

Vertrag zur Auftragsverarbeitung

gemäß Art. 28 DSGVO · Anlage 1 zu den AGB für auraQuote

zwischen dem Kunden (nachfolgend "Verantwortlicher") und der auraNexus.AI GmbH i. G., vertreten durch den Geschäftsführer Oliver Range, Augustinusstraße 11a, 50226 Frechen (nachfolgend "Auftragsverarbeiter") · Stand: Juli 2026

§ 1 Gegenstand und Dauer der Verarbeitung

(1) Der Auftragsverarbeiter erbringt für den Verantwortlichen Leistungen auf Grundlage des Vertrags über die Nutzung der Software auraQuote (nachfolgend "Hauptvertrag"). Dabei verarbeitet der Auftragsverarbeiter personenbezogene Daten im Auftrag des Verantwortlichen. Dieser Vertrag konkretisiert die datenschutzrechtlichen Pflichten der Parteien.

(2) Die Dauer dieses Vertrags entspricht der Laufzeit des Hauptvertrags einschließlich der Bereitstellungsfrist für den Datenexport nach dessen Beendigung.

§ 2 Art und Zweck der Verarbeitung, Datenarten, Betroffene

(1) Art und Zweck der Verarbeitung: Hosting, Speicherung, Anzeige und Verarbeitung der vom Verantwortlichen in die Software eingegebenen Daten zum Zweck der Erstellung, Kalkulation und Verwaltung von Angeboten, einschließlich KI-gestützter Erzeugung von Angebotsentwürfen, Texten und Kalkulationsvorschlägen sowie Dokumentenexport (unter anderem GAEB, PDF, Word).

Arten personenbezogener Daten:

- Stammdaten der Endkunden des Verantwortlichen (Name, Firma, Anschrift)
- Kontaktdaten (E-Mail-Adresse, Telefonnummer)
- Vertrags- und Angebotsdaten (Projektbeschreibungen, Leistungspositionen, Preise, Objekt- und Standortangaben)
- Nutzerdaten der Mitarbeiter des Verantwortlichen (Name, E-Mail-Adresse, Rolle, Protokolldaten)

Kategorien betroffener Personen:

- Endkunden und Interessenten des Verantwortlichen sowie deren Ansprechpartner
- Mitarbeiter und sonstige Nutzer des Verantwortlichen

(2) Besondere Kategorien personenbezogener Daten (Art. 9 DSGVO) sind nicht Gegenstand der Verarbeitung. Der Verantwortliche wird solche Daten nicht in die Software eingeben.

§ 3 Verantwortlichkeit und Weisungsrecht

(1) Der Verantwortliche ist im Verhältnis der Parteien für die Rechtmäßigkeit der Verarbeitung und für die Wahrung der Rechte der betroffenen Personen verantwortlich.

(2) Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Verantwortlichen, sofern er nicht durch das Recht der Union oder der Mitgliedstaaten zur Verarbeitung verpflichtet ist; in einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht verbietet. Der Hauptvertrag sowie die Nutzung der Softwarefunktionen durch den Verantwortlichen gelten als Weisungen. Ergänzende Weisungen bedürfen der Textform.

(3) Ist der Auftragsverarbeiter der Ansicht, dass eine Weisung gegen die DSGVO oder andere Datenschutzbestimmungen verstößt, informiert er den Verantwortlichen unverzüglich und ist berechtigt, die Ausführung bis zur Bestätigung oder Änderung der Weisung auszusetzen.

§ 4 Pflichten des Auftragsverarbeiters

(1) Der Auftragsverarbeiter gewährleistet, dass sich die zur Verarbeitung befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.

(2) Der Auftragsverarbeiter ergreift alle gemäß Art. 32 DSGVO erforderlichen technischen und organisatorischen Maßnahmen. Die zum Zeitpunkt des Vertragsschlusses getroffenen Maßnahmen sind in Anlage A beschrieben. Der Auftragsverarbeiter darf die Maßnahmen an die technische Entwicklung anpassen, sofern das vereinbarte Schutzniveau nicht unterschritten wird.

(3) Der Auftragsverarbeiter benennt dem Verantwortlichen auf Anfrage einen Ansprechpartner für Datenschutzfragen.

(4) Die Verarbeitung erfolgt grundsätzlich in Rechenzentren in der Bundesrepublik Deutschland. Eine Verarbeitung in Drittländern findet nur unter den Voraussetzungen der Art. 44 ff. DSGVO statt, insbesondere auf Grundlage eines Angemessenheitsbeschlusses der EU-Kommission oder von Standardvertragsklauseln; Einzelheiten ergeben sich aus Anlage B.

§ 5 Unterauftragsverarbeiter

(1) Der Verantwortliche erteilt dem Auftragsverarbeiter die allgemeine Genehmigung zur Einschaltung von Unterauftragsverarbeitern. Die zum Zeitpunkt des Vertragsschlusses eingesetzten Unterauftragsverarbeiter sind in Anlage B aufgeführt.

(2) Der Auftragsverarbeiter informiert den Verantwortlichen über beabsichtigte Änderungen in Bezug auf die Hinzuziehung oder Ersetzung von Unterauftragsverarbeitern in Textform. Der Verantwortliche kann innerhalb von 30 Tagen nach Zugang der Information aus wichtigem datenschutzrechtlichem Grund widersprechen. Im Fall eines berechtigten Widerspruchs, dem nicht abgeholfen werden kann, steht beiden Parteien ein außerordentliches Kündigungsrecht hinsichtlich des Hauptvertrags zu.

(3) Der Auftragsverarbeiter erlegt jedem Unterauftragsverarbeiter im Wesentlichen dieselben Datenschutzpflichten auf, wie sie in diesem Vertrag festgelegt sind. Kommt ein Unterauftragsverarbeiter seinen Datenschutzpflichten nicht nach, haftet der Auftragsverarbeiter gegenüber dem Verantwortlichen für die Einhaltung der Pflichten des Unterauftragsverarbeiters.

§ 6 Unterstützung des Verantwortlichen

(1) Der Auftragsverarbeiter unterstützt den Verantwortlichen mit geeigneten technischen und organisatorischen Maßnahmen dabei, Anträge betroffener Personen auf Wahrnehmung ihrer Rechte nach Kapitel III der DSGVO zu beantworten. Anträge, die unmittelbar beim Auftragsverarbeiter eingehen, leitet dieser unverzüglich an den Verantwortlichen weiter.

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

§ 7 Meldung von Verletzungen des Schutzes personenbezogener Daten

(1) Der Auftragsverarbeiter meldet dem Verantwortlichen Verletzungen des Schutzes personenbezogener Daten, die die im Auftrag verarbeiteten Daten betreffen, unverzüglich nach Bekanntwerden. Die Meldung enthält, soweit verfügbar, die in Art. 33 Abs. 3 DSGVO genannten Informationen.

(2) Die Meldung an die Aufsichtsbehörde und die Benachrichtigung betroffener Personen obliegen dem Verantwortlichen.

§ 8 Nachweise und Kontrollrechte

(1) Der Auftragsverarbeiter stellt dem Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung der in Art. 28 DSGVO niedergelegten Pflichten zur Verfügung. Der Nachweis kann insbesondere durch Selbstauskünfte, aktuelle Testate oder Berichte unabhängiger Prüfer sowie geeignete Zertifizierungen erbracht werden.

(2) Der Verantwortliche ist berechtigt, nach vorheriger Anmeldung mit angemessener Frist Überprüfungen einschließlich Inspektionen während der üblichen Geschäftszeiten durchzuführen oder durch einen zur Verschwiegenheit verpflichteten Dritten durchführen zu lassen, soweit die Nachweise nach Absatz 1 im Einzelfall nicht ausreichen. Betriebsabläufe des Auftragsverarbeiters dürfen dabei nicht unverhältnismäßig gestört werden.

§ 9 Löschung und Rückgabe

(1) Nach Beendigung des Hauptvertrags löscht der Auftragsverarbeiter sämtliche im Auftrag verarbeiteten personenbezogenen Daten nach Maßgabe der im Hauptvertrag vereinbarten Export- und Löschfristen, sofern nicht gesetzliche Aufbewahrungspflichten entgegenstehen. Die Löschung aus rollierenden Datensicherungen erfolgt spätestens mit deren turnusmäßiger Überschreibung.

(2) Für die kostenlose Testphase gilt ergänzend: Erfolgt kein Abschluss eines kostenpflichtigen Vertrags, werden die Daten spätestens 14 Tage nach Ablauf der Testphase gelöscht.

(3) Auf Verlangen bestätigt der Auftragsverarbeiter die Löschung in Textform.

§ 10 Haftung, Schlussbestimmungen

(1) Für die Haftung der Parteien gelten Art. 82 DSGVO sowie die Haftungsregelungen des Hauptvertrags.

(2) Im Fall von Widersprüchen zwischen diesem Vertrag und dem Hauptvertrag gehen hinsichtlich der Verarbeitung personenbezogener Daten die Regelungen dieses Vertrags vor.

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

Anlage A: Technische und organisatorische Maßnahmen (Art. 32 DSGVO)

Zutritts- und Zugangskontrolle:

- Hosting in zertifizierten Rechenzentren in Deutschland mit physischen Zutrittskontrollen des Rechenzentrumsbetreibers
- Administrativer Zugriff auf Server ausschließlich über verschlüsselte Verbindungen (SSH) mit Schlüsselauthentifizierung, beschränkt auf autorisierte Personen
- Zugang zur Software nur mit persönlichen Zugangsdaten; Passwörter werden ausschließlich als kryptografische Hashes gespeichert

Zugriffs- und Trennungskontrolle:

- Rollen- und Rechtekonzept innerhalb der Software
- Mandantentrennung: logische Trennung der Daten je Kunde auf Datenbankebene
- Begrenzung fehlgeschlagener Anmeldeversuche, Protokollierung sicherheitsrelevanter Ereignisse

Übertragungskontrolle:

- Verschlüsselte Datenübertragung zwischen Client und Server (TLS)

Verfügbarkeits- und Wiederherstellbarkeitskontrolle:

- Regelmäßige automatisierte Datensicherungen mehrmals täglich

- Zusätzliche Sicherungen vor wesentlichen Systemänderungen
- Dokumentierte Wiederherstellungsverfahren

Organisatorische Maßnahmen:

- Verpflichtung aller mit der Verarbeitung befassten Personen auf Vertraulichkeit
- Prinzip der Datensparsamkeit; Weitergabe an KI-Dienste nur im für die Funktion erforderlichen Umfang
- Regelmäßige Überprüfung und Aktualisierung der Maßnahmen

Anlage B: Unterauftragsverarbeiter

Unternehmen	Leistung	Ort der Verarbeitung	Garantien
IONOS SE, Montabaur, Deutschland	Hosting der Software, Datenbanken und Datensicherungen	Deutschland	AVV nach Art. 28 DSGVO
Resend Inc., USA	Versand von Transaktions-E-Mails (u. a. Passwort-Zurücksetzung, Benachrichtigungen)	USA	Data Processing Agreement nach Art. 28 DSGVO abgeschlossen; Übermittlung auf Grundlage des EU-US Data Privacy Framework bzw. der EU-Standardvertragsklauseln
Anthropic PBC, USA	KI-gestützte Text- und Angebotsgenerierung	USA	Data Processing Agreement nach Art. 28 DSGVO abgeschlossen; EU-US Data Privacy Framework bzw. EU-Standardvertragsklauseln; keine Nutzung der Kundendaten zum Training von KI-Modellen
OpenAI, L.L.C., USA	KI-gestützte Datenanreicherung und Dokumentverarbeitung	USA	Data Processing Agreement nach Art. 28 DSGVO abgeschlossen; EU-US Data Privacy Framework bzw. EU-Standardvertragsklauseln; keine Nutzung der Kundendaten zum Training von KI-Modellen
Google Ireland Ltd. /	Geocoding von	EU / USA	Auftragsverarbeitung

Google LLC	Projektadressen, Gelände-/Höhendaten, Solar-, Wetter-, Pollen- und Luftqualitätsdaten		g auf Grundlage der Google-Datenverarbeitungsbedingungen (Art. 28 DSGVO); EU-Standardvertragsklauseln für Übermittlungen in Drittländer
Cloudflare, Inc., USA	Proxy-Infrastruktur für Geo-API-Aufrufe	global	Data Processing Addendum (Version 6.4) als Bestandteil der Self-Service-Abonnementvereinbarung; EU-US Data Privacy Framework, hilfsweise EU-Standardvertragsklauseln