf Veranlassung des Nutzers können Dokumente außerdem per E-Mail versendet werden (Mailgun, EU-Server).
6. **Speicherung:** Transkripte, Notizen, Briefe und Patientendaten werden in Google Cloud SQL (Frankfurt) gespeichert. Sensible Inhaltsfelder verschlüsselt Nixi AI zusätzlich auf Anwendungsebene (AES-256-GCM).
7. **Löschung:** Sitzungsdaten werden nach der vom Verantwortlichen eingestellten Aufbewahrungsfrist automatisch gelöscht (siehe Nr. 6 dieser Anlage).

Zur Verbesserung des Dienstes nutzt Nixi AI ausschließlich anonymisierte Daten (§ 12).

4. Kategorien betroffener Personen

- Patientinnen und Patienten des Verantwortlichen;
- Beschäftigte des Verantwortlichen und sonstige Nutzer des Dienstes;
- gegebenenfalls im Gespräch oder in Dokumenten genannte Dritte, zum Beispiel Angehörige oder mitbehandelnde Ärzte.

5. Kategorien personenbezogener Daten

Gesundheitsdaten und weitere Patientendaten (besondere Kategorien personenbezogener Daten nach Art. 9 DSGVO):

- Audioaufnahmen der Gespräche;

- Transkripte;
- klinische Notizen, Patientenbriefe, Überweisungen, Entlassberichte und Übersetzungen;
- Diagnosen sowie ICD-10-GM-Kodier- und EBM-Abrechnungsvorschläge;
- im Gespräch genannte Identifikationsdaten, zum Beispiel Name oder Geburtsdatum;
- vom Arzt eingegebene Patientendaten;
- hochgeladene Dokumente und der daraus erkannte Text.

Nutzerdaten:

- Kontodaten der Nutzer, zum Beispiel Name, E-Mail-Adresse und Fachrichtung;
- Zuordnung von Sitzungen und Dokumenten zum jeweiligen Nutzerkonto;
- Sicherheits- und Audit-Protokolle.

Für Daten, für die Nixi AI selbst Verantwortlicher ist, gilt § 14 Abs. 4.

6. Speicherfristen

Daten	Löschung
Audio auf Servern von Nixi AI (Google Cloud, Frankfurt)	automatisch nach 72 Stunden
Verschlüsselte Sicherungskopie des Audios im Browser	spätestens nach 4 Stunden
Sitzungsdaten (Transkripte, Notizen, Briefe)	automatisch nach der Aufbewahrungsfrist von 1–90 Tagen (Standard: 30 Tage; individuelle Frist in Pro- und Enterprise-Tarifen)
Diktat-Sicherung im Browser (unverschlüsselter lokaler Zwischenspeicher für diktierten Text)	bis zur erfolgreichen Speicherung, höchstens 7 Tage
Sonstige Inhalte im Konto, soweit nicht bereits mit der Sitzung gelöscht (z. B. eingegebene Patientendaten, hochgeladene Dokumente)	spätestens mit der endgültigen Löschung des Nutzerkontos oder bei Vertragsende (siehe unten)
Gelöschtes Nutzerkonto	endgültige Löschung nach 30 Tagen
Datensicherungen (täglich, in der EU)	Aufbewahrung 30 Tage
Sicherheits- und Audit-Protokolle	1 Jahr
Alle Daten des Verantwortlichen bei Vertragsende	Löschung innerhalb von 30 Tagen; Datensicherungen werden spätestens 30 Tage nach der Löschung überschrieben

Anlage 2 — Technische und organisatorische Maßnahmen (TOM)

Gesondertes Dokument „Technische und organisatorische Maßnahmen (TOM)“, Version 2.0 · Zuletzt aktualisiert: 11. September 2026. Maßgeblich ist die jeweils aktuelle Fassung (§ 5 Abs. 2).

Anlage 3 — Liste der Unterauftragsverarbeiter

Gesondertes Dokument „Liste der Unterauftragsverarbeiter“, Version 2.0 · Zuletzt aktualisiert: 11. September 2026, mit Leistung, verarbeiteten Daten, Ort der Verarbeitung und Garantien je Anbieter. Änderungen erfolgen nach § 6.