Auftragsverarbeitungsvertrag (AVV)

gem. Art. 28 DSGVO

Template | Stand: April 2026 | Version 2.0

1. Vertragsparteien

Auftraggeber (Verantwortlicher): [Firmenname des Kunden], [Adresse des Kunden], vertreten durch [Name, Funktion]

- nachfolgend "Auftraggeber" -

Auftragnehmer (Auftragsverarbeiter): NOURIX GbR, [Platzhalter Adresse], vertreten durch Mussa [Nachname], Gabriel Lewalter, Joschua [Nachname]

- nachfolgend "Auftragnehmer" -

2. Gegenstand und Dauer der Verarbeitung

2.1 Gegenstand

Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers im Rahmen der Bereitstellung eines KI-gestützten Telefonassistenten. Der Assistent nimmt eingehende Anrufe entgegen, qualifiziert Leads und protokolliert Gesprächsinhalte.

2.2 Dauer

Die Verarbeitung beginnt mit Vertragsabschluss und endet mit Beendigung des Hauptvertrages über die Nutzung des NOURIX-Dienstes.

3. Art und Zweck der Verarbeitung

Die Verarbeitung umfasst:

- Entgegennahme und Verarbeitung eingehender Telefonanrufe
- Spracherkennung und Text-to-Speech-Verarbeitung
- Transkription von Gesprächsinhalten
- Lead-Qualifizierung und -Kategorisierung
- Speicherung und Bereitstellung von Anrufprotokollen im Dashboard
- Benachrichtigung des Auftraggebers per E-Mail/SMS über eingehende Leads

3a. KI-Transparenz und automatisierte Verarbeitung

3a.1 Der NOURIX-Telefonassistent ist ein KI-gestütztes System. Zu Beginn jedes Gesprächs wird der Anrufer automatisiert darauf hingewiesen, dass er mit einem digitalen Assistenten spricht und dass das Gespräch zur Bearbeitung seines Anliegens verarbeitet und protokolliert wird. Diese Transparenz-Ansage ist technisch im Produkt implementiert und kann vom Auftraggeber nicht deaktiviert werden.

3a.2 Die Lead-Qualifizierung erfolgt mittels automatisierter Verarbeitung durch ein KI-Sprachmodell (Large Language Model). Es handelt sich hierbei nicht um eine automatisierte Entscheidung im Sinne von Art. 22 DSGVO, da keine rechtliche oder vergleichbar erhebliche Wirkung für den Anrufer entsteht. Die Kategorisierung dient ausschließlich der internen Priorisierung durch den Auftraggeber. Der Auftraggeber trifft alle kundenbezogenen Entscheidungen (z.B. Rückruf, Terminvergabe, Angebotsstellung) eigenständig auf Basis der bereitgestellten Informationen.

4. Art der personenbezogenen Daten

Datenkategorie	Beispiele
Kontaktdaten	Telefonnummer des Anrufers
Gesprächsinhalte	Transkription des Gesprächs, Anliegen des Anrufers
Lead-Daten	Name, Adresse, Art des Anliegens (z.B. Heizungsreparatur)
Metadaten	Anrufzeitpunkt, Gesprächsdauer, Anrufstatus

5. Kategorien betroffener Personen

Betroffene Personen sind Anrufer, die den Telefonanschluss des Auftraggebers kontaktieren. Dies sind in der Regel Kunden, potenzielle Kunden (Leads) oder Geschäftspartner des Auftraggebers.

6. Weisungen des Auftraggebers

6.1 Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Auftraggebers (Art. 28 Abs. 3 lit. a DSGVO), es sei denn, er ist nach Unionsrecht oder dem Recht der Mitgliedstaaten zur Verarbeitung verpflichtet.

6.2 Weisungen werden vom Auftraggeber schriftlich per E-Mail an datenschutz@nourix.de erteilt. Der Auftragnehmer bestätigt den Eingang der Weisung unverzüglich und setzt diese innerhalb von 5 Werktagen um, sofern die Weisung technisch und rechtlich umsetzbar ist.

6.3 Ist der Auftragnehmer der Ansicht, dass eine Weisung gegen datenschutzrechtliche Vorschriften verstößt, informiert er den Auftraggeber unverzüglich. Der Auftragnehmer ist berechtigt, die Umsetzung der Weisung bis zur Klärung auszusetzen.

6.4 Mündliche Weisungen sind unverzüglich schriftlich per E-Mail zu bestätigen.

7. Pflichten des Auftragnehmers

7.1 Der Auftragnehmer gewährleistet, dass sich die zur Verarbeitung befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

7.2 Der Auftragnehmer ergreift alle gemäß Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen (siehe Anlage 1).

7.3 Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in Art. 32-36 DSGVO genannten Pflichten (Datensicherheit, Meldepflichten, Datenschutz-Folgenabschätzung).

7.4 Der Auftragnehmer unterstützt den Auftraggeber bei der Beantwortung von Anträgen betroffener Personen nach Kapitel III der DSGVO (Auskunft, Löschung, Berichtigung, Datenübertragbarkeit).

7a. Datenschutz-Folgenabschätzung (DSFA)

7a.1 Die Verarbeitung personenbezogener Daten durch den KI-gestützten Telefonassistenten kann ein hohes Risiko für die Rechte und Freiheiten betroffener Personen darstellen (Art. 35 DSGVO), insbesondere aufgrund der systematischen Verarbeitung von Gesprächsinhalten mittels KI.

7a.2 Der Auftragnehmer stellt dem Auftraggeber auf Anfrage alle erforderlichen Informationen zur Verfügung, die der Auftraggeber zur Durchführung einer Datenschutz-Folgenabschätzung benötigt. Dies umfasst insbesondere: Art und Umfang der Verarbeitung, eingesetzte Technologien und Sub-Processoren, implementierte Schutzmaßnahmen sowie Risikoeinschätzungen.

7a.3 Der Auftragnehmer hat eine eigene Risikobewertung der Verarbeitung durchgeführt und stellt diese dem Auftraggeber auf Anfrage zur Verfügung.

8. Unterauftragsverarbeiter (Sub-Processors)

8.1 Der Auftraggeber erteilt dem Auftragnehmer die allgemeine Genehmigung, weitere Auftragsverarbeiter (Unterauftragsverarbeiter) hinzuzuziehen. Der Auftragnehmer informiert den Auftraggeber über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder Ersetzung von Unterauftragsverarbeitern mindestens 14 Tage vor der Änderung per E-Mail.

8.2 Der Auftraggeber kann der Änderung innerhalb von 14 Tagen nach Benachrichtigung widersprechen. Bei Widerspruch steht dem Auftragnehmer ein Sonderkündigungsrecht zu.

8.3 Aktuelle Liste der Unterauftragsverarbeiter (Stand: April 2026):

Sub-Processor	Sitz	Zweck	Serverstandort	Transfergrundlage
Twilio Inc.	San Francisco, USA	Telefonie, Anrufvermittlung	USA + EU	EU-US DPF, BCRs
ElevenLabs Inc.	USA/UK/PL	Text-to-Speech (Stimme)	USA (Zero Retention)	EU-US DPF

Anthropic Inc.	San Francisco, USA	LLM-Verarbeitung	USA	EU-US DPF, SCCs
[Hosting-Anbieter]	Deutschland	Hosting, Datenbank	Deutschland	Kein Drittlandtransfer

8.4 Der Auftragnehmer stellt sicher, dass mit allen Unterauftragsverarbeitern Vereinbarungen geschlossen werden, die mindestens den gleichen Datenschutzpflichten entsprechen wie in diesem AVV festgelegt.

8.5 Der Auftragnehmer weist darauf hin, dass die in Anlage 1 genannte Maßnahme "Zero Retention Mode" bei ElevenLabs Inc. von der fortgesetzten Verfügbarkeit dieses Features durch ElevenLabs abhängt. Sollte ElevenLabs dieses Feature einschränken oder einstellen, informiert der Auftragnehmer den Auftraggeber unverzüglich und trifft geeignete Ersatzmaßnahmen (z.B. Wechsel zu einem EU-basierten TTS-Anbieter oder Aktivierung von EU Data Residency).

9. Übermittlung in Drittländer

9.1 Eine Übermittlung personenbezogener Daten in Drittländer (insbesondere USA) erfolgt ausschließlich auf Grundlage eines Angemessenheitsbeschlusses (Art. 45 DSGVO), insbesondere des EU-US Data Privacy Framework (DPF), oder auf Grundlage geeigneter Garantien gemäß Art. 46 DSGVO (Standard Contractual Clauses).

9.2 Der Auftragnehmer informiert den Auftraggeber unverzüglich, falls eine Transfergrundlage entfällt (z.B. bei Ungültigerklärung des EU-US DPF durch den EuGH) und trifft geeignete Ersatzmaßnahmen.

10. Löschfristen und Datenrückgabe

Datenart	Löschfrist	Begründung
Transkriptionen / Gesprächsinhalte	90 Tage nach Erstellung	Datenminimierung; Lead-Bearbeitung typischerweise innerhalb dieses Zeitraums
Lead-Daten (Name, Kontakt, Anliegen)	Bis Löschung durch Auftraggeber oder Vertragsende + 30 Tage	Berechtigtes Interesse des Auftraggebers an Lead-Nachverfolgung
Anrufmetadaten (Zeit, Dauer)	6 Monate	Abrechnungszwecke und Qualitätssicherung

10.1 Nach Beendigung des Hauptvertrages hat der Auftraggeber die Wahl, die Rückgabe oder die Löschung aller personenbezogenen Daten zu verlangen.

10.2 Bei Wahl der Rückgabe stellt der Auftragnehmer die Daten innerhalb von 30 Tagen nach Vertragsende in einem gängigen, maschinenlesbaren Format (CSV oder JSON) zum Download bereit.

10.3 Nach Ablauf der 30-Tage-Frist oder nach ausdrücklicher Wahl der Löschung durch den Auftraggeber löscht der Auftragnehmer alle personenbezogenen Daten unwiderruflich, sofern keine gesetzliche Aufbewahrungspflicht entgegensteht. Die Löschung wird dem Auftraggeber auf Verlangen schriftlich bestätigt.

11. Kontrollrechte des Auftraggebers

11.1 Der Auftraggeber hat das Recht, die Einhaltung der technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung und sodann regelmäßig zu überprüfen. Der Auftragnehmer stellt dem Auftraggeber alle erforderlichen Informationen zum Nachweis der Einhaltung der in Art. 28 DSGVO niedergelegten Pflichten zur Verfügung.

11.2 Inspektionen durch den Auftraggeber oder einen von ihm beauftragten Prüfer erfolgen nach angemessener Vorankündigung (mindestens 14 Werktage) während der üblichen Geschäftszeiten und ohne Störung des Betriebsablaufs.

11.3 Der Auftragnehmer kann alternativ einen aktuellen Nachweis über ein bestehendes Datenschutz- oder Sicherheitsaudit vorlegen (z.B. ISO 27001, SOC 2).

12. Meldepflicht bei Datenschutzverletzungen

12.1 Der Auftragnehmer meldet dem Auftraggeber jede Verletzung des Schutzes personenbezogener Daten unverzüglich, spätestens jedoch innerhalb von 24 Stunden nach Kenntniserlangung. Die Meldung erfolgt an:

Ansprechpartner Datenschutz: Gabriel Lewalter

E-Mail: datenschutz@nourix.de

12.2 Die Meldung enthält mindestens: Art der Verletzung, betroffene Datenkategorien und Personen, wahrscheinliche Folgen, ergriffene und vorgeschlagene Maßnahmen.

12.3 Der Auftragnehmer unterstützt den Auftraggeber bei der Erfüllung seiner Meldepflichten gegenüber der Aufsichtsbehörde (Art. 33 DSGVO, 72-Stunden-Frist) und gegenüber betroffenen Personen (Art. 34 DSGVO).

13. Haftung

13.1 Die Haftung der Parteien richtet sich nach den gesetzlichen Bestimmungen, insbesondere Art. 82 DSGVO, soweit in diesem Abschnitt nichts anderes geregelt ist.

13.2 Der Auftragnehmer haftet gegenüber dem Auftraggeber für Schäden, die durch eine nicht den Bestimmungen dieses AVV oder der DSGVO entsprechende Verarbeitung verursacht werden. Die Haftung des Auftragnehmers ist auf Fälle von Vorsatz und grober Fahrlässigkeit beschränkt, soweit gesetzlich zulässig.

13.3 Die Haftung des Auftragnehmers für Schadensersatzansprüche des Auftraggebers aus oder im Zusammenhang mit diesem AVV ist der Höhe nach begrenzt auf die Summe der vom Auftraggeber in den letzten 12 Monaten vor dem schadensauslösenden Ereignis an den Auftragnehmer gezahlten Entgelte. Diese Begrenzung gilt nicht bei Vorsatz oder grober Fahrlässigkeit.

13.4 Für Schäden, die durch Unterauftragsverarbeiter (Sub-Processors) verursacht werden, haftet der Auftragnehmer nur, sofern er seine Sorgfaltspflichten bei der Auswahl und Überwachung des Unterauftragsverarbeiters verletzt hat. Der Auftragnehmer stellt sicher, dass mit allen Unterauftragsverarbeitern angemessene vertragliche Regelungen zur Haftung bestehen.

13.5 Die Parteien stellen sich gegenseitig von Ansprüchen Dritter frei, die auf eine Verletzung der jeweiligen datenschutzrechtlichen Pflichten durch die andere Partei zurückzuführen sind, einschließlich der angemessenen Kosten der Rechtsverteidigung.

14. Schlussbestimmungen

14.1 Dieser AVV unterliegt dem Recht der Bundesrepublik Deutschland unter Ausschluss des UN-Kaufrechts.

14.2 Ausschließlicher Gerichtsstand für alle Streitigkeiten aus oder im Zusammenhang mit diesem AVV ist Berlin, Deutschland.

14.3 Änderungen und Ergänzungen dieses AVV bedürfen der Schriftform. Dies gilt auch für die Aufhebung dieser Schriftformklausel.

14.4 Sollte eine Bestimmung dieses AVV unwirksam oder undurchführbar sein oder werden, so wird die Wirksamkeit der übrigen Bestimmungen hiervon nicht berührt. Die unwirksame oder undurchführbare Bestimmung ist durch eine wirksame zu ersetzen, die dem wirtschaftlichen Zweck der unwirksamen Bestimmung am nächsten kommt.

14.5 Dieser AVV tritt mit Unterzeichnung durch beide Parteien in Kraft und ist Bestandteil des Hauptvertrages über die Nutzung des NOURIX-Dienstes.

Anlage 1: Technisch-organisatorische Maßnahmen (TOMs)

Der Auftragnehmer ergreift folgende Maßnahmen zum Schutz personenbezogener Daten:

Vertraulichkeit

- Verschlüsselung der Datenübertragung (TLS 1.2+)
- Verschlüsselung gespeicherter Daten (AES-256)
- Zugriffskontrolle: Nur autorisierte Mitarbeiter haben Zugang zu personenbezogenen Daten
- Passwortrichtlinie: Mindestens 12 Zeichen, Zwei-Faktor-Authentifizierung für alle Systemzugänge

Integrität

- Protokollierung aller Datenzugriffe und -änderungen (Audit-Log)
- Eingabekontrolle: Nachvollziehbarkeit wer wann welche Daten eingegeben oder verändert hat

Verfügbarkeit

- Regelmäßige Backups der Datenbank
- Hosting auf deutschen Servern mit garantierter Verfügbarkeit (SLA des Hosters)

Belastbarkeit

- Skalierbare Cloud-Infrastruktur zur Abfederung von Lastspitzen
- Zero Retention Mode bei ElevenLabs aktiviert (keine Speicherung von Sprachdaten beim Sub-Processor). Hinweis: Diese Maßnahme ist abhängig von der fortgesetzten Verfügbarkeit des Features durch ElevenLabs (siehe Abschnitt 8.5)

Verfahren zur regelmäßigen Überprüfung

- Vierteljährliche Überprüfung der Zugriffsberechtigungen
- Jährliche Überprüfung und Aktualisierung der TOMs

Unterschriften

Auftraggeber	**Auftragnehmer**
Ort, Datum:	Ort, Datum:
_____	_____
Name, Funktion	NOURIX GbR, vertreten durch Mussa [Nachname]