Auftragsverarbeitungsvertrag gemäß Art. 28 DSGVO

Version 1.0 · Stand: 18. Mai 2026

Diese Online-Fassung zeigt den AVV mit Platzhaltern ([Firma Kunde] etc.). Die konkreten Vertragsdaten werden bei Vertragsunterzeichnung im Offline-PDF eingetragen.

Präambel

Zwischen

[Firma Kunde]
[Adresse]
[PLZ Ort]

— nachfolgend „Verantwortlicher" —

und

AGC Consult
Friedenstraße 59
97072 Würzburg

— nachfolgend „Auftragsverarbeiter" —

§ 1 Gegenstand und Dauer der Verarbeitung

(1) Gegenstand dieses Vertrags ist die Verarbeitung personenbezogener Daten durch den Auftragsverarbeiter im Auftrag des Verantwortlichen im Rahmen der Bereitstellung der Software-as-a-Service-Lösung „AGC Suite" sowie damit verbundener Leistungen (Implementierung, Support, Beratung).

(2) Der Vertrag gilt für die Dauer des zugrunde liegenden Hauptvertrags zwischen den Parteien.

(3) Bei Beendigung des Hauptvertrags endet auch dieser Auftragsverarbeitungsvertrag, vorbehaltlich der Bestimmungen zu Datenlöschung und Aufbewahrung gemäß § 10.

§ 2 Art und Zweck der Verarbeitung

(1) Die Verarbeitung erfolgt zum Zweck der Bereitstellung und des Betriebs der AGC Suite sowie der Erbringung damit verbundener Leistungen für den Verantwortlichen.

(2) Die Art der Verarbeitung umfasst insbesondere: Erheben, Erfassen, Organisieren, Ordnen, Speichern, Anpassen, Auslesen, Abfragen, Verwenden, Übermitteln (innerhalb der vom Verantwortlichen autorisierten Empfänger), Abgleichen, Verknüpfen, Einschränken, Löschen oder Vernichten personenbezogener Daten.

§ 3 Art der personenbezogenen Daten

Im Rahmen der Auftragsverarbeitung können folgende Kategorien personenbezogener Daten verarbeitet werden:

- Stammdaten (z.B. Name, Anschrift, Geburtsdatum, Geschlecht)

- Kontaktdaten (z.B. Telefon, E-Mail, Geschäftsadressen)
- Vertragsdaten (z.B. Vertragsbeziehungen, Konditionen, Laufzeiten)
- Kommunikationsdaten (z.B. Schriftverkehr, Gesprächsnotizen)
- Identifikationsdaten (z.B. Ausweisinformationen im Rahmen von KYC-Prozessen, soweit vom Verantwortlichen verarbeitet)
- Vertriebs- und Transaktionsdaten (z.B. Angebote, Bestellungen, Umsätze)
- IT-Nutzungsdaten (z.B. Login-Zeiten, IP-Adressen, Aktivitätsprotokolle der Nutzer der AGC Suite)

§ 4 Kategorien betroffener Personen

Betroffene Personen können sein:

- Mitarbeitende und Nutzer der AGC Suite beim Verantwortlichen
- Kunden, Interessenten und Geschäftspartner des Verantwortlichen
- Vertragspartner des Verantwortlichen
- Sonstige Personen, deren Daten der Verantwortliche im Rahmen seiner Geschäftstätigkeit in der AGC Suite verarbeitet

§ 5 Pflichten des Auftragsverarbeiters

(1) Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Verantwortlichen. Dies gilt auch für die Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation, sofern er nicht durch das Recht der Union oder der Mitgliedstaaten zur Verarbeitung verpflichtet ist.

(2) Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, wenn er der Auffassung ist, dass eine Weisung gegen geltendes Datenschutzrecht verstößt.

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

(4) Der Auftragsverarbeiter unterstützt den Verantwortlichen im Rahmen seiner Möglichkeiten bei der Erfüllung von Anfragen und Ansprüchen betroffener Personen gemäß Kapitel III der DSGVO sowie bei der Einhaltung der in den Artikeln 32 bis 36 DSGVO genannten Pflichten.

(5) Der Auftragsverarbeiter stellt dem Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung der in Art. 28 DSGVO niedergelegten Pflichten zur Verfügung und ermöglicht Überprüfungen gemäß § 9 dieses Vertrags.

§ 6 Pflichten des Verantwortlichen

(1) Der Verantwortliche ist im Rahmen des Vertragsverhältnisses für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragsverarbeiter sowie für die Rechtmäßigkeit der Datenverarbeitung verantwortlich.

(2) Der Verantwortliche erteilt Weisungen schriftlich oder in einem dokumentierten elektronischen Format. Mündliche Weisungen sind unverzüglich schriftlich oder elektronisch zu bestätigen.

(3) Der Verantwortliche informiert den Auftragsverarbeiter unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Auftragsverarbeitung feststellt.

§ 7 Technische und organisatorische Maßnahmen (TOMs)

(1) Der Auftragsverarbeiter trifft die erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 32 DSGVO zur Sicherheit der Verarbeitung. Die Maßnahmen sind in Anlage 1 zu diesem Vertrag dokumentiert.

(2) Die Maßnahmen werden regelmäßig überprüft und an den jeweiligen Stand der Technik angepasst.

(3) Wesentliche Änderungen der Maßnahmen werden mit dem Verantwortlichen abgestimmt und dokumentiert.

§ 8 Unterauftragsverarbeiter

(1) Der Verantwortliche genehmigt mit Abschluss dieses Vertrags den Einsatz folgender Unterauftragsverarbeiter:

Name	Anschrift	Leistung	Standort der Verarbeitung
Hetzner Online GmbH	Industriestraße 25, 91710 Gunzenhausen	Hosting der AGC Suite	Falkenstein, Deutschland

(2) Der Auftragsverarbeiter informiert den Verantwortlichen über beabsichtigte Änderungen in Bezug auf die Hinzuziehung oder Ersetzung weiterer Unterauftragsverarbeiter mindestens 30 Tage vor der Änderung in Textform. Der Verantwortliche hat das Recht, gegen solche Änderungen Einspruch zu erheben.

(3) Im Falle eines berechtigten Einspruchs des Verantwortlichen, der nicht innerhalb angemessener Frist einvernehmlich gelöst werden kann, hat der Verantwortliche das Recht zur außerordentlichen Kündigung des Hauptvertrags.

(4) Der Auftragsverarbeiter verpflichtet die Unterauftragsverarbeiter vertraglich auf gleichwertige Datenschutzpflichten, wie sie in diesem Vertrag vereinbart sind.

§ 9 Kontrollrechte des Verantwortlichen

(1) Der Verantwortliche hat das Recht, die Einhaltung der vereinbarten Pflichten beim Auftragsverarbeiter zu überprüfen. Der Auftragsverarbeiter stellt hierfür auf Anfrage angemessene Nachweise zur Verfügung (z.B. aktuelle TOMs, Zertifizierungen, Auditberichte).

(2) Vor-Ort-Prüfungen sind nach vorheriger Anmeldung mit angemessener Frist (mindestens 14 Tage) zu üblichen Geschäftszeiten möglich. Sie dürfen den Geschäftsbetrieb des Auftragsverarbeiters nicht unverhältnismäßig beeinträchtigen.

(3) Der Auftragsverarbeiter ist berechtigt, den Aufwand für umfangreiche Prüfungen, die über das übliche Maß hinausgehen, zu marktüblichen Konditionen in Rechnung zu stellen.

§ 10 Löschung und Rückgabe von Daten

(1) Nach Beendigung des Hauptvertrags stellt der Auftragsverarbeiter dem Verantwortlichen die personenbezogenen Daten für einen Zeitraum von 30 Tagen zum Export bereit.

(2) Nach Ablauf der Exportfrist löscht der Auftragsverarbeiter sämtliche personenbezogenen Daten des Verantwortlichen aus seinen Systemen, einschließlich Backups, soweit dem keine gesetzlichen Aufbewahrungspflichten entgegenstehen.

(3) Die Löschung wird dem Verantwortlichen auf Anfrage schriftlich bestätigt.

(4) Backup-Daten werden automatisiert nach 30 Tagen gelöscht.

§ 11 Meldung von Datenschutzvorfällen

(1) Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, spätestens innerhalb von 24 Stunden nach Kenntniserlangung, über Verletzungen des Schutzes personenbezogener Daten (Datenpannen) sowie über bedeutende Störungen bei der Auftragserledigung.

(2) Die Meldung umfasst, soweit zum Zeitpunkt der Meldung verfügbar:

- Beschreibung der Art der Verletzung
- Kategorien und ungefähre Zahl der betroffenen Personen und Datensätze
- voraussichtliche Folgen
- ergriffene oder vorgeschlagene Maßnahmen zur Behebung

(3) Der Auftragsverarbeiter unterstützt den Verantwortlichen bei der Erfüllung etwaiger Meldepflichten an Aufsichtsbehörden und betroffene Personen gemäß Art. 33 und 34 DSGVO.

§ 12 Haftung

Die Haftung der Parteien richtet sich nach den allgemeinen gesetzlichen Bestimmungen, insbesondere Art. 82 DSGVO, sowie den Regelungen des Hauptvertrags.

§ 13 Schlussbestimmungen

(1) Bei Widersprüchen zwischen diesem Vertrag und Regelungen aus anderen Vereinbarungen zwischen den Parteien — insbesondere dem Hauptvertrag — gehen die Regelungen dieses Vertrags in datenschutzrechtlichen Fragen vor.

(2) Sollten einzelne Bestimmungen dieses Vertrags unwirksam sein oder werden, berührt dies die Wirksamkeit der übrigen Bestimmungen nicht.

(3) Änderungen und Ergänzungen dieses Vertrags bedürfen der Schriftform.

(4) Es gilt deutsches Recht. Gerichtsstand ist Würzburg.

Anlage 1: Technische und organisatorische Maßnahmen (TOMs)

Die folgenden technischen und organisatorischen Maßnahmen werden vom Auftragsverarbeiter und seinem Hosting-Unterauftragnehmer Hetzner Online GmbH zur Sicherheit der Verarbeitung gemäß Art. 32 DSGVO umgesetzt.

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

Zutrittskontrolle (Schutz vor unbefugtem physischen Zutritt):

- Rechenzentren mit kontrolliertem Zutritt, Videoüberwachung, Alarmanlagen (Hetzner)
- Zutritt nur für autorisiertes Personal mittels Authentifizierung
- Dokumentierte Besucherprotokolle

Zugangskontrolle (Schutz vor unbefugter Systemnutzung):

- Authentifizierung per Benutzername und Passwort, Passwortrichtlinien (Mindestlänge, Komplexität)
- Möglichkeit zur Multi-Faktor-Authentifizierung
- Automatische Sperre bei wiederholten Fehleingaben
- Verschlüsselte Übertragung der Zugangsdaten (TLS)

Zugriffskontrolle (Schutz vor unbefugtem Zugriff auf Daten):

- Rollen- und Berechtigungskonzept innerhalb der AGC Suite
- Differenzierte Zugriffsrechte je Nutzerrolle
- Protokollierung von Zugriffen und Änderungen (Audit-Trail)
- Trennung von Produktiv- und Testumgebungen

Trennungskontrolle (separate Verarbeitung getrennt erhobener Daten):

- Mandantenfähige Architektur, logische Trennung der Kundendaten
- Eigene Datenbanken oder Schemata je Tenant

Pseudonymisierung und Verschlüsselung:

- Verschlüsselte Datenübertragung (TLS 1.2 oder höher)
- Verschlüsselte Speicherung sensibler Daten in der Datenbank
- Verschlüsselte Backups

2. Integrität (Art. 32 Abs. 1 lit. b DSGVO)

Weitergabekontrolle (Schutz bei elektronischer Übertragung):

- Verschlüsselte Übertragung über HTTPS/TLS
- Sichere API-Zugänge mit Authentifizierung

Eingabekontrolle (Nachvollziehbarkeit von Änderungen):

- Protokollierung von Datenerfassung, -änderung und -löschung
- Audit-Trail mit Zeitstempel und Nutzeridentifikation

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b und c DSGVO)

- Tägliche automatisierte Backups, Aufbewahrung 30 Tage
- Redundante Infrastruktur des Hosting-Anbieters (Hetzner)
- Notfallplan für die Wiederherstellung im Schadensfall
- Monitoring von Verfügbarkeit und Systemzustand
- Schutz vor DDoS-Angriffen auf Infrastrukturebene (Hetzner)
- Antivirus- und Schadcodeschutz auf Systemebene

4. Verfahren zur regelmäßigen Überprüfung (Art. 32 Abs. 1 lit. d DSGVO)

- Regelmäßige Überprüfung der Wirksamkeit der TOMs
- Sicherheitsupdates und Patches werden zeitnah eingespielt
- Schulung und Sensibilisierung der mit der Verarbeitung befassten Mitarbeitenden
- Datenschutzfreundliche Voreinstellungen (Privacy by Default)
- Datenschutz durch Technikgestaltung (Privacy by Design)

5. Auftragskontrolle (Verarbeitung im Sinne des Verantwortlichen)

- Verarbeitung ausschließlich auf dokumentierte Weisung des Verantwortlichen
- Schriftliche Vereinbarung der Pflichten in diesem AVV
- Auswahl der Unterauftragsverarbeiter nach Datenschutzkriterien
- Vertragliche Verpflichtung der Unterauftragsverarbeiter auf gleichwertige Standards

Anmerkung: Diese TOMs entsprechen dem Stand zum [Datum] und werden regelmäßig überprüft und an den aktuellen Stand der Technik angepasst. Wesentliche Änderungen werden dem Verantwortlichen mitgeteilt.
