Auftragsverarbeitungsvertrag (AVV)

gemäß Art. 28 DSGVO – Stand: März 2026

English-speaking customers: this data processing agreement (Art. 28 GDPR) is provided in German; the German version is the legally binding one.

Parteien

Auftragsverarbeiter:

Assetflow – Inh. Marco Koppenhöfer

Kaiserslauterer Straße 325, 67098 Bad Dürkheim, Deutschland

E-Mail: datenschutz@profitkonsole.de

Verantwortlicher (Auftraggeber):

Der Kunde der SaaS-Lösung „profitkonsole“ gemäß den Allgemeinen Geschäftsbedingungen.

§ 1 Gegenstand und Dauer

(1) Dieser Auftragsverarbeitungsvertrag (nachfolgend „AVV“) konkretisiert die datenschutzrechtlichen Verpflichtungen der Parteien gemäß Art. 28 DSGVO im Zusammenhang mit der Nutzung der SaaS-Plattform „profitkonsole“.

(2) Der AVV ergänzt die Allgemeinen Geschäftsbedingungen (AGB) und die Datenschutzerklärung der profitkonsole. Im Falle von Widersprüchen in datenschutzrechtlichen Belangen geht dieser AVV vor.

(3) Die Laufzeit dieses AVV richtet sich nach der Laufzeit des Hauptvertrags (AGB). Er endet automatisch mit Beendigung der Kundenbeziehung.

§ 2 Art und Zweck der Verarbeitung

Die Verarbeitung personenbezogener Daten erfolgt zum Zweck der:

- Bereitstellung und Betrieb der SaaS-Plattform profitkonsole
- Benutzerkontenverwaltung und Authentifizierung
- Synchronisation und Analyse von Geschäftsdaten via OTTO Market API
- Versand transaktionaler E-Mails (Registrierung, Passwort-Reset, Team-Einladungen)
- (optional, nur bei Aktivierung) KI-gestützte Beantwortung von Fragen zu den eigenen Geschäftsdaten in natürlicher Sprache (Funktion „Cortex“, siehe § 7a)

Verarbeitungsarten: Erhebung, Speicherung, Änderung, Auslesen, Abfrage, Verwendung, Löschung.

§ 3 Art der personenbezogenen Daten

Im Rahmen der Auftragsverarbeitung werden folgende Arten personenbezogener Daten verarbeitet:

- E-Mail-Adressen der Account-Nutzer
- Namen der Account-Nutzer
- Organisationsbezeichnungen
- Nutzungsdaten (Login-Zeiten, aufgerufene Seiten innerhalb der Anwendung)
- Technische Daten (IP-Adressen in Server-Logs)

Ausdrücklicher Hinweis: Personenbezogene Endkundendaten (Namen, Adressen, Kontaktdaten von Bestellern aus dem OTTO-Konto des Auftraggebers) werden vom Auftragsverarbeiter weder erhoben noch gespeichert. Die über die OTTO-Schnittstelle synchronisierten Daten umfassen ausschließlich aggregierte Geschäftsdaten (Bestellnummern, Umsätze, Produktdaten, Gebühren).

§ 4 Kategorien betroffener Personen

Betroffene Personen sind ausschließlich Beschäftigte und Beauftragte des Auftraggebers, die über einen Account in der profitkonsole verfügen.

§ 5 Pflichten des Auftraggebers

(1) Der Auftraggeber ist als Verantwortlicher im Sinne der DSGVO für die Rechtmäßigkeit der Datenverarbeitung verantwortlich.

(2) Der Auftraggeber erteilt dem Auftragsverarbeiter Weisungen in Bezug auf die Verarbeitung personenbezogener Daten. Der Hauptvertrag (AGB) sowie dieser AVV gelten als dokumentierte Weisung.

(3) Der Auftraggeber ist verpflichtet, seine eigenen Beschäftigten über die Datenverarbeitung im Rahmen der Plattformnutzung zu informieren.

(4) Die Meldepflicht bei Datenschutzvorfällen gegenüber der Aufsichtsbehörde (Art. 33 DSGVO) obliegt dem Auftraggeber als Verantwortlichem.

(5) Der Auftraggeber kann innerhalb der Plattform weitere Nutzer (Teammitglieder, Administratoren, externe Berater/Agenturen) einladen und ihnen Zugriff auf seine Daten gewähren. Die Auswahl dieser Personen, die Vergabe ihrer Berechtigungen sowie deren Einhaltung datenschutzrechtlicher Vorgaben liegen in der alleinigen Verantwortung des Auftraggebers. Der Auftragsverarbeiter stellt lediglich die technische Infrastruktur zur Verwaltung dieser Zugriffe bereit.

§ 6 Pflichten des Auftragsverarbeiters

(1) Der Auftragsverarbeiter verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Auftraggebers, es sei denn, er ist gesetzlich zur Verarbeitung verpflichtet.

(2) Der Auftragsverarbeiter gewährleistet, dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet haben.

(3) Der Auftragsverarbeiter trifft die erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 32 DSGVO (siehe § 9 dieses AVV).

(4) Der Auftragsverarbeiter unterstützt den Auftraggeber bei der Erfüllung der Betroffenenrechte (Art. 15–22 DSGVO) sowie bei Datenschutz-Folgenabschätzungen (Art. 35–36 DSGVO), soweit dies erforderlich und zumutbar ist.

(5) Der Auftragsverarbeiter informiert den Auftraggeber ohne unangemessene Verzögerung über Datenschutzverletzungen gemäß Art. 33 Abs. 2 DSGVO. Die Meldung umfasst die Art der Verletzung, die betroffenen Datenkategorien, die voraussichtlichen Folgen sowie die ergriffenen Gegenmaßnahmen.

(6) Nach Beendigung des Hauptvertrags löscht der Auftragsverarbeiter sämtliche personenbezogenen Daten gemäß den Löschregeln in den AGB (§ 7a), sofern keine gesetzliche Aufbewahrungspflicht besteht.

§ 7 Unterauftragsverarbeitung

(1) Der Auftraggeber erteilt dem Auftragsverarbeiter die allgemeine Genehmigung, Unterauftragsverarbeiter einzusetzen.

(2) Der Auftragsverarbeiter stellt sicher, dass Unterauftragsverarbeitern mindestens die gleichen Datenschutzpflichten auferlegt werden wie in diesem AVV.

(3) Der Auftragsverarbeiter informiert den Auftraggeber über beabsichtigte Änderungen bei Unterauftragsverarbeitern. Der Auftraggeber kann innerhalb von 14 Tagen nach Mitteilung Widerspruch einlegen. Im Falle eines berechtigten Widerspruchs steht dem Auftraggeber ein Sonderkündigungsrecht zu.

Aktuelle Unterauftragsverarbeiter:

Dienstleister	Zweck	Standort	Garantie
Supabase Inc.	Datenbank, Authentifizierung	EU (Stockholm)	DPA, SOC 2
Vercel Inc.	Hosting, Functions, CDN	EU (Frankfurt)	DPA, SOC 2

Dienstleister	Zweck	Standort	Garantie
Trigger.dev	Background Jobs, Sync	EU (Frankfurt)	DPA
Resend	Transaktionale E-Mails	USA	DPA, EU-US DPF
Sentry	Error Monitoring	USA/EU	DPA, EU-US DPF
Stripe Inc.	Zahlungsabwicklung	Irland / USA	DPA, EU-US DPF
Mistral AI SAS	KI-Assistent „Cortex“ (optional, nur bei Aktivierung)	EU (Frankreich)	DPA, EU, kein Training, Löschung ≤ 30 Tage

§ 7a Optionaler KI-Assistent „Cortex“

(1) Diese Bestimmung gilt ausschließlich, sofern der Auftraggeber die optionale Funktion „Cortex“ aktiviert. Ohne Aktivierung werden keine Daten an den KI-Dienstleister übermittelt; für Auftraggeber ohne Cortex-Nutzung entfaltet diese Bestimmung keine Wirkung.

(2) Bei Nutzung von Cortex werden die vom Nutzer eingegebene Frage, daraus abgeleitete aggregierte Kennzahlen (z. B. Umsätze, Margen, Retouren – keine personenbezogenen Endkundendaten) sowie die erzeugte Antwort an Mistral AI SAS (Frankreich, EU) übermittelt, um die Antwort zu generieren.

(3) Mistral verarbeitet diese Daten ausschließlich zur Erbringung der Antwort, nicht zum Training eigener Modelle, und löscht sie nach maximal 30 Tagen (Missbrauchserkennung). Die Verarbeitung erfolgt in der EU.

(4) Der Auftragsverarbeiter protokolliert Anfrage und Antwort zur Qualitätssicherung und Verbesserung im Mandanten-Schema des Auftraggebers. Diese Protokolle werden nach 90 Tagen automatisch gelöscht; bei Deaktivierung von Cortex werden die Protokolle des jeweiligen Nutzers unverzüglich gelöscht.

(5) Die Aktivierung erfolgt pro Nutzer und ist jederzeit widerrufbar. Im Übrigen gelten die Pflichten dieses AVV (insbesondere § 7) für Mistral AI SAS als Unterauftragsverarbeiter entsprechend.

§ 8 Kontrollrechte

(1) Der Auftraggeber hat das Recht, die Einhaltung der datenschutzrechtlichen Vorgaben zu überprüfen.

(2) Der Nachweis erfolgt in der Regel durch Vorlage geeigneter Nachweise wie aktueller Zertifizierungen, Auditberichte oder Selbstauskünfte des Auftragsverarbeiters.

(3) Vor-Ort-Prüfungen sind nur nach vorheriger Vereinbarung mit angemessener Vorlaufzeit und auf Kosten des Auftraggebers möglich, sofern die Vorlage von Nachweisen gemäß Absatz 2 nicht ausreichend ist.

§ 9 Technisch-organisatorische Maßnahmen (TOMs)

Der Auftragsverarbeiter trifft die folgenden technischen und organisatorischen Maßnahmen gemäß Art. 32 DSGVO:

Vertraulichkeit

- Verschlüsselung: TLS 1.2+ (Transport), AES-256 (Encryption at Rest)
- Mandantentrennung: Separate PostgreSQL-Schemas pro Kunde
- Zugriffssteuerung: Row-Level Security (RLS), JWT-basierte Authentifizierung
- Rollenkonzept: Owner/Admin/Moderator mit Least-Privilege-Prinzip
- MFA für alle administrativen Zugänge (Vercel, Supabase, GitHub)
- Secrets in Umgebungsvariablen, keine Hardcodierung im Quellcode

Verfügbarkeit und Wiederherstellung

- Serverless-Hosting mit Auto-Scaling und DDoS-Schutz
- Automatische tägliche Datenbank-Backups
- Point-in-Time Recovery innerhalb der Backup-Retention
- Code-Versionierung via Git; Deployment-Rollback jederzeit möglich

Regelmäßige Überprüfung

- Schwachstellenscans alle 180 Tage (OWASP ZAP)
- Automatisierte Dependency-Checks (Dependabot, npm audit)
- Regelmäßige Aktualisierung aller Abhängigkeiten

Die Maßnahmen werden regelmäßig überprüft und dem Stand der Technik angepasst.

§ 10 Meldung von Datenschutzverletzungen

Der Auftragsverarbeiter informiert den Auftraggeber ohne unangemessene Verzögerung über Datenschutzverletzungen gemäß Art. 33 DSGVO. Die Meldung umfasst die Art der Verletzung, die betroffenen Datenkategorien, die voraussichtlichen Folgen sowie die ergriffenen Gegenmaßnahmen.

§ 11 Haftung

Die Haftung der Parteien richtet sich nach Art. 82 DSGVO. Beide Parteien haften nur im Rahmen ihrer jeweiligen Verantwortlichkeit für Schäden, die aus einer unrechtmäßigen Verarbeitung entstehen.

§ 12 Drittlandübermittlung

Soweit Unterauftragsverarbeiter personenbezogene Daten in Drittländer übermitteln, erfolgt dies unter Einhaltung von Kapitel V DSGVO, insbesondere auf Grundlage des EU-US Data Privacy Frameworks (DPF) oder Standardvertragsklauseln (SCC). Die primäre Datenhaltung erfolgt in EU-Rechenzentren.

§ 13 Schlussbestimmungen

(1) Änderungen und Ergänzungen dieses AVV bedürfen der Schriftform.

(2) Sollten einzelne Bestimmungen dieses AVV unwirksam sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt.

(3) Es gilt das Recht der Bundesrepublik Deutschland.

(4) Dieser AVV ergänzt die AGB der profitkonsole und geht in datenschutzrechtlichen Belangen im Zweifelsfall vor.

Dieser Auftragsverarbeitungsvertrag wird bei Bedarf angepasst, um rechtliche Anforderungen oder Änderungen unserer Leistungen abzubilden.

© 2026 profitkonsole. Alle Rechte vorbehalten.