DATENSCHUTZ

Auftragsverarbeitungsvereinbarung (AVV)

gemäß Art. 28 DSGVO

Diese Auftragsverarbeitungsvereinbarung (AVV) ist die Standard-Auftragsverarbeitungsvereinbarung der EVOMECS GmbH, Kanalstraße 6, 80538 München (nachfolgend „EVOMECS“) im Sinne des Art. 28 DSGVO. Sie gilt für alle Kunden (nachfolgend „Verantwortlicher“), für die EVOMECS im Rahmen der Cloud-Leistungen oder von Support-, Pflege-, Wartungs- oder Beratungsleistungen personenbezogene Daten verarbeitet, und wird durch Bezugnahme Bestandteil der jeweiligen Vertragsbeziehung.

1. Verhältnis zum Hauptvertrag und Rangfolge

(1) Diese AVV ergänzt die zwischen den Parteien geschlossenen Verträge, insbesondere die EVOMECS Cloud-Bedingungen, Softwarelizenzbedingungen, Pflegebedingungen und IT-Services AGB (nachfolgend gemeinsam „Hauptvertrag“).

(2) Sie wird durch Bezugnahme im Angebot, in der Auftragsbestätigung oder im Bestellvorgang des EVOMECS Online-Stores in der bei Vertragsschluss gültigen Fassung Bestandteil der vertraglichen Vereinbarung.

(3) Die Laufzeit dieser AVV richtet sich nach der Laufzeit des Hauptvertrags. Sie endet nicht, solange EVOMECS noch personenbezogene Daten des Verantwortlichen verarbeitet.

(4) Bei Widersprüchen zwischen dieser AVV und dem Hauptvertrag geht diese AVV in allen Fragen des Datenschutzes vor. In allen übrigen Fragen, insbesondere zu Leistungsumfang und Vergütung, gilt der Hauptvertrag.

2. Rollen der Parteien

(1) Der Kunde ist Verantwortlicher im Sinne von Art. 4 Nr. 7 DSGVO. Er ist für die Rechtmäßigkeit der Verarbeitung verantwortlich, einschließlich der Zulässigkeit der Verarbeitung von Beschäftigtendaten und etwaiger Beteiligungsrechte eines Betriebsrats.

(2) EVOMECS ist Auftragsverarbeiter im Sinne von Art. 4 Nr. 8 DSGVO und verarbeitet personenbezogene Daten ausschließlich im Auftrag und nach Weisung des Verantwortlichen.

(3) Soweit EVOMECS Daten zu eigenen Zwecken verarbeitet, etwa anonymisierte und aggregierte Daten nach dem Hauptvertrag oder Vertrags- und Abrechnungsdaten des Kunden, handelt EVOMECS insoweit nicht als Auftragsverarbeiter. Anonymisierte Daten sind keine personenbezogenen Daten.

3. Gegenstand, Zweck und Dauer der Verarbeitung

3.1 Cloud-Betrieb

(1) Bei Cloud-Leistungen betreibt EVOMECS die EVOMECS-Software auf einer Cloud-Infrastruktur und verarbeitet die personenbezogenen Daten des Verantwortlichen dauerhaft für die Dauer des Hauptvertrags.

(2) Zweck der Verarbeitung ist die Bereitstellung der EVOMECS-Software zur digitalen Steuerung und Dokumentation der Fertigung des Verantwortlichen, einschließlich Speicherung, Datensicherung, Betrieb, Wartung, Support und Datenexport.

(3) Die Verarbeitung erfolgt ausschließlich innerhalb der Europäischen Union bzw. des Europäischen Wirtschaftsraums, soweit nicht Ziffer 9 etwas anderes zulässt. Die eingesetzten Unterauftragsverarbeiter ergeben sich aus Anlage 2.

3.2 On-Premise-Betrieb

(1) Beim On-Premise-Betrieb läuft die EVOMECS-Software auf Systemen im Verantwortungsbereich des Verantwortlichen. EVOMECS hat keinen dauerhaften Zugriff auf produktive Daten und keine Verfügungsgewalt über diese Systeme.

(2) EVOMECS verarbeitet personenbezogene Daten hier nur anlassbezogen, zeitlich begrenzt und auf Weisung, insbesondere bei Fernwartung, Support, Pflege oder Beratung.

3.3 Hybride Szenarien

Kombinierte Betriebsmodelle sind zulässig. Für jeden Teil gelten die Regelungen der Ziffer 3.1 bzw. 3.2 entsprechend dem vereinbarten Betriebsmodell.

4. Art der Daten und betroffene Personen

(1) Je nach Nutzung und Konfiguration werden folgende Arten personenbezogener Daten verarbeitet:

- Benutzer- und Kontaktdaten (Name, Benutzerkennung, E-Mail-Adresse, Rolle, Abteilung);
- Tätigkeits- und Rückmeldedaten (an Arbeitsplätzen und Aufträgen gebuchte Tätigkeiten, Zeitstempel, Mengen, Qualitätsmerkmale, Kommentare);
- Maschinen- und Prozessdaten, soweit sie einer Person zugeordnet werden können (z. B. angemeldeter Bediener, Schicht);
- Zugriffs- und Protokolldaten (Anmeldezeiten, IP-Adressen, Systemprotokolle);
- Inhalte in Dokumenten, Zeichnungen und Anhängen, soweit sie personenbezogene Daten enthalten;
- Support- und Kommunikationsinhalte.

(2) Betroffene Personen sind Beschäftigte des Verantwortlichen, sonstige vom Verantwortlichen autorisierte Nutzer sowie Ansprechpartner von Kunden und Lieferanten des Verantwortlichen, soweit deren Daten in der EVOMECS-Software gespeichert werden.

(3) Die Verarbeitung besonderer Kategorien personenbezogener Daten (Art. 9 DSGVO) ist nicht vorgesehen. Der Verantwortliche wird solche Daten nicht in die EVOMECS-Software einbringen.

5. Weisungen

(1) EVOMECS verarbeitet personenbezogene Daten nur auf dokumentierte Weisung des Verantwortlichen, auch in Bezug auf Übermittlungen in Drittländer, es sei denn, EVOMECS ist nach Unionsrecht oder dem Recht eines Mitgliedstaats zur Verarbeitung verpflichtet. In diesem Fall teilt EVOMECS dem Verantwortlichen diese Pflicht vor der Verarbeitung mit, sofern das Recht dies nicht verbietet.

(2) Die Weisungen werden durch den Hauptvertrag und diese AVV festgelegt. Der Verantwortliche kann sie in Textform ergänzen oder ändern.

(3) Ist EVOMECS der Ansicht, dass eine Weisung gegen Datenschutzvorschriften verstößt, informiert EVOMECS den Verantwortlichen unverzüglich und kann die Ausführung aussetzen, bis der Verantwortliche sie bestätigt oder ändert.

(4) Weisungen, die über den vertraglich vereinbarten Leistungsumfang hinausgehen, vergütet der Verantwortliche nach den IT-Services AGB, soweit sie nicht aufgrund eines Verstoßes von EVOMECS erforderlich werden.

6. Vertraulichkeit

EVOMECS gewährleistet, dass alle Personen, die Zugang zu den personenbezogenen Daten des Verantwortlichen haben, zur Vertraulichkeit verpflichtet sind oder einer gesetzlichen Verschwiegenheitspflicht unterliegen und mit den einschlägigen Datenschutzvorschriften vertraut gemacht wurden. Der Zugriff ist auf die Personen beschränkt, die ihn für die Leistungserbringung benötigen. Die Verpflichtung gilt über das Ende der Tätigkeit hinaus.

7. Technische und organisatorische Maßnahmen

(1) EVOMECS trifft die in Anlage 1 beschriebenen technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

(2) Die Maßnahmen unterliegen dem technischen Fortschritt. EVOMECS darf sie durch gleichwertige oder bessere Maßnahmen ersetzen; das Schutzniveau darf dabei nicht unterschritten werden. Wesentliche Änderungen dokumentiert EVOMECS.

(3) Verantwortungsabgrenzung:

- Im Cloud-Betrieb ist EVOMECS für die Sicherheit der Anwendung, der Datenhaltung und der Datensicherung verantwortlich, gemeinsam mit dem in Anlage 2 genannten Infrastrukturanbieter.
- Der Verantwortliche ist in jedem Betriebsmodell verantwortlich für die Verwaltung seiner Nutzerkonten und Berechtigungen, den Schutz der Zugangsdaten und die Sicherheit seiner Endgeräte, Netzwerke und Maschinenanbindungen.
- Im On-Premise-Betrieb ist der Verantwortliche zusätzlich für die Sicherheit seiner Server, Systeme und Datensicherungen verantwortlich.

8. Unterauftragsverarbeiter

(1) Der Verantwortliche erteilt EVOMECS die allgemeine Genehmigung, weitere Auftragsverarbeiter (Unterauftragsverarbeiter) einzusetzen. Die bei Vertragsschluss eingesetzten Unterauftragsverarbeiter sind in Anlage 2 aufgeführt und gelten als genehmigt.

(2) EVOMECS informiert den Verantwortlichen mindestens vier (4) Wochen vor der Hinzuziehung oder Ersetzung eines Unterauftragsverarbeiters in Textform. Der Verantwortliche kann innerhalb dieser Frist aus wichtigem datenschutzrechtlichem Grund widersprechen. Können sich die Parteien nicht einigen, kann der Verantwortliche den betroffenen Vertrag zum Zeitpunkt des Wechsels kündigen. Der Wegfall eines Unterauftragsverarbeiters wird lediglich mitgeteilt.

(3) Bei Gefahr im Verzug, insbesondere wenn ein Unterauftragsverarbeiter aus Sicherheitsgründen kurzfristig ersetzt werden muss, kann EVOMECS die Frist nach Absatz 2 verkürzen; das Widerspruchs- und Kündigungsrecht bleibt bestehen.

(4) EVOMECS verpflichtet jeden Unterauftragsverarbeiter vertraglich auf Datenschutzpflichten, die denen dieser AVV im Wesentlichen entsprechen, und bleibt dem Verantwortlichen gegenüber für die Einhaltung dieser Pflichten verantwortlich.

(5) Keine Unterauftragsverarbeitung im Sinne dieser Ziffer sind Nebenleistungen ohne Zugriff auf personenbezogene Daten des Verantwortlichen, etwa Telekommunikationsleistungen oder Reinigungsdienste.

9. Verarbeitung außerhalb der EU/des EWR

(1) Die Speicherung der Daten im Cloud-Betrieb erfolgt ausschließlich in Rechenzentren innerhalb der EU bzw. des EWR.

(2) Eine Verarbeitung außerhalb der EU bzw. des EWR, etwa durch Zugriffe eines in Anlage 2 genannten Unterauftragsverarbeiters im Rahmen von Support oder Kommunikation, ist nur zulässig, wenn die Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind, insbesondere bei einem Angemessenheitsbeschluss der EU-Kommission (z. B. EU-US Data Privacy Framework) oder auf Grundlage von Standardvertragsklauseln.

(3) EVOMECS teilt dem Verantwortlichen die jeweilige Grundlage auf Anfrage mit.

10. Unterstützungspflichten

(1) EVOMECS unterstützt den Verantwortlichen mit geeigneten technischen und organisatorischen Maßnahmen bei der Erfüllung der Rechte betroffener Personen (Art. 12 bis 22 DSGVO). Wendet sich eine betroffene Person direkt an EVOMECS, leitet EVOMECS die Anfrage unverzüglich an den Verantwortlichen weiter und beantwortet sie nicht selbst.

(2) EVOMECS unterstützt den Verantwortlichen unter Berücksichtigung der verfügbaren Informationen bei der Einhaltung der Pflichten aus Art. 32 bis 36 DSGVO, insbesondere bei Datenschutz-Folgenabschätzungen und der Konsultation der Aufsichtsbehörde.

(3) Im Cloud-Betrieb kann der Verantwortliche Auskunfts-, Berichtigungs- und Löschungsersuchen in der Regel selbst über die Funktionen der EVOMECS-Software erfüllen. Soweit Unterstützung durch EVOMECS darüber hinaus erforderlich ist und nicht auf einem Verstoß von EVOMECS beruht, kann EVOMECS den Aufwand nach den IT-Services AGB berechnen.

11. Meldung von Datenschutzverletzungen

(1) EVOMECS meldet dem Verantwortlichen eine Verletzung des Schutzes personenbezogener Daten unverzüglich, spätestens innerhalb von 48 Stunden nachdem EVOMECS davon Kenntnis erlangt hat, an die vom Verantwortlichen benannte Kontaktadresse.

(2) Die Meldung enthält, soweit bekannt, die Art der Verletzung, die Kategorien und ungefähre Zahl der betroffenen Personen und Datensätze, die wahrscheinlichen Folgen sowie die ergriffenen und vorgeschlagenen Maßnahmen. Informationen, die noch nicht vorliegen, reicht EVOMECS schrittweise nach.

(3) EVOMECS ergreift unverzüglich die erforderlichen Maßnahmen zur Sicherung der Daten und zur Minderung möglicher nachteiliger Folgen und unterstützt den Verantwortlichen bei dessen Melde- und Benachrichtigungspflichten nach Art. 33 und 34 DSGVO.

12. Nachweise und Kontrollen

(1) EVOMECS stellt dem Verantwortlichen auf Anfrage alle Informationen zur Verfügung, die zum Nachweis der Einhaltung dieser AVV erforderlich sind. Der Nachweis kann insbesondere durch aktuelle Testate, Zertifikate oder Prüfberichte unabhängiger Stellen erfolgen, auch solche der Unterauftragsverarbeiter (z. B. ISO/IEC 27001 oder BSI C5 des Infrastrukturanbieters).

(2) Reichen diese Nachweise im Einzelfall nicht aus, ist der Verantwortliche berechtigt, Überprüfungen einschließlich Inspektionen selbst oder durch einen zur Verschwiegenheit verpflichteten Prüfer durchzuführen. Inspektionen sind mit einer Frist von mindestens vier (4) Wochen anzukündigen, finden während der üblichen Geschäftszeiten statt und dürfen den Betriebsablauf nicht unverhältnismäßig stören. Sie sind höchstens

einmal je Kalenderjahr zulässig, es sei denn, es liegt ein konkreter Anlass vor, insbesondere eine Datenschutzverletzung.

(3) Bei Inspektionen ist die Vertraulichkeit der Daten anderer Kunden von EVOMECS zu wahren. Ein Zugriff auf Systeme oder Daten anderer Kunden ist ausgeschlossen.

(4) Den eigenen Aufwand für Inspektionen trägt jede Partei selbst. Den Aufwand von EVOMECS für Inspektionen über die erste im Kalenderjahr hinaus kann EVOMECS nach den IT-Services AGB berechnen, es sei denn, die Inspektion deckt einen erheblichen Verstoß von EVOMECS auf.

13. Rückgabe und Löschung

(1) Nach Ende der Leistungserbringung löscht EVOMECS nach Wahl des Verantwortlichen alle personenbezogenen Daten oder gibt sie zurück, sofern nicht nach Unionsrecht oder dem Recht eines Mitgliedstaats eine Pflicht zur Speicherung besteht.

(2) Im Cloud-Betrieb erfolgt die Rückgabe durch einen Export der Daten nach den Regelungen der Cloud-Bedingungen (Ziffer 12) in einem gängigen, maschinenlesbaren Format. Nach Ablauf der dort geregelten Abholfrist löscht EVOMECS die Daten aus den Produktivsystemen; Datensicherungen werden mit Ablauf ihrer Aufbewahrungsfrist von 14 Tagen gelöscht. EVOMECS bestätigt die Löschung in Textform.

(3) Im On-Premise-Betrieb befinden sich die produktiven Daten im Verantwortungsbereich des Verantwortlichen; eine Rückgabe entfällt. EVOMECS löscht Daten, die es anlassbezogen etwa im Rahmen von Support erhalten hat, sobald sie für den jeweiligen Zweck nicht mehr erforderlich sind, spätestens mit Ende des Vertrags.

(4) Dokumentationen, die dem Nachweis der ordnungsgemäßen Verarbeitung dienen, darf EVOMECS entsprechend den gesetzlichen Aufbewahrungsfristen über das Vertragsende hinaus aufbewahren.

14. Haftung

(1) Für die Haftung der Parteien im Verhältnis zueinander gelten die Haftungsregelungen des Hauptvertrags. Die Haftung gegenüber betroffenen Personen nach Art. 82 DSGVO bleibt unberührt.

(2) Im Innenverhältnis trägt jede Partei den Schaden, der auf ihren eigenen Verantwortungsbereich zurückzuführen ist. EVOMECS haftet nicht für Verstöße, die auf Weisungen des Verantwortlichen oder auf dessen System- und Organisationsbereich beruhen.

15. Schlussbestimmungen

(1) Änderungen und Ergänzungen dieser AVV bedürfen der Textform. Anlage 2 aktualisiert EVOMECS nach dem Verfahren der Ziffer 8.

(2) Kontakt für Datenschutzanfragen und Meldungen an EVOMECS: info@evomecs.com, Betreff „Datenschutz“.

(3) Sollte eine Bestimmung dieser AVV unwirksam sein, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt.

(4) Es gelten das im Hauptvertrag vereinbarte Recht und der dort vereinbarte Gerichtsstand.

Anlage 1: Technische und organisatorische Maßnahmen

Die Maßnahmen gelten für den Cloud-Betrieb und für den Support-Zugriff auf On-Premise-Systeme.

BEREICH	MASSNAHMEN
Rechenzentrum und physischer Schutz	Hosting bei einem Infrastrukturanbieter mit zertifizierten Rechenzentren in der EU (siehe Anlage 2); Zutrittskontrolle, Videoüberwachung, Brand- und Stromausfallschutz durch den Anbieter; Nachweis über dessen Zertifikate.
Zugangskontrolle	Individuelle Benutzerkonten, Passwortrichtlinie, Sperre nach wiederholten Fehlversuchen.
Zugriffskontrolle	Rollen- und Berechtigungskonzept nach dem Need-to-know-Prinzip; Administrationszugriffe nur für berechtigte EVOMECS-Mitarbeiter.
Trennungskontrolle	Logische Trennung der Daten verschiedener Kunden (Mandantentrennung); Trennung von Produktiv-, Test- und Entwicklungsumgebung.
Weitergabekontrolle	Verschlüsselte Übertragung nach dem Stand der Technik (TLS); gesicherter Download für Datenexporte.
Eingabekontrolle	Protokollierung von Anmeldungen und administrativen Änderungen mit angemessener Aufbewahrungsfrist.
Verfügbarkeit und Wiederherstellbarkeit	Tägliche Datensicherung, 14 Tage Aufbewahrung, getrennt vom Produktivsystem; Überwachung der Systeme; regelmäßige Tests der Wiederherstellung.
Organisation	Vertraulichkeitsverpflichtung und Datenschutzschulung der Mitarbeiter; Verfahren zur Meldung von Sicherheitsvorfällen; regelmäßige Überprüfung der Maßnahmen; sorgfältige Auswahl und Kontrolle der Unterauftragsverarbeiter.
Fernwartung (On-Premise)	Zugriff nur nach Freigabe durch den Kunden, über verschlüsselte Verbindung, zeitlich begrenzt und protokolliert.

Anlage 2: Unterauftragsverarbeiter

Stand: 10/2026

- STACKIT (Schwarz Digits Cloud GmbH & Co. KG)
- Google (Google Workspace)
- TeamViewer
- Lovable
- Atlassian
- Grafana Labs
- Univedo