

Vereinbarung zur Auftragsverarbeitung gemäß Art. 28 DSGVO

MOKATI Fotos und Film OHG · Marke AINOVORA · Stand: 09.10.2026

zwischen

dem Auftraggeber, wie im zugrundeliegenden Hauptvertrag mit dem Auftragnehmer bezeichnet, nachfolgend „Auftraggeber“

und

MOKATI Fotos und Film OHG
Ottostr. 2, 85551 Kirchheim bei München, Deutschland
nachfolgend „Auftragnehmer“

1. Gegenstand und Dauer

1.1 Gegenstand dieser Vereinbarung ist die Verarbeitung personenbezogener Daten durch den Auftragnehmer im Auftrag des Auftraggebers im Zusammenhang mit den vereinbarten Leistungen.

1.2 Die Vereinbarung gilt insbesondere für folgende Leistungen, soweit diese beauftragt sind:

- Visibility OS
- Hosting und Betrieb von Websites oder Landingpages
- Formular- und Anfrageverarbeitung
- CRM- und Kontaktverwaltung
- Tracking und Monitoring
- Google-/Instagram-Integrationen
- Content- und KI-gestützte Assistenzfunktionen
- Kundenportal „Dein Projekt“ (Projektfragebogen, Sprachaufnahmen, Uploads von Projektmaterial)
- Fotopaket (Sichtung und Bearbeitung von Rohfotos), nur soweit dieses Modul gebucht und aktiv ist
- technische Wartung und Support

1.3 Die Dauer richtet sich nach dem zugrundeliegenden Vertrag. Diese Vereinbarung endet grundsätzlich mit Beendigung des Hauptvertrags, sofern keine gesetzlichen Aufbewahrungspflichten oder Nachlaufpflichten bestehen.

2. Art und Zweck der Verarbeitung

2.1 Zweck der Verarbeitung ist die Erbringung der vertraglich vereinbarten Leistungen für den Auftraggeber.

2.2 Dazu gehören insbesondere:

- Bereitstellung und Betrieb von Visibility OS
- Verwaltung von Workspaces
- Speicherung und Bearbeitung von Anfragen

- CRM-Unterstützung
- Website- und Formularbetrieb
- technische Analyse und Monitoring
- Content-Planung
- Sichtbarkeitsanalyse
- Integration von Google- und Instagram-Diensten
- KI-gestützte Erstellung von Vorschlägen, Entwürfen und Zusammenfassungen über eine kontrollierte interne Schnittstelle (Assembler) mit vorgeschalteter Datenminimierung
- Entgegennahme von Projektangaben über das Kundenportal, einschließlich Abschrift von Sprachaufnahmen und Übernahme der Antworten in das Unternehmenswissen (Company Brain) und die Markenstimme des Auftraggebers
- Dokumentation der für den Auftraggeber erbrachten Tätigkeiten, Zeiten und Änderungen sowie Monatsberichte für Betreuungspakete
- Support, Fehleranalyse und Sicherheit

3. Datenarten

Je nach Nutzung können folgende Datenarten verarbeitet werden:

- Stammdaten
- Kontaktdaten
- Kommunikationsdaten
- Anfrage- und Lead-Daten
- CRM-Daten
- Vertrags- und Projektdaten
- Website-Nutzungsdaten
- technische Logdaten
- Tracking- und Eventdaten
- Content- und Redaktionsdaten
- Google Search Console Daten
- Google Business Profile Daten
- Instagram-Profil- und Mediendaten
- OAuth-Verbindungsdaten
- Rollen- und Berechtigungsdaten
- Notizen und interne Bearbeitungsstände
- Gesprächsnotizen, Umsatzangaben je Anfrage oder Kunde, Kundenstimmen
- KI-generierte Vorschläge und Zusammenfassungen
- Antworten im Projektfragebogen, Sprachaufnahmen und deren Transkripte
- hochgeladenes Projektmaterial (z. B. PDF, Logos, Bilder, Schriften, Videos)
- Rohfotos (nur bei gebuchtem Fotopaket)
- Protokolldaten (Zugriffe, Änderungen, Tätigkeiten)

4. Kategorien betroffener Personen

Betroffen sein können Mitarbeiter des Auftraggebers, Nutzer des Workspaces, Kunden und Interessenten des Auftraggebers, Websitebesucher, Anfragende über Formulare, Geschäftspartner, Eventteilnehmer sowie sonstige Personen, deren Daten der Auftraggeber in das System einbringt.

5. Weisungsgebundenheit

5.1 Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Auftraggebers, auch hinsichtlich der Übermittlung in Drittländer, sofern keine gesetzliche Pflicht entgegensteht.

5.2 Die Weisungen ergeben sich aus dem Hauptvertrag, dieser Vereinbarung und den vom Auftraggeber im System vorgenommenen Einstellungen.

5.3 Einzelweisungen können in Textform erteilt werden.

5.4 Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn eine Weisung nach seiner Auffassung gegen Datenschutzrecht verstößt.

6. Vertraulichkeit

6.1 Der Auftragnehmer verpflichtet alle mit der Verarbeitung betrauten Personen zur Vertraulichkeit, soweit sie nicht bereits gesetzlich zur Vertraulichkeit verpflichtet sind.

6.2 Zugriff auf personenbezogene Daten erhalten nur Personen, die diesen Zugriff zur Leistungserbringung benötigen.

6.3 Personen des Auftragnehmers mit Betreiberrechten (Plattform-Administration) sehen personenbezogene Daten der Kunden und Interessenten des Auftraggebers nur geschwärzt. Das betrifft insbesondere Anfragen, Kundenliste, Gesprächsnotizen, Umsätze je Anfrage oder Kunde, Kundenstimmen, Anfrage-Auswertungen und Protokolle. Die Schwärzung wird in der Datenbank durch Zeilensicherheit (Row Level Security) durchgesetzt und nicht nur in der Oberfläche. Ausgenommen sind Testanfragen, die von E-Mail-Adressen des Auftragnehmers stammen.

6.4 Benötigt der Auftragnehmer für Support oder Fehleranalyse Einsicht in Klardaten, kann ein Owner oder Admin des Auftraggebers eine Service-PIN erzeugen und dem Auftragnehmer mitteilen. Die Freigabe gilt höchstens 24 Stunden und kann vom Auftraggeber jederzeit beendet werden. Die PIN wird nur als Hashwert gespeichert. Jede Einlösung wird in einem für den Auftraggeber sichtbaren Protokoll erfasst. Der Auftragnehmer kann sich selbst keine PIN ausstellen. Die Erzeugung einer Service-PIN gilt als Einzelweisung im Sinne von Ziffer 5.3.

6.5 Ändert der Auftragnehmer das Team des Auftraggebers im System (Mitglied hinzufügen, einladen, Rolle ändern oder entfernen), erhalten die Owner des Auftraggebers sofort eine E-Mail. Die Änderung wird zusätzlich im Protokoll vermerkt.

6.6 Angaben, die der Auftraggeber über sein eigenes Unternehmen einträgt (Unternehmensprofil, Medien, Antworten im Projektfragebogen, Projektmaterial), sieht der Auftragnehmer, soweit dies zur Leistungserbringung erforderlich ist. Rohfotos des Auftraggebers sieht der Auftragnehmer nur, wenn das Modul „Fotopaket“ gebucht und aktiv ist.

6.7 Ist der Auftraggeber Berufsgeheimnisträger, insbesondere Rechtsanwalt, Steuerberater oder vergleichbar nach § 203 StGB, § 43e BRAO oder § 62a StBerG zur Verschwiegenheit verpflichtet, gilt ergänzend: Der Auftragnehmer verpflichtet alle Personen, die an der Leistung mitwirken, schriftlich zur Verschwiegenheit und belehrt sie über die strafrechtlichen Folgen einer Pflichtverletzung. Der Auftragnehmer verschafft sich und diesen Personen nur insoweit Kenntnis von fremden Geheimnissen, wie dies zur Leistungserbringung erforderlich ist; technisch ist dies durch Ziffer 6.3 und 6.4 umgesetzt. Der Auftragnehmer ist sich bewusst, dass er sich nach § 203 Abs. 4 StGB strafbar machen kann. Die Verpflichtung erfolgt mindestens in Textform. Der Auftragnehmer setzt Unterauftragsverarbeiter nur nach Ziffer 8 ein und verpflichtet sie in Textform entsprechend dieser Ziffer, einschließlich Belehrung über die

strafrechtlichen Folgen. Für Leistungen im Ausland gilt ergänzend Ziffer 9; der Auftraggeber prüft, ob der Geheimnisschutz dort vergleichbar ist. Ob Inhalte von Mandanten an KI-Anbieter außerhalb der EU gehen, entscheidet der Auftraggeber selbst über Ziffer 6.8; holt er dafür eine Einwilligung seiner Mandanten ein (§ 43e Abs. 5 BRAO, § 62a Abs. 5 StBerG), liegt dies in seiner Verantwortung.

6.8 Ob KI-Funktionen Inhalte von Endkunden des Auftraggebers verarbeiten (Anfragen, Kunden, Gesprächsnotizen, Kundenstimmen) und ob KI Google-Bewertungen des Auftraggebers verarbeitet, legt der Auftraggeber über zwei Schalter im System fest („KI bei Personendaten“, „KI bei Bewertungen“). Diese Einstellung ist eine Weisung im Sinne von Ziffer 5.2 und wird mit Zeitpunkt protokolliert. Bei neuen Workspaces sind beide Schalter bis zur Entscheidung des Auftraggebers ausgeschaltet; der Auftragnehmer kann eine Empfehlung vorbelegen, die erst durch Bestätigung des Auftraggebers wirksam wird. Die Sperre ist serverseitig umgesetzt. Auch bei eingeschaltetem Schalter werden Namen und Kontaktdaten vor der Übermittlung entfernt, soweit technisch möglich (nicht bei Sprachaufnahmen und Bildern), und es werden nur Modellanbieter ohne Datenspeicherung genutzt. Berufsgeheimnisträgern empfiehlt der Auftragnehmer, die Schalter ausgeschaltet zu lassen, solange keine Einwilligung der Mandanten vorliegt.

7. Technische und organisatorische Maßnahmen

7.1 Der Auftragnehmer trifft geeignete technische und organisatorische Maßnahmen nach Art. 32 DSGVO.

7.2 Die Maßnahmen sind in der beigefügten TOM-Anlage beschrieben.

7.3 Der Auftragnehmer kann Maßnahmen an technische Entwicklungen anpassen, sofern das Schutzniveau nicht wesentlich unterschritten wird.

8. Unterauftragsverarbeiter

8.1 Der Auftraggeber genehmigt den Einsatz der in der beigefügten Subunternehmerliste genannten Unterauftragsverarbeiter.

8.2 Der Auftragnehmer informiert den Auftraggeber über wesentliche Änderungen bei Unterauftragsverarbeitern, insbesondere über die Aufnahme oder den Austausch eines Unterauftragsverarbeiters, mit einem Vorlauf von mindestens 14 Tagen.

8.3 Der Auftraggeber kann aus wichtigem datenschutzrechtlichem Grund widersprechen.

8.4 Unterauftragsverarbeitern werden dieselben Datenschutzpflichten auferlegt wie in dieser Vereinbarung (Art. 28 Abs. 4 DSGVO).

9. Drittlandübermittlungen

9.1 Die zentrale Datenhaltung erfolgt in Rechenzentren innerhalb der Europäischen Union:

- Supabase-Backend (Datenbank, CRM, Anfragen): AWS Frankfurt (eu-central-1)
- E-Mail-Versand: All-Inkl/KasServer (Deutschland)

9.2 Das Frontend (Cloudflare Pages) verarbeitet Anfragen im globalen Cloudflare-Netzwerk, das außerhalb der EU liegen kann. Cloudflare ist zertifiziert nach dem EU Cloud Code of Conduct und hat Standardvertragsklauseln (SCCs) im Data Processing Addendum abgeschlossen.

9.3 Soweit einzelne Unterauftragsverarbeiter, insbesondere im Bereich KI-Verarbeitung (OpenRouter als Vermittler, Google Gemini, Anthropic Claude), Daten außerhalb der EU/des EWR verarbeiten, stellt der Auftragnehmer sicher, dass geeignete Garantien nach Art. 46 DSGVO vorliegen, bevor eine solche Übermittlung stattfindet. Dazu gehören insbesondere Angemessenheitsbeschlüsse, EU-Standardvertragsklauseln oder eine Zertifizierung nach dem EU-U.S. Data Privacy Framework.

10. Unterstützungspflichten

10.1 Der Auftragnehmer unterstützt den Auftraggeber im angemessenen Umfang bei Betroffenenanfragen, Löschung, Berichtigung oder Auskunft, Datenschutz-Folgenabschätzungen, Meldung von Datenschutzverletzungen sowie Nachweisen gegenüber Aufsichtsbehörden.

10.2 Für Auskunft und Löschung stellt der Auftragnehmer im System ein Werkzeug bereit. Owner und Admins des Auftraggebers können damit zu einer E-Mail-Adresse alle zugehörigen Daten als Export (JSON) abrufen oder löschen, einschließlich verknüpfter Daten in Nebentabellen. Der Vorgang wird protokolliert; das Protokoll enthält die E-Mail-Adresse nur als Hashwert. Der Auftragnehmer kann dieses Werkzeug ohne Service-PIN (Ziffer 6.4) nicht nutzen.

11. Datenschutzverletzungen

11.1 Der Auftragnehmer informiert den Auftraggeber unverzüglich, spätestens jedoch innerhalb von 48 Stunden nach Kenntniserlangung, wenn ihm eine Verletzung des Schutzes personenbezogener Daten bekannt wird, die Daten des Auftraggebers betrifft.

11.2 Die Information enthält, soweit verfügbar, Art und Umfang des Vorfalls, betroffene Daten, mögliche Folgen und ergriffene Maßnahmen.

12. Nachweise und Kontrollen

12.1 Der Auftragnehmer stellt dem Auftraggeber auf Anfrage angemessene Nachweise zur Einhaltung dieser Vereinbarung zur Verfügung.

12.2 Vor-Ort-Kontrollen sind nach vorheriger Abstimmung möglich, wenn berechtigte Gründe bestehen und Betriebs- und Sicherheitsinteressen angemessen berücksichtigt werden.

12.3 Tätigkeiten, Zeiten und Änderungen, die der Auftragnehmer für den Auftraggeber vornimmt, werden in einem unveränderbaren Protokoll mit Serverzeit dokumentiert. Dazu gehören Benachrichtigungen über neue Fragen und Antworten im Kundenportal sowie die automatische Erfassung, wann der Auftragnehmer auf eine Rückmeldung wartet und wann sie eingeht. Für Betreuungspakete erhält der Auftraggeber einen Monatsbericht. Das Protokoll dient auch als Nachweis im Sinne von Ziffer 12.1.

13. Löschung und Rückgabe

13.1 Nach Ende des Hauptvertrags löscht oder gibt der Auftragnehmer personenbezogene Daten innerhalb von 30 Tagen nach Weisung des Auftraggebers zurück, soweit keine gesetzlichen Aufbewahrungspflichten entgegenstehen.

13.2 Backups können aus technischen Gründen verzögert gelöscht werden und werden bis zur Löschung nicht mehr aktiv verarbeitet. Backups werden beim Unterauftragsverarbeiter Supabase in der EU (Frankfurt) gespeichert und nach 7 Tagen (tägliche Sicherung, keine Wiederherstellung auf beliebige Zeitpunkte; geprüft am 09.10.2026) automatisch überschrieben.

13.3 Der Export erfolgt in offenen, weiterverwendbaren Formaten (Markdown und JSON) ohne Anbieterbindung.

14. Berichtigung, Einschränkung und Löschung im laufenden Betrieb

14.1 Der Auftragnehmer setzt Weisungen zur Berichtigung, Sperrung, Einschränkung oder Löschung im Rahmen der technischen Möglichkeiten und vertraglichen Vereinbarungen um.

14.2 Die Löschfrist für Anfragen legt der Auftraggeber als Verantwortlicher im System fest; diese Einstellung ist eine Weisung im Sinne von Ziffer 5.2. Voreingestellt ist „keine automatische Löschung“. Der Auftragnehmer empfiehlt 12 Monate; die Frist ist zwischen 1 und 120 Monaten wählbar. Der Auftraggeber wählt zwischen zwei Verfahren; voreingestellt ist Anonymisieren:

- **Anonymisieren (Statistik bleibt):** Name, Kontaktdaten, Nachricht, Notizen, Verlauf, Status-Verlauf, KI-Entwürfe, Erinnerungen, geschätzte Werte, Freitext-Angaben zur Quelle sowie Besuchererkennung werden entfernt. Erhalten bleiben nur Monat des Eingangs, Status, Quellkategorie, Formular, Seite in grober Form, Kategorien (z. B. Event-Art), Zahlen und Beträge als Spannen und Termine als Quartal. Exakte Zeitpunkte werden auf den Monat vergrößert, damit sich eine Anfrage auch mit Zusatzwissen (z. B. der Benachrichtigungsmail im Postfach) keiner Person mehr zuordnen lässt.
- **Vollständig löschen:** Die Anfrage wird mit allen zugehörigen Daten gelöscht.

14.3 Gebuchte Anfragen sind von der automatischen Löschung ausgenommen.

14.4 Am Ersten jedes Monats erhalten Owner und Admins des Auftraggebers eine Sammelmail mit den Anfragen, die am Ersten des Folgemonats gelöscht oder anonymisiert werden. Einzelne Anfragen können behalten werden. Jede Entscheidung des Auftraggebers zur Löschfrist und zu einzelnen Anfragen wird mit Zeitpunkt gespeichert.

15. Verantwortlichkeit des Auftraggebers

15.1 Der Auftraggeber bleibt Verantwortlicher für die Rechtmäßigkeit der Verarbeitung, die Rechtsgrundlagen, Informationspflichten und die Rechte betroffener Personen.

15.2 Der Auftraggeber ist verantwortlich für die Rechtmäßigkeit der von ihm eingegebenen oder verbundenen Daten.

16. Schlussbestimmungen

16.1 Im Fall von Widersprüchen geht diese AVV datenschutzrechtlichen Regelungen im Hauptvertrag vor.

16.2 Änderungen bedürfen der Textform.

16.3 Sollte eine Bestimmung unwirksam sein, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt.

Anlagen

- Anlage 1: Technische und organisatorische Maßnahmen (TOM)
- Anlage 2: Subunternehmerliste

Technische und organisatorische Maßnahmen (TOM) – Anlage

Stand 09.10.2026 · **Entwurf, anwaltlich/technisch prüfen** · Anlage zum AVV · noch nicht prominent verlinken (§10).

Vertraulichkeit

- Zugriffskontrolle: rollenbasierte Rechte (Owner/Admin/Member, Platform-Admin), serverseitige Durchsetzung (Row Level Security, SECURITY-DEFINER-RPCs).
- OAuth-Tokens werden **nur serverseitig** gespeichert, nie an das Frontend ausgegeben und nicht in Logs geschrieben.
- Mandantentrennung pro Workspace (tenant-scoped).
- **Geschwärzter Betreiberzugriff:** Platform-Admins sehen personenbezogene Daten der Endkunden eines Workspaces (Anfragen, Kundenliste, Gesprächsnotizen, Umsätze je Anfrage/Kunde, Kundenstimmen, Anfrage-Auswertungen, Protokolle) nur geschwärzt. Die Sperre sitzt in der Datenbank (Row Level Security), nicht nur in der Oberfläche. Ausnahme: Testanfragen von AINOVORA-eigenen E-Mail-Adressen.
- **Service-PIN:** Klardaten nur, wenn ein Owner oder Admin des Kunden eine PIN erzeugt und AINOVORA mitteilt. Gültig höchstens 24 Stunden, jederzeit vom Kunden beendbar, PIN nur als Hashwert gespeichert, jede Einlösung im für den Kunden sichtbaren Protokoll. Ein Platform-Admin kann sich keine PIN selbst ausstellen.
- **Team-Änderungen durch AINOVORA** (Mitglied hinzufügen, einladen, Rolle ändern, entfernen) lösen sofort eine E-Mail an die Owner des Workspaces aus und werden protokolliert.
- Unternehmensangaben des Kunden (Unternehmensprofil, Medien, Antworten im Projektfragebogen, Projektmaterial) sind für AINOVORA zur Leistungserbringung sichtbar. Rohfotos nur bei gebuchtem und aktivem Modul „Fotopaket“.
- **Berufsgeheimnisträger:** Alle an der Leistung mitwirkenden Personen sind schriftlich zur Verschwiegenheit verpflichtet und über die Folgen nach § 203 StGB belehrt. Zugriff nur soweit erforderlich (technisch über Schwärzung und Service-PIN).
- **Kundenportal-Uploads** (PDF, Logo, Bilder, Schriften, Videos bis 25 MB) liegen in einem privaten Speicher. Abruf nur über kurzlebige signierte Links. Nach Projektabschluss wird das Portal eingefroren.
- **Öffentliche Mediendateien:** Medien für Website und Beiträge liegen in einem Speicher, dessen Einzeldateien über nicht erratbare Links öffentlich abrufbar sind (für Website und Social Media erforderlich). Das Auflisten fremder Dateien ist gesperrt.

Integrität

- Versionierte Migrationen; Änderungen über GitHub nachvollziehbar.
- Eingabevalidierung; SSRF-Schutz bei URL-Verarbeitung (Potential-Scan).
- **Projekt-Protokoll:** Tätigkeiten, Zeiten und Änderungen für den Kunden werden in einem unveränderbaren Protokoll mit Serverzeit dokumentiert; Monatsbericht für Betreuungspakete.
- Entscheidungen des Kunden zur Löschfrist und zu einzelnen Anfragen werden mit Zeitpunkt gespeichert.

Verfügbarkeit und Belastbarkeit

- Managed Backend (Supabase, EU/Frankfurt) mit Backups. Aufbewahrung: 7 Tage (tägliche Sicherung, geprüft am 09.10.2026).
- Uptime-Monitoring; Fehler-/Betriebslogs mit sparsamer Aufbewahrung.

Datenschutzfreundliche Voreinstellungen

- Datensparsames Tracking (kein cookiebasiertes Nutzer-Tracking im Standard).
- KI-Prompts PII-reduziert (Namen, Kontaktdaten, Anschriften werden vor dem Versand ersetzt, zusätzlich zentrale Prüfung); keine Speicherung vollständiger Prompts; Modellanbieter nur mit Zero Data Retention.
- Schalter je Workspace „KI bei Personendaten“ und „KI bei Bewertungen“: Entscheidung des Kunden, serverseitig in allen betroffenen Funktionen durchgesetzt, bei neuen Workspaces bis zur Entscheidung aus.
- Sprachaufnahmen im Kundenportal werden nur zur Abschrift an den KI-Anbieter laut Subunternehmerliste übertragen.

Auftragskontrolle / Sub-Auftragsverarbeiter

- Einsatz nur gemäß Subunternehmerliste; Drittlandtransfers mit geeigneten Garantien.

Löschung

- Löschkonzept mit Fristen (siehe Datenschutzerklärung, Abschnitt Speicherdauer).
- **Löschfrist für Anfragen** legt der Kunde fest (Standard: keine automatische Löschung; Empfehlung 12 Monate; frei wählbar in Monaten). Modus „anonymisieren (Statistik bleibt)“ oder „vollständig löschen“; gebuchte Anfragen ausgenommen. Vorankündigung per Sammelmail am Monatsersten an Owner/Admins, einzelne Anfragen können behalten werden. Details: AVV Ziffer 14.
- **Betroffenenrechte-Werkzeug**: Auskunft (Export JSON) und Löschung je E-Mail-Adresse, einschließlich Nebentabellen; Protokoll nur mit Hashwert der Adresse. Nutzbar nur für Owner/Admins des Kunden, nicht für AINOVORA ohne Service-PIN.

Subunternehmer / Auftragsverarbeiter (Anlage zum AVV)

Stand: 09.10.2026 · Version 1.1

Abrufbar unter: <https://www.ainovora.de/datenschutz/subunternehmer>

Dienstleister	Zweck	Sitz / Datentransfer
Supabase Inc.	Backend / Datenbank / Auth / Storage	EU / Frankfurt (eu-central-1) — kein Drittlandtransfer
Cloudflare Inc.	Hosting / CDN / Sicherheit	USA — Übermittlung auf Basis EU-SCC / DPF
GitHub Inc. (Microsoft)	Code-Versionierung / Betrieb	USA — Übermittlung auf Basis EU-SCC / DPF
OpenRouter, Inc.	Vermittlung von KI-Anfragen an freigegebene Modellanbieter (u. a. Texte, Abschrift von Sprachaufnahmen); nur Anbieter ohne Datenspeicherung (Zero Data Retention, data_collection: deny); personenbezogene Daten werden vor dem Versand entfernt, soweit technisch möglich (Ausnahme: Audio); Auftragsverarbeitungsvertrag: OpenRouter-DPA, durch Annahme der Nutzungsbedingungen (Abschnitt 10.2) für geschäftliche Nutzung wirksam, Stand 26.08.2026 (openrouter.ai/data-processing-agreement); Löschung von Ein- und Ausgaben direkt nach Verarbeitung, Meldung von Datenschutzverletzungen binnen 72 Stunden	USA — keine DPF-Zertifizierung bekannt; Übermittlung auf Basis der im DPA enthaltenen EU-SCC (Modul 2, irisches Recht)
Google LLC	KI (Gemini, Ersatzweg bei Ausfall von OpenRouter, auch für Abschriften); GSC / GBP bei verbundenem Konto	USA — Übermittlung auf Basis EU-SCC / DPF
Anthropic PBC	KI-Funktionen (Claude), überwiegend über OpenRouter	USA — nicht DPF-zertifiziert (Stand 09.10.2026); Übermittlung auf Basis EU-SCC (Module 2/3) laut Anthropic-DPA
Meta Platforms Ireland Ltd.	Social-Verbindung Instagram (nur bei aktiviertem Konto)	Irland / USA — Übermittlung auf Basis EU-SCC
Firecrawl (Mendable Inc.)	Web-Crawling für Inhaltsanalyse	USA — Übermittlung auf Basis EU-SCC
All-Inkl.com / Neue Medien Münnich	E-Mail-Versand (SMTP: kasserver.com Port 465 TLS, Absender noreply@ainovora.de)	Deutschland — kein Drittlandtransfer
Steuerberatungskanzlei	Buchführung / Rechnungswesen	Deutschland — kein Drittlandtransfer

Ausdrücklich NICHT enthalten

- **OpenAI / ChatGPT** — keine Verarbeitung von Kundendaten. ChatGPT Business wird nur intern (ohne Kundendaten) genutzt und ist kein Bestandteil von Visibility OS.
- **Netlify** — nicht im Einsatz.
- **Lovable Cloud** — nicht im Einsatz.

Änderungen

Änderungen an dieser Liste werden den betroffenen Auftraggebern gemäß AVV Ziffer 8.2 mit mindestens 14 Tagen Vorlauf mitgeteilt.