Vereinbarung über die Auftragsverarbeitung

gemäß Art. 28 Datenschutz-Grundverordnung (DSGVO) · Muster / Stand 22. Juli 2026

zwischen

{{KUNDE_FIRMA}}, {{KUNDE_ANSCHRIFT}}

– nachfolgend „Verantwortlicher“ –

und

AUVISO GmbH, Wien / Innsbruck, Österreich, UID ATU74688803, Firmenbuch FN 516504 s

– nachfolgend „Auftragsverarbeiter“ –

gemeinsam die „Parteien“.

§ 1 Gegenstand und Dauer der Verarbeitung

(1) Der Auftragsverarbeiter betreibt für den Verantwortlichen die jeweils beauftragte Software-Plattform ({{PLATTFORM}}) zur Verwaltung und Dokumentation von Service- und Instandhaltungsleistungen (insbesondere Arbeitspositionen, Zeiterfassung, Belegerfassung, Fotodokumentation, Freigabe-Workflows und Monatsabrechnung) einschließlich Wartung, Support und Weiterentwicklung (nachfolgend „Hauptvertrag“).

(2) Diese Vereinbarung konkretisiert die datenschutzrechtlichen Pflichten der Parteien aus dem Hauptvertrag. Sie gilt für alle Tätigkeiten, bei denen der Auftragsverarbeiter oder durch ihn beauftragte Unterauftragsverarbeiter personenbezogene Daten im Auftrag des Verantwortlichen verarbeiten.

(3) Die Laufzeit dieser Vereinbarung entspricht der Laufzeit des Hauptvertrags.

§ 2 Art, Zweck und Umfang der Verarbeitung

(1) Zweck der Verarbeitung ist der Betrieb der Plattform einschließlich Speicherung, Bereitstellung, Sicherung und Auswertung der vom Verantwortlichen und seinen Nutzern eingegebenen Daten sowie die Erbringung von Support-, Wartungs- und Weiterentwicklungsleistungen; ferner – soweit vom Verantwortlichen genutzt – KI-gestützte Funktionen (z. B. Belegauslesung, Text- und Auswertungsassistenz).

(2) Kategorien betroffener Personen:

- Mitarbeiter und Erfassungskräfte des Verantwortlichen
- Ansprechpartner von Auftraggebern, Lieferanten und Nachunternehmern des Verantwortlichen
- sonstige in Projekt-, Beleg- und Fotodokumentation erfasste Personen

(3) Kategorien personenbezogener Daten:

- Stammdaten (Name, Funktion, Kontaktdaten, Zugangsdaten/Benutzerkonten)
- Arbeitszeit- und Leistungsdaten (Zeiterfassung, Zuschläge, Einsatzorte, Tätigkeitsbeschreibungen)
- Abrechnungs- und Belegdaten (Rechnungen, Quittungen, Beträge, Unterschriften)
- Foto- und Dokumentationsdaten von Einsatzorten, auf denen Personen abgebildet sein können
- Protokoll- und Nutzungsdaten (Anmeldungen, Freigaben, technische Logdaten)

(4) Besondere Kategorien personenbezogener Daten (Art. 9 DSGVO) sind nicht Gegenstand der Verarbeitung. Der Verantwortliche stellt sicher, dass solche Daten nicht eingegeben werden.

§ 3 Ort der Verarbeitung

Die Speicherung und Verarbeitung der Daten erfolgt in der Region Frankfurt am Main, Deutschland (AWS eu-central-1), auf der Managed-Plattform der Supabase Inc. Zugriffe des Auftragsverarbeiters zu Betriebs-, Support- und Entwicklungszwecken erfolgen aus Österreich. Verlagerungen der Datenhaltung außerhalb der EU/des EWR bedürfen der vorherigen Zustimmung des Verantwortlichen.

§ 4 Weisungsrecht

(1) Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Verantwortlichen, sofern er nicht durch Unions- oder Mitgliedstaatenrecht zur Verarbeitung verpflichtet ist; in einem solchen Fall teilt er dem Verantwortlichen diese Anforderungen vor der Verarbeitung mit, sofern das Recht dies nicht verbietet.

(2) Weisungen können in Textform (z. B. E-Mail oder Ticket) erteilt werden. Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen die DSGVO oder andere Datenschutzbestimmungen verstößt; er ist berechtigt, die Durchführung bis zur Bestätigung oder Änderung der Weisung auszusetzen.

§ 5 Vertraulichkeit

Der Auftragsverarbeiter setzt für die Verarbeitung nur Personen ein, die zur Vertraulichkeit verpflichtet wurden oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Die Verpflichtung besteht auch nach Beendigung der Tätigkeit fort.

§ 6 Technische und organisatorische Maßnahmen

(1) Der Auftragsverarbeiter trifft die in Anlage 1 beschriebenen technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO und hält diese während der Vertragslaufzeit aufrecht.

(2) Die Maßnahmen dürfen an die technische Weiterentwicklung angepasst werden, sofern das Schutzniveau nicht unterschritten wird. Wesentliche Änderungen werden dokumentiert.

§ 7 Unterauftragsverarbeiter

(1) Der Verantwortliche erteilt die allgemeine Genehmigung zum Einsatz von Unterauftragsverarbeitern. Die bei Vertragsschluss eingesetzten Unterauftragsverarbeiter sind in Anlage 2 aufgeführt und hiermit genehmigt.

(2) Der Auftragsverarbeiter informiert den Verantwortlichen über beabsichtigte Änderungen (Hinzuziehung oder Ersetzung) in Textform. Der Verantwortliche kann aus wichtigem datenschutzrechtlichem Grund binnen 14 Tagen widersprechen; im Fall des Widerspruchs suchen die Parteien einvernehmlich eine Lösung.

(3) Der Auftragsverarbeiter erlegt jedem Unterauftragsverarbeiter vertraglich dieselben Datenschutzpflichten auf, wie sie in dieser Vereinbarung festgelegt sind, insbesondere hinreichende Garantien für geeignete technische und organisatorische Maßnahmen.

(4) Soweit Unterauftragsverarbeiter in Drittländern eingesetzt werden oder ein Drittlandzugriff nicht ausgeschlossen werden kann, stellt der Auftragsverarbeiter geeignete Garantien nach Kap. V DSGVO sicher (insbesondere EU-Standardvertragsklauseln bzw. eine Zertifizierung nach dem EU-U.S. Data Privacy Framework).

§ 8 Unterstützung des Verantwortlichen

(1) Der Auftragsverarbeiter unterstützt den Verantwortlichen mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung der Rechte betroffener Personen (Art. 12–23 DSGVO), insbesondere bei Auskunft, Berichtigung, Löschung und Datenübertragbarkeit.

(2) Er unterstützt den Verantwortlichen ferner bei der Einhaltung der Pflichten aus Art. 32–36 DSGVO (Sicherheit der Verarbeitung, Meldung von Verletzungen, Datenschutz-Folgenabschätzung, Konsultation), unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen.

§ 9 Meldung von Verletzungen des Schutzes personenbezogener Daten

Der Auftragsverarbeiter meldet dem Verantwortlichen jede Verletzung des Schutzes personenbezogener Daten unverzüglich, spätestens jedoch binnen 48 Stunden nach Kenntniserlangung, unter Angabe der nach Art. 33 Abs. 3 DSGVO erforderlichen Informationen, soweit verfügbar. Er dokumentiert Verletzungen einschließlich der Abhilfemaßnahmen.

§ 10 Nachweise und Kontrollen

(1) Der Auftragsverarbeiter stellt dem Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung der Pflichten aus Art. 28 DSGVO zur Verfügung, insbesondere aktuelle Zertifikate und Auditberichte der Unterauftragsverarbeiter (z. B. ISO/IEC 27001, SOC 2 Type 2, BSI C5) sowie eine Beschreibung der eigenen Maßnahmen.

(2) Der Verantwortliche ist nach vorheriger Ankündigung mit angemessener Frist berechtigt, die Einhaltung dieser Vereinbarung zu überprüfen oder durch einen zur Verschwiegenheit verpflichteten Dritten überprüfen zu lassen. Kontrollen erfolgen während der üblichen Geschäftszeiten, ohne den Betrieb unverhältnismäßig zu stören. Bei Unterauftragsverarbeitern, die zertifizierte Rechenzentrums- oder Plattformleistungen erbringen, treten deren Auditberichte und Zertifikate an die Stelle von Vor-Ort-Kontrollen.

§ 11 Löschung und Rückgabe

(1) Nach Abschluss der Erbringung der Verarbeitungsleistungen gibt der Auftragsverarbeiter nach Wahl des Verantwortlichen alle personenbezogenen Daten in einem gängigen, maschinenlesbaren Format heraus oder löscht sie, sofern nicht eine gesetzliche Pflicht zur Speicherung besteht. Die Löschung wird auf Verlangen schriftlich bestätigt.

(2) Sicherungskopien werden entsprechend den Aufbewahrungszyklen automatisch überschrieben; bis dahin bleiben die Schutzmaßnahmen dieser Vereinbarung anwendbar.

§ 12 Haftung und Schlussbestimmungen

(1) Für die Haftung gilt Art. 82 DSGVO; im Innenverhältnis haften die Parteien entsprechend ihrem Verantwortungsanteil. Haftungsregelungen des Hauptvertrags bleiben unberührt.

(2) Änderungen und Ergänzungen dieser Vereinbarung bedürfen der Textform. Bei Widersprüchen zwischen dieser Vereinbarung und dem Hauptvertrag geht in datenschutzrechtlichen Fragen diese Vereinbarung vor.

(3) Es gilt österreichisches Recht unter Ausschluss der Verweisungsnormen; zwingende Bestimmungen der DSGVO bleiben unberührt. Gerichtsstand ist Innsbruck.

(4) Sollten einzelne Bestimmungen unwirksam sein, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt.

Ort, Datum	Ort, Datum
{{KUNDE_FIRMA}} {{KUNDE_VERTRETER}}	AUVISO GmbH René Fleischer

Anlage 1 – Technische und organisatorische Maßnahmen (Art. 32 DSGVO)

Maßnahme	Beschreibung
Zutritts- und Zugangskontrolle	Betrieb ausschließlich in zertifizierten Rechenzentren (AWS Frankfurt, ISO 27001 / BSI C5); kein physischer Zugriff des Auftragsverarbeiters; personalisierte Administrationszugänge mit Mehrfaktor-Absicherung.
Benutzer- und Berechtigungskontrolle	Personalisierte Benutzerkonten; Einmalpasswort-/SSO-Anmeldung mit signierten Sitzungstoken; Row-Level-Security: serverseitige Autorisierung jedes Datenzugriffs auf Datensatzebene; abgestuftes Rollen- und Freigabekonzept (Erfassung, Freigabe, Verwaltung); strikte Mandantentrennung.
Übertragungskontrolle	Ausschließlich TLS-verschlüsselte Verbindungen (HTTPS) für sämtliche Zugriffe und Schnittstellen.
Speicherkontrolle	AES-256-Verschlüsselung der Datenbank- und Dateispeicher (at rest); Geheimnisse und Zugangsdaten in getrennten, verschlüsselten Secret-Stores.
Eingabe- und Protokollkontrolle	Protokollierung sicherheitsrelevanter Vorgänge, Freigaben und Abrechnungsläufe; revisionssichere Monatsabschlüsse mit eingefrorenen Dokumentständen.
Verfügbarkeitskontrolle	Automatische tägliche Backups innerhalb der Region Frankfurt; Point-in-Time-Wiederherstellung; Monitoring der Plattformdienste.
Trennungskontrolle	Getrennte Datenbank-Instanzen je Mandant; logische Trennung von Produktions- und Entwicklungsumgebungen.
Datenminimierung und Löschung	Erhebung nur projekt- und abrechnungsbezogener Daten; Lösch- bzw. Sperrkonzept nach Zweckwegfall unter Beachtung gesetzlicher Aufbewahrungsfristen.
Organisation	Vertraulichkeitsverpflichtung aller eingesetzten Personen; dokumentierte Änderungs- und Deployment-Prozesse mit Versionsständen; unverzügliche Meldung von Sicherheitsvorfällen.

Anlage 2 – Genehmigte Unterauftragsverarbeiter

Unternehmen	Leistung	Ort der Verarbeitung	Garantien / Nachweise
Supabase Inc., USA	Managed-Database- und Backend-Plattform (PostgreSQL, Authentifizierung, Datei-Speicher, Serverless-Funktionen)	Datenhaltung: AWS eu-central-1, Frankfurt am Main (DE)	ISO/IEC 27001, SOC 2 Type 2; DPA mit EU-Standardvertragsklauseln
Amazon Web Services EMEA SARL, Luxemburg	Cloud-Infrastruktur (Rechenzentrum, Speicher, Netzwerk) als Subdienstleister von Supabase	Region eu-central-1, Frankfurt am Main (DE)	ISO/IEC 27001/27017/27018, SOC 1/2/3, BSI C5
Netlify Inc., USA	Auslieferung der statischen Anwendungsdateien (CDN); keine Speicherung personenbezogener Nutzdaten	globales CDN; Verarbeitung technischer Verbindungsdaten	DPA mit EU-Standardvertragsklauseln
Anthropic PBC, USA	KI-gestützte Funktionen (z. B. Belegauslesung, Text- und Auswertungsassistenz); Verarbeitung nur der hierfür übermittelten Inhalte, keine Nutzung zu Trainingszwecken	USA / EU-Endpunkte	DPA; EU-Standardvertragsklauseln / EU-U.S. Data Privacy Framework
Microsoft Ireland Operations Ltd., Irland	E-Mail- und Kalenderdienste (Microsoft 365) – sofern E-Mail-Funktionen aktiviert sind	EU-Rechenzentren	ISO/IEC 27001, SOC 2, EU Data Boundary

Stand: 22. Juli 2026. Änderungen werden gemäß § 7 dieser Vereinbarung mitgeteilt.