

Auftragsverarbeitungsvertrag (AVV)

Muster-Vertrag — Stand 2026-05-15

zwischen

[KOORDINATOR-NAME], [KOORDINATOR-ANSCHRIFT] — nachfolgend „Verantwortlicher“ —

und

EcoHub München GmbH, Ohlenschlagerstraße 14, 81369 München HRB München,

Geschäftsführung: Müge Fuchsenberger — nachfolgend „Auftragsverarbeiter“ —

zusammen die „Parteien“.

§ 1 Gegenstand und Dauer

(1) Der Auftragsverarbeiter erbringt für den Verantwortlichen die in **Anlage A** beschriebenen Verarbeitungsleistungen im Rahmen der CE-Doc-Plattform.

(2) Der Vertrag tritt mit Unterzeichnung in Kraft und läuft bis zur Beendigung der zugrunde liegenden Hauptleistung. Eine außerordentliche Kündigung gemäß § 11 bleibt unberührt.

§ 2 Art und Zweck der Verarbeitung

Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich zum Zweck der automatisierten Erstellung von technischen Dokumentationen (CE-Akten) nach EU-Maschinenverordnung 2023/1230 für die vom Verantwortlichen betreuten Mandanten. Art und Umfang sind in **Anlage A** konkretisiert.

§ 3 Art der Daten und Kategorien betroffener Personen

(1) Verarbeitete Daten umfassen: - Stamm- und Kontaktdaten der Hersteller-Mandanten (Unternehmensname, Anschrift, Ansprechpartner, E-Mail, Telefon) - Technische Maschinen-Dokumentation (Stücklisten, Schaltpläne, Konstruktionszeichnungen, Risiko-Analysen, Software-Dokumentation) - E-Mail-Korrespondenz im CE-Akten-Workflow - Portal-Zugriffsdaten (Login, gehashte Passwörter, Session-Logs)

(2) Kategorien betroffener Personen: - Mitarbeiter und Geschäftsführer der Hersteller-Mandanten - Mitarbeiter des Verantwortlichen mit Portal-Zugang - ggf. Endkunden des Verantwortlichen, deren Daten in technischen Unterlagen auftreten (z.B. Kontakt-Daten in Wartungs-Plänen)

§ 4 Pflichten des Auftragsverarbeiters

- (1) Der Auftragsverarbeiter verarbeitet die Daten **ausschließlich auf dokumentierte Weisung** des Verantwortlichen, sofern er nicht durch das Recht der Union oder eines Mitgliedstaats verpflichtet wird; in diesem Fall teilt er dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit.
- (2) Der Auftragsverarbeiter stellt sicher, dass die zur Verarbeitung befugten Personen sich zur **Vertraulichkeit verpflichtet haben** oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen.
- (3) Der Auftragsverarbeiter ergreift alle gemäß **Art. 32 DSGVO** erforderlichen Maßnahmen — siehe **Anlage B (TOMs)**.
- (4) Der Auftragsverarbeiter unterstützt den Verantwortlichen bei der Beantwortung von Anträgen Betroffener (Art. 12-22 DSGVO) sowie bei der Einhaltung seiner Pflichten nach Art. 32-36 DSGVO, soweit dies dem Auftragsverarbeiter aufgrund seiner Stellung möglich ist.
- (5) Der Auftragsverarbeiter meldet **Verletzungen des Schutzes personenbezogener Daten** unverzüglich, spätestens binnen 48 Stunden nach Kenntnisnahme, an den Verantwortlichen unter Angabe aller verfügbaren Informationen nach Art. 33 Abs. 3 DSGVO.

§ 5 Unterauftragsverarbeitung

- (1) Die Beauftragung von Unter-Auftragsverarbeitern bedarf der vorherigen schriftlichen oder textlichen Zustimmung des Verantwortlichen.
- (2) Zum Zeitpunkt des Vertragsschlusses sind die in **Anlage C** genannten Unter-Auftragsverarbeiter bereits zugelassen.
- (3) Der Auftragsverarbeiter wird jede beabsichtigte Änderung der Unter-Auftragsverarbeiter dem Verantwortlichen mindestens 30 Tage vor Wirksamwerden in Textform mitteilen. Der Verantwortliche kann der Änderung innerhalb von 14 Tagen begründet widersprechen; in diesem Fall verständigen sich die Parteien gütlich, andernfalls steht dem Verantwortlichen ein außerordentliches Kündigungsrecht zu.

§ 6 Rechte und Pflichten des Verantwortlichen

- (1) Der Verantwortliche ist für die Beurteilung der Zulässigkeit der Datenverarbeitung sowie für die Wahrung der Rechte der Betroffenen allein verantwortlich.
- (2) Der Verantwortliche dokumentiert seine Weisungen schriftlich (auch elektronisch); die Konfigurations-Einstellungen in der CE-Doc-Plattform gelten als dokumentierte Weisung im Sinne dieser Vereinbarung.

§ 7 Drittland-Transfer

- (1) Die Verarbeitung erfolgt grundsätzlich im **Geltungsbereich der DSGVO**.
- (2) **Hosting**: Server in der Europäischen Union (Hetzner Online GmbH, Rechenzentrum Helsinki/ Finnland).

(3) **KI-Modell-Provider:** Mistral AI SAS (Frankreich, EU) als Primär-Provider. Cross-Provider-Konsens optional über Anthropic PBC (USA) und Groq Inc. (USA) auf Basis EU-Standardvertragsklauseln (SCC Modul 2). Die Inhalte werden ausschließlich für den jeweiligen Call übertragen und gemäß Provider-Vertrag nicht für Training verwendet.

(4) Auf Wunsch des Verantwortlichen kann eine **On-Premise-Konfiguration** ohne Drittland-Transfer eingerichtet werden (siehe Anlage A).

§ 8 Kontrollen und Audits

(1) Der Verantwortliche kann sich zu üblichen Geschäftszeiten von der Einhaltung der TOMs überzeugen, insbesondere durch Einsicht in Sicherheitsberichte, technische Dokumentationen und ggf. Vor-Ort-Audits.

(2) Audits werden mit angemessener Vorankündigung (mindestens 14 Tage) abgestimmt und in einem für den Geschäftsbetrieb des Auftragsverarbeiters zumutbaren Rahmen durchgeführt.

(3) Der Auftragsverarbeiter stellt auf Anfrage **Audit-Logs der eigenen Mandanten** des Verantwortlichen für Read-Only-Einsicht bereit.

§ 9 Datenlöschung und -rückgabe

(1) Nach Beendigung der Hauptleistung hat der Auftragsverarbeiter alle im Auftrag verarbeiteten personenbezogenen Daten **nach Wahl des Verantwortlichen** entweder herauszugeben oder zu löschen, einschließlich aller Kopien.

(2) **Aufbewahrungs-Fristen:** - CE-Akten und zugehörige Audit-Trails: 10 Jahre nach Inverkehrbringen-Datum (MVO 2023/1230) - Test-Daten und verworfene Entwürfe: automatische Löschung nach 30 Tagen - E-Mail-Korrespondenz: 6 Jahre (HGB §257) oder Koordinator-Vorgabe

(3) Soweit der Auftragsverarbeiter aufgrund gesetzlicher Aufbewahrungs- Pflichten zur weiteren Aufbewahrung verpflichtet ist, gilt die Pflicht zur Löschung erst nach Ablauf dieser Frist.

§ 10 Haftung

Die Haftung der Parteien bestimmt sich nach Art. 82 DSGVO und den Regelungen des Hauptvertrags.

§ 11 Kündigung und Beendigung

(1) Dieser AVV endet automatisch mit dem Hauptvertrag.

(2) Bei wesentlichen Verstößen gegen diese Vereinbarung kann jede Partei außerordentlich mit Frist von 14 Tagen kündigen.

§ 12 Sonstiges

(1) Es gilt das Recht der Bundesrepublik Deutschland.

(2) Gerichtsstand ist München.

(3) Änderungen und Ergänzungen bedürfen der Textform.

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

Anlagen: - Anlage A — Leistungsbeschreibung und Verarbeitungs-Details - Anlage B — Technische und organisatorische Maßnahmen (TOMs) - Anlage C — Unter-Auftragsverarbeiter

Ort, Datum: Ort, Datum:

Verantwortlicher Auftragsverarbeiter (Koordinator) EcoHub München GmbH

Anlage A — Leistungsbeschreibung

Verarbeitungs-Schritte: 1. Annahme von Eingangsdokumenten (E-Mail, ZIP-Upload) 2. Klassifikation und Analyse durch spezialisierte KI-Agenten 3. Aggregation der Analyse-Ergebnisse zu Anhang-IV-Sektionen 4. Cross-Provider-Konsens-Prüfung (Mistral + optional Anthropic/Groq) 5. Lektor-Konsolidierung 6. Render zu PDF/Markdown-Akte 7. Versand-Workflow (OPL-Rückfragen an Hersteller, Akte-Versand) 8. Audit-Trail-Speicherung

Hosting-Standort: Hetzner Online GmbH, Rechenzentrum Helsinki (Finnland)

KI-Provider: - Primär: Mistral AI SAS, 91100 Massy, Frankreich (Enterprise-Account, vertraglich kein Training) - Optional Cross-Provider: Anthropic PBC, San Francisco USA (SCC Modul 2); Groq Inc., Mountain View USA (SCC Modul 2) - On-Premise-Option: lokale LLMs ohne externe Provider (auf Anfrage)

Zugriffsberechtigte beim Auftragsverarbeiter: - Geschäftsführung EcoHub München GmbH - Technischer Administrator (1 Person, namentlich benannt) - Support-Mitarbeiter (im Bedarfsfall, schriftlich beauftragt, NDA-bindlich)

Anlage B — Technische und organisatorische Maßnahmen (TOMs)

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

- **Zutrittskontrolle:** Rechenzentrum Hetzner Helsinki ist ISO 27001 zertifiziert; physischer Zugriff nur autorisiertes Personal.
- **Zugangskontrolle:** SSH-Public-Key-Auth, kein Passwort-Login auf Server; Multi-Faktor-Auth für administrative Zugänge.
- **Zugriffskontrolle:** Tenant-physisch getrennte Verzeichnisse pro Koordinator. Lese-Zugriff nur über Portal-Login mit Koordinator-Cookie-Session.

- **Trennungskontrolle:** Mandanten eines Koordinators sind in Verzeichnis-Bäumen physisch getrennt. Es gibt keine gemeinsame Datenbank, daher architektonisch kein Cross-Mandanten-Zugriff möglich.
- **Pseudonymisierung/Verschlüsselung:** TLS 1.3 für alle externen Verbindungen. Dateisystem-Verschlüsselung des Daten-Pfades. Passwörter bcrypt-gehasht.

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

- **Eingabekontrolle:** Audit-Log über alle State-Mutationen mit Zeitstempel, Benutzer-ID, Rolle.
- **Übermittlungskontrolle:** TLS 1.3 + Zertifikats-Pinning für interne Service-Kommunikation.
- **Konfigurations-Stempel:** kryptografischer Fingerabdruck der CE-Akte bei Freigabe (SHA-256 über Stückliste + Akte + Audit-Trail).

B.3 Verfügbarkeit und Belastbarkeit

- **Backup:** tägliches inkrementelles Backup, wöchentliches Vollbackup, Retention 30 Tage.
- **Wiederherstellung:** dokumentiertes Recovery-Procedure, RTO 4 Stunden, RPO 24 Stunden.
- **Monitoring:** Health-Endpoint, Alert-Pattern für Service-Ausfall, Provider-Verfügbarkeits-Tracking.

B.4 Regelmäßige Überprüfung

- **Penetrations-Tests** mindestens jährlich.
- **DSGVO-Compliance-Review** alle 6 Monate.
- **Auditor-Schleife** für externe Akten-Prüfung im Standard-Workflow.

Anlage C — Unter-Auftragsverarbeiter (Stand 2026-05-15)

Name	Sitz	Funktion	Vertrag
Hetzner Online GmbH	Industriestr. 25, 91710 Gunzenhausen / RZ Helsinki, Finnland	Server-Hosting	AVV nach DSGVO Art. 28
Mistral AI SAS	38 Avenue Ledru-Rollin, 75012 Paris, Frankreich	LLM-Provider primary	Enterprise-Vertrag, vertraglich kein Training
Anthropic PBC	548 Market St #93953, San Francisco CA 94104, USA	LLM-Provider Cross-Konsens (optional)	SCC Modul 2 + Anthropic-DPA
Groq Inc.	400 Castro St, Mountain View CA 94041, USA	LLM-Provider Cross-Konsens (optional)	SCC Modul 2 + Groq-DPA

Auf Wunsch des Verantwortlichen kann der Einsatz einzelner Sub-Verarbeiter deaktiviert werden (z.B. On-Premise-only ohne Cross-Provider). Die deaktivierten Provider werden in der Konfiguration und im Audit-Trail sichtbar dokumentiert.