

Auftragsverarbeitungsvertrag nach Art. 28 DSGVO

Entwurf zur juristischen Prüfung. Dieser Text ist noch nicht freigegeben; Angaben in eckigen Klammern sind Platzhalter.
Stand 21.10.2026.

Vertragsparteien

Auftragsverarbeitungsvertrag zwischen dem Kunden (Verantwortlicher) und [Firma des Anbieters, z. B. DemKar Group GmbH], [Straße und Hausnummer], [PLZ] [Ort] (Auftragsverarbeiter). Dieser Vertrag ist Bestandteil der Allgemeinen Geschäftsbedingungen von Saldino und gilt mit der Registrierung bzw. dem Abschluss des Abonnements als geschlossen; der Kunde kann ihn als PDF herunterladen und für seine Unterlagen aufbewahren.

Vertragspartner (Verantwortlicher): _____ (Firma, Anschrift, vertreten durch)

Datum, Unterschrift Verantwortlicher: _____ Datum, Unterschrift Auftragsverarbeiter:

1. Gegenstand und Dauer

Der Auftragsverarbeiter verarbeitet personenbezogene Daten im Auftrag des Verantwortlichen zum Betrieb der Rechnungs- und Buchhaltungssoftware Saldino (Software-as-a-Service). Die Dauer entspricht der Laufzeit des Nutzungsvertrags einschließlich des Lesemodus nach Vertragsende bis zur Löschung des Kontos.

2. Art und Zweck der Verarbeitung, Datenarten, betroffene Personen

- Zweck: Speicherung, Verarbeitung und Bereitstellung der vom Verantwortlichen erfassten Daten für Rechnungsstellung, Belegverwaltung, Zahlungsabgleich, Buchführung und Auswertungen.
- Datenarten: Stammdaten von Kunden und Lieferanten (Name, Anschrift, Kontaktdaten, Bankverbindung, Steuernummern), Belegdaten (Positionen, Beträge, Zahlungsinformationen), Bankumsätze (Buchungstext, Gegenkonto, Beträge), Benutzerdaten des Verantwortlichen (Name, E-Mail, Rolle, Protokolldaten), Dateien (Belege, Logos).
- Betroffene Personen: Kunden, Lieferanten, Ansprechpartner und Mitarbeitende des Verantwortlichen sowie dessen Steuerberater.

3. Weisungen

Der Auftragsverarbeiter verarbeitet die Daten ausschließlich auf dokumentierte Weisung des Verantwortlichen; die Nutzung der Anwendung und deren Konfiguration gelten als Weisung. Der Auftragsverarbeiter informiert den Verantwortlichen unverzüglich, wenn er eine Weisung für rechtswidrig hält. Weisungen außerhalb des Funktionsumfangs bedürfen der Textform.

4. Pflichten des Auftragsverarbeiters

- Verpflichtung der mit der Verarbeitung befassten Personen zur Vertraulichkeit.
- Umsetzung der technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO (Anlage 2) und deren regelmäßige Überprüfung.
- Unterstützung des Verantwortlichen bei der Beantwortung von Anfragen betroffener Personen durch Funktionen der Anwendung (Datenauskunft je Kontakt, Löschen, Export) und, soweit erforderlich, durch weitere Unterstützung.
- Unterstützung bei der Einhaltung der Pflichten aus Art. 32 bis 36 DSGVO (Sicherheit, Meldung von Verletzungen, Datenschutz-Folgenabschätzung).
- Meldung von Verletzungen des Schutzes personenbezogener Daten an den Verantwortlichen unverzüglich, spätestens innerhalb von 48 Stunden nach Kenntnis, mit den nach Art. 33 Abs. 3 DSGVO erforderlichen Angaben.
- Löschung oder Rückgabe aller Daten nach Abschluss der Verarbeitung nach Wahl des Verantwortlichen (Datenexport in der Anwendung, Kontolöschung mit Sperrfrist), soweit keine gesetzliche Aufbewahrungspflicht besteht.
- Bereitstellung aller zum Nachweis der Einhaltung erforderlichen Informationen und Ermöglichung von Überprüfungen (Ziffer 7).

5. Unterauftragsverarbeiter

Der Verantwortliche genehmigt die in Anlage 1 genannten Unterauftragsverarbeiter. Der Auftragsverarbeiter informiert den Verantwortlichen über beabsichtigte Änderungen (Hinzufügen oder Ersetzen) mindestens vier Wochen vorher per E-Mail; der Verantwortliche kann innerhalb von zwei Wochen aus wichtigem Grund widersprechen. Mit jedem Unterauftragsverarbeiter werden gleichwertige Datenschutzpflichten vertraglich vereinbart.

6. Verarbeitung in Drittländern

Die Verarbeitung erfolgt in Deutschland bzw. in der Europäischen Union. Soweit ein Unterauftragsverarbeiter (Stripe) Daten in die USA übermittelt, geschieht dies auf Grundlage der EU-Standardvertragsklauseln und der Zertifizierung nach dem EU-US Data Privacy Framework; der Umfang ist auf die Zahlungsabwicklung des Abonnements beschränkt und betrifft keine Daten der Kunden des Verantwortlichen.

7. Kontrollrechte

Der Verantwortliche kann die Einhaltung dieses Vertrags überprüfen. Der Auftragsverarbeiter stellt hierzu Dokumentationen (TOM, Verzeichnis der Verarbeitungstätigkeiten, Verfahrensdokumentation, Zertifikate des Rechenzentrums) bereit. Vor-Ort-Prüfungen sind nach Ankündigung mit angemessener Frist während der üblichen Geschäftszeiten möglich, höchstens einmal jährlich, sofern kein konkreter Anlass besteht.

8. Haftung

Für die Haftung gilt Art. 82 DSGVO sowie die Haftungsregelung der Allgemeinen Geschäftsbedingungen.

9. Schlussbestimmungen

Änderungen und Ergänzungen bedürfen der Textform. Bei Widersprüchen zwischen diesem Vertrag und den AGB gehen die Regelungen dieses Vertrags vor, soweit sie den Datenschutz betreffen. Es gilt deutsches Recht.

Anlage 1: Unterauftragsverarbeiter

Unternehmen	Leistung	Ort	Grundlage
Hostinger International Ltd. (Rechenzentrum Deutschland)	Hosting des Servers (Datenbank, Web-App, Dateien)	Deutschland (Rechenzentrum), Anbieter mit Sitz in Zypern (EU)	AVV mit Hostinger
Supabase (self-hosted auf dem eigenen Server)	Datenbank, Authentifizierung, Dateiablage als Software, keine Datenübermittlung an Supabase Inc.	Deutschland (eigener Server)	kein Auftragsverarbeiter, Open-Source-Software
Brevo (Sendinblue GmbH, Berlin)	Versand von Transaktions-E-Mails (Rechnungen, Mahnungen, Bestätigungen)	EU (Rechenzentren in der EU)	AVV mit Brevo
Stripe Payments Europe, Ltd. (Dublin)	Zahlungsabwicklung des Abonnements (Kreditkarte, SEPA), Rechnungsstellung an den Kunden	EU; Stripe Inc. (USA) als weiterer Verarbeiter unter EU-Standardvertragsklauseln und EU-US Data Privacy Framework	Stripe Data Processing Agreement

Anlage 2: Technische und organisatorische Maßnahmen – Zutritts- und Zugangskontrolle

- Server in einem zertifizierten Rechenzentrum in Deutschland (Zutritt nur für Rechenzentrumsbetreiber).
- Administrativer Zugang nur per SSH-Schlüssel, keine Passwortanmeldung, Firewall mit ausschließlich benötigten Ports (80, 443, SSH).

- Benutzerzugang zur Anwendung mit E-Mail und Passwort, optional Zwei-Faktor-Authentifizierung (TOTP); Administratoren können diese erzwingen.

Anlage 2 – Zugriffskontrolle

- Mandantentrennung auf Datenbankebene (Row Level Security): jede Abfrage ist auf die Organisation des angemeldeten Benutzers beschränkt.
- Rollenmodell (Administration, Finanzen, Vertrieb, Steuerberater) mit abgestuften Rechten, serverseitig durchgesetzt.
- Dateiablage (Belege, Logos) nur über signierte, zeitlich begrenzte Zugriffe.

Anlage 2 – Weitergabe- und Eingabekontrolle

- Transportverschlüsselung (TLS 1.2 oder höher) für alle Verbindungen, HSTS.
- Vollständiges Audit-Log aller Änderungen (Benutzer, Zeitpunkt, Vorher/Nachher) mit Hashkette gegen nachträgliche Manipulation.
- Festschreibung abgeschlossener Belege (GoBD), Storno nur als Gegenbuchung.

Anlage 2 – Verfügbarkeitskontrolle

- Tägliche verschlüsselte Datenbank-Backups mit Aufbewahrung von [30] Tagen, [Off-Site-Kopie].
- Überwachung der Dienste, automatischer Neustart, Statusseite unter /status.
- Wiederherstellungstest [halbjährlich].

Anlage 2 – Trennungskontrolle

- Logische Trennung der Mandanten in einer gemeinsamen Datenbank über Row Level Security und organisationsgebundene Schlüssel.
- Test- und Produktivsysteme getrennt.

Anlage 2 – Löschung und Datenportabilität

- Datenexport (ZIP mit allen Tabellen als CSV, Belegdateien, Einstellungen) jederzeit durch den Kunden.
- Kontolöschung mit Sperrfrist von 30 Tagen, danach vollständige Löschung inklusive Dateien und Löschprotokoll.
- Backups werden nach Ablauf der Aufbewahrung überschrieben.

Anlage 2 – Organisation

- Verzeichnis der Verarbeitungstätigkeiten, Verfahrensdokumentation (GoBD) und dieses TOM-Dokument werden bei Änderungen fortgeschrieben.
- Meldung von Datenschutzverletzungen an den Verantwortlichen unverzüglich, spätestens innerhalb von 48 Stunden nach Kenntnis.
- Mitarbeitende und Dienstleister sind auf Vertraulichkeit verpflichtet.