

Stand: 24.07.2026

TM TM

Gemäß Art. 28 Datenschutz-Grundverordnung (DSGVO)

TM TM

Präambel und elektronischer Vertragsschluss

TM TM

Dieser Vertrag zur Auftragsverarbeitung (nachfolgend „AVV“) bindet die CoaSoft - Consulting & Software UG (haftungsbeschränkt), Am Wäldchen 24, 66424 Homburg, Deutschland (nachfolgend „Auftragsverarbeiter“ oder „Nahlo“) und den jeweiligen gewerblichen Nutzer, Händler, die Stadt oder Kommune (nachfolgend „Verantwortlicher“ oder „Kunde“).

TM TM

Dieser AVV ergänzt die Allgemeinen Geschäftsbedingungen (AGB) bzw. den bestehenden Hauptvertrag über die Nutzung der Nahlo-Plattform.

TM TM

Schluss des Vertrages: Der Abschluss dieses Vertrages erfolgt im Rahmen des digitalen Onboardings, der Erstellung eines Dashboard-Kontos oder des Abschlusses eines Abonnements durch die ausdrückliche elektronische Zustimmung des Verantwortlichen (z. B. durch Aktivieren der entsprechenden Checkbox). Gemäß Art. 28 Abs. 9 DSGVO ist die elektronische Form der Schriftform gleichgestellt.

TM TM

§ 1 Gegenstand und Dauer der Vereinbarung

TM TM

Gegenstand: Der Auftragsverarbeiter erbringt für den Verantwortlichen die im Hauptvertrag (AGB) vereinbarten Leistungen der mandantenfähigen KI-Such- und Chat-Plattform „Nahlo“. Hierbei verarbeitet der Auftragsverarbeiter im Auftrag und nach Weisung des Verantwortlichen bestimmte personenbezogene Daten.

TM TM

Dauer: Die Laufzeit dieses AVV richtet sich nach der Laufzeit des Hauptvertrages. Er endet automatisch mit der Beendigung des Hauptvertrages, ohne dass es einer gesonderten Kündigung bedarf.

TM TM

§ 2 Art, Zweck und Gegenstand der Verarbeitung

TM TM

Die Verarbeitung der Daten erfolgt ausschließlich zum Zwecke der Bereitstellung, des Betriebs und der Verbesserung der im Hauptvertrag vereinbarten Plattform-Dienstleistungen. Dies umfasst insbesondere:

TM TM

TM TM•

- Die Speicherung und Verwaltung von Zugangs- und Kontodaten (User Management im Händler- und City-Dashboard).

TM TM•

- Die Extraktion, Strukturierung und Vektorisierung von hochgeladenen Dokumenten (z. B. PDF-, TXT-, Excel-Dateien, Produktlisten, Händlerverzeichnisse) zur Indizierung in Vektordatenbanken.

TM TM•

- Die automatisierte Analyse und Generierung von Auskünften und Antworten durch Künstliche Intelligenz (Large Language Models) auf Basis der bereitgestellten Händler- und Städtedaten.

TM TM•

- Die Protokollierung von Systemzugriffen und Telemetriedaten zur Gewährleistung der IT-Sicherheit und Fehleranalyse.

TM TM

TM TM

§ 3 Art der personenbezogenen Daten und Kreis der Betroffenen

TM TM

Art der verarbeiteten personenbezogenen Daten:

TM TM

TM TM•

- Dashboard- & Team-Daten: E-Mail-Adressen, Namen, Benutzer-IDs (UUID), Rollen- und Berechtigungsdaten von eingeladenen Mitarbeitern, Shop-Managern und City-Managern.

TM TM•

- Inhaltsdaten (Uploads): Personenbezogene Daten, die der Verantwortliche im Rahmen von Freitexten, Dokumenten oder Bulk-Importen in das System einpflegt (z. B. Ansprechpartner von Händlern, telefonische Kontaktdaten, städtische Registerdaten).

TM TM•

- System- & Protokolldaten: IP-Adressen, Zeitstempel (Timestamps), Zugriffsprotokolle und Authentifizierungstokens im Zusammenhang mit der Nutzung des Administrationsbereichs.

TM TM

TM TM

Kategorien betroffener Personen:

TM TM

TM TM•

- Mitarbeiter, Angestellte, Beauftragte und Team-Mitglieder des Verantwortlichen.

TM TM•

- Lokale Händler, Gewerbetreibende und städtische Ansprechpartner, soweit deren Daten vom Verantwortlichen in die Plattform importiert oder hochgeladen werden.

TM TM

TM TM

§ 4 Weisungsgebundenheit des Auftragsverarbeiters

TM TM

Der Auftragsverarbeiter darf Daten nur im Rahmen des Hauptvertrages und auf dokumentierte Weisung des Verantwortlichen verarbeiten, es sei denn, er ist durch das Recht der Europäischen Union oder der Bundesrepublik Deutschland hierzu verpflichtet. In einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit.

TM TM

Die Weisungen des Verantwortlichen sind grundsätzlich durch die vertraglichen Leistungen der Plattform (z. B. das Auslösen von Uploads, Lösch-Befehlen oder Datenexporten über die Benutzeroberfläche) definiert. Zusätzliche Weisungen bedürfen der Textform (z. B. E-Mail).

TM TM

Ist der Auftragsverarbeiter der Ansicht, dass eine Weisung des Verantwortlichen gegen die DSGVO oder andere Datenschutzbestimmungen verstößt, wird er den Verantwortlichen unverzüglich darauf hinweisen. Der Auftragsverarbeiter ist berechtigt, die Durchführung der betreffenden Weisung auszusetzen, bis diese durch den Verantwortlichen bestätigt oder geändert wird.

TM TM

§ 5 Pflichten des Auftragsverarbeiters

TM TM

Der Auftragsverarbeiter verpflichtet sich zur Einhaltung folgender Pflichten nach Art. 28 Abs. 3 DSGVO:

TM TM

TM TM •

- Vertraulichkeit: Alle Personen, die beim Auftragsverarbeiter Zugang zu personenbezogenen Daten haben (Mitarbeiter und Subunternehmer), sind zur Vertraulichkeit verpflichtet oder unterliegen einer angemessenen gesetzlichen Verschwiegenheitspflicht.

TM TM •

- Unterstützung bei Betroffenenrechten: Der Auftragsverarbeiter unterstützt den Verantwortlichen mit geeigneten technischen und organisatorischen Maßnahmen (insbesondere durch automatisierte Self-Service-Funktionen für Datenexport und Löschung) bei der Erfüllung von Ansprüchen betroffener Personen gemäß Art. 12 bis 23 DSGVO (z. B. Auskunft, Berichtigung, Löschung).

TM TM •

- Unterstützung bei Pflichten des Verantwortlichen: Der Auftragsverarbeiter unterstützt den Verantwortlichen unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Einhaltung der in den Art. 32 bis 36 DSGVO genannten Pflichten (Sicherheit der Verarbeitung, Meldung von Verletzungen des Schutzes personenbezogener Daten, Datenschutz-Folgenabschätzung).

TM TM •

- Meldepflicht bei Schutzverletzungen: Erlangt der Auftragsverarbeiter Kenntnis von einer Verletzung des Schutzes der im Auftrag verarbeiteten personenbezogenen Daten, informiert er den Verantwortlichen unverzüglich nach Bekanntwerden der Verletzung in Textform.

TM TM

TM TM

§ 6 Pflichten des Verantwortlichen

TM TM

Der Verantwortliche ist für die Beurteilung der Zulässigkeit der Verarbeitung gemäß Art. 6 DSGVO sowie für die Wahrung der Rechte betroffener Personen allein verantwortlich (Art. 4 Nr. 7 DSGVO).

TM TM

Der Verantwortliche garantiert, dass er für alle von ihm in die Plattform hochgeladenen personenbezogenen Daten Dritter (z. B. Mitarbeiter, Händleradressen) über eine ausreichende Rechtsgrundlage verfügt.

TM TM

Der Verantwortliche hat den Auftragsverarbeiter unverzüglich zu informieren, wenn er in den Auftragsergebnissen Fehler oder Unregelmäßigkeiten bezüglich datenschutzrechtlicher Bestimmungen feststellt.

TM TM

§ 7 Unterauftragsverhältnisse (Subunternehmer)

TM TM

Allgemeine Genehmigung: Der Verantwortliche erteilt dem Auftragsverarbeiter hiermit die allgemeine Genehmigung, weitere Auftragsverarbeiter (Subunternehmer) zur Erfüllung der vertraglichen Leistungen hinzuzuziehen.

TM TM

Vertragliche Absicherung: Der Auftragsverarbeiter stellt sicher, dass dem Subunternehmer dieselben datenschutzrechtlichen Pflichten auferlegt werden, die auch in diesem AVV festgelegt sind. Bei Datenübermittlungen in Drittländer außerhalb der EU/des EWR garantiert der Auftragsverarbeiter das Vorliegen eines angemessenen Schutzniveaus (z. B. EU-U.S. Data Privacy Framework oder EU-Standardvertragsklauseln).

TM TM

Informationsrecht und Widerspruch: Der Auftragsverarbeiter informiert den Verantwortlichen mindestens 14 Tage vorab über jede geordnete Hinzuziehung oder Ersetzung eines Subunternehmers (z. B. per E-Mail oder Benachrichtigung im Dashboard). Der Verantwortliche kann der Änderung aus einem berechtigten datenschutzrechtlichen Grund innerhalb von 14 Tagen widersprechen. Erfolgt kein Widerspruch, gilt die Änderung als genehmigt.

TM TM

Aktuelle Unterauftragnehmer: Zum Zeitpunkt des Vertragsschlusses sind folgende Subunternehmer genehmigt:

TM TM

TM TM•

Unternehmen / Dienstleister | Sitz / Datenregion | Aufgabe / Zweck | Garantie bei Drittlandtransfer

Supabase Inc. | USA / EU (Frankfurt a. M.) | Datenbank, Benutzer-Authentifizierung, Dateispeicher | EU-Standardvertragsklauseln (SCCs)

Google Cloud / Firebase (Vertragspartner: Google Ireland Ltd.) | EU (Belgien, Frankfurt a. M.) | Server-Infrastruktur (Cloud Run), KI-Sprachmodelle (Vertex AI), Systemlogs (Cloud Logging), Firestore-Datenbank für Chat-Nutzungsstatistiken | EU-U.S. Data Privacy Framework / SCCs

Amazon Web Services EMEA | Luxemburg / EU (Frankfurt a. M.) | Adressauflösung (Geocoding), Umkreissuche | EU-U.S. Data Privacy Framework

Firebase Hosting (Vertragspartner: Google Ireland Ltd.) | EU / globales CDN | Statische Auslieferung (Content Delivery) des Dashboard-Auftritts | EU-U.S. Data Privacy Framework / SCCs

Stripe Payments Europe Ltd. | Irland / EU | Zahlungsabwicklung für Händler-Abonnements (Rechnungs- und Zahlungsstatusdaten; keine Roh-Kreditkartendaten bei Nahlo) | EU-U.S. Data Privacy Framework / SCCs

Telegram Messenger Inc. | Drittland (außerhalb der EU/EWR) | Optionaler Bot-Kanal zur

Nachrichtenübermittlung des Chat-Assistenten | AV-Vertrag: in Klärung (TECH-024); ergänzend gelten die Nutzungsbedingungen von Telegram im eigenen Verhältnis zwischen Nutzer und Telegram

SMTP-/E-Mail-Anbieter | In Klärung (TECH-024) | Versand von Transaktions-E-Mails (OTP, Team-Einladungen, Datenexport-Benachrichtigung) | In Klärung (TECH-024) — Produktiv-Anbieter aktuell nicht in Terraform/Cloud Run hinterlegt

TM TM

TM TM

§ 8 Technische und organisatorische Maßnahmen (TOM)

TM TM

Der Auftragsverarbeiter hat vor Beginn der Verarbeitung geeignete technische und organisatorische Maßnahmen (Art. 32 DSGVO) zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus getroffen. Die Maßnahmen sind so gestaltet, dass die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme dauerhaft sichergestellt sind:

TM TM

TM TM•

- Verschlüsselung: Durchgängige Verschlüsselung aller Datenübertragungen nach aktuellem Stand der Technik (TLS 1.2/1.3, HTTPS). Verschlüsselung ruhender Daten auf den Speicher-Servern (Encryption at Rest).

TM TM•

- Zugriffskontrolle & Mandantentrennung: Strikte, rollenbasierte Zugriffskontrollen (Role-Based Access Control) und logische Datentrennung auf Datenbankebene (Row Level Security). Händler und Städte-Partner haben ausschließlich Zugriff auf die ihrer Instanz zugewiesenen Daten.

TM TM•

- Datensparsamkeit bei KI & Logs: Automatische Filterung kritischer Header- und Token-Inhalte aus Server-Logfiles. Hochgeladene Rohdokumente werden nach erfolgreicher Vektorisierung nicht dauerhaft zwischengespeichert. Der Anbieter der KI-Modelle (Google) nutzt Kundendaten gemäß den Enterprise-Bedingungen nicht zum Training eigener Modelle.

TM TM•

- Belastbarkeit & Schutz gegen Angriffe: Einsatz moderner Content Security Policies und automatischer API-Drosselung (Rate Limiting) zum Schutz vor Denial-of-Service-Angriffen und unbefugtem Massenabruf.

TM TM•

- Verfügbarkeit & Backups: Regelmäßige automatisierte Datensicherungen und redundante Datenhaltung in europäischen Rechenzentren zur schnellen Wiederherstellung nach physikalischen oder technischen Zwischenfällen.

TM TM

TM TM

§ 9 Kontroll- und Auditrechte des Verantwortlichen

TM TM

Der Verantwortliche hat das Recht, die Einhaltung dieses AVV und der rechtlichen Vorgaben vor Beginn der Verarbeitung und während der Laufzeit zu überprüfen oder durch einen im Einzelfall benannten, zur Verschwiegenheit verpflichteten Prüfer überprüfen zu lassen.

TM TM

Der Auftragsverarbeiter erbringt den Nachweis der Einhaltung der Pflichten primär durch die Vorlage

geeigneter Dokumentationen, aktueller Testate von unabhängigen Stellen oder Zertifizierungen der eingesetzten Cloud-Infrastrukturen (z. B. ISO 27001, SOC 2 der Subunternehmer).

TM TM

Soweit eine Überprüfung vor Ort in den Geschäftsräumen des Auftragsverarbeiters gesetzlich zwingend erforderlich ist, findet diese nach einer Vorankündigung von mindestens 14 Werktagen zu den üblichen Geschäftszeiten statt, ohne den betrieblichen Ablauf unverhältnismäßig zu stören. Die für eine solche Vor-Ort-Prüfung anfallenden Personalkosten des Auftragsverarbeiters sind vom Verantwortlichen zu angemessenen Stundensätzen zu tragen, es sei denn, die Prüfung wurde durch einen vom Auftragsverarbeiter zu vertretenden Verstoß oder Vorfall veranlasst.

TM TM

§ 10 Löschung und Rückgabe der Daten nach Vertragsende

TM TM

Nach Beendigung des Hauptvertrages ist der Auftragsverarbeiter verpflichtet, alle im Auftrag verarbeiteten personenbezogenen Daten, hochgeladenen Dokumente sowie sämtliche Kopien auf Weisung des Verantwortlichen innerhalb von maximal 30 Tagen aus den produktiven Systemen zu löschen.

TM TM

Eine Rückgabe (Export) der Daten kann der Verantwortliche bis zum Zeitpunkt der Vertragsbeendigung jederzeit eigenständig über die standardmäßigen Self-Service-Exportfunktionen (JSON-Export) des Dashboards durchführen.

TM TM

Systemseitige Sicherungskopien (Backups) und historische Telemetrie-Datensätze verbleiben aus Gründen der technischen Systemintegrität bis zum Ablauf des regulären Rotationszyklus von maximal 90 Tagen in den gesicherten Backup-Speichern, bevor sie endgültig überschrieben werden. Während dieser Zeit sind sie von jeglicher produktiven Verarbeitung oder KI-Indizierung isoliert.

TM TM

Dokumentationen, die dem Nachweis der ordnungsgemäßen Datenverarbeitung dienen (z. B. Protokolle über erfolgte Zustimmungen oder Logfiles), werden vom Auftragsverarbeiter nach den jeweiligen gesetzlichen Aufbewahrungsfristen verwahrt und anschließend gelöscht.

TM TM

§ 11 Schlussbestimmungen

TM TM

Es gilt das Recht der Bundesrepublik Deutschland. Gerichtsstand für alle Streitigkeiten aus oder im Zusammenhang mit diesem Vertrag ist der Sitz des Auftragsverarbeiters (Homburg), sofern der Verantwortliche Kaufmann, eine juristische Person des öffentlichen Rechts oder ein öffentlich-rechtliches Sondervermögen ist.

TM TM

Sollten einzelne Bestimmungen dieses AVV ganz oder teilweise unwirksam sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen hiervon unberührt. Die Parteien verpflichten sich, die unwirksame Bestimmung durch eine rechtlich zulässige Bestimmung zu ersetzen, die dem wirtschaftlichen und datenschutzrechtlichen Zweck der ursprünglichen Bestimmung am nächsten kommt.