

Auftragsverarbeitungsvertrag (AVV)

Stand: Version 1.1 · 19. Juli 2026



AVV als PDF

Version 1.1 — gegenzeichnen und zu Ihren Unterlagen nehmen

Herunterladen

nach Art. 28 DSGVO zwischen dem Kunden (nachfolgend „Verantwortlicher“) und der Soberciety GmbH, Junkersstraße 20, 93055 Regensburg (nachfolgend „Auftragsverarbeiter“). Dieser Vertrag wird mit Annahme der [AGB](#) Bestandteil des Nutzungsvertrags über Camtly (elektronischer Abschluss gemäß Art. 28 Abs. 9 DSGVO).

1. Gegenstand und Dauer

1.1 Gegenstand ist die Bereitstellung der SaaS-Anwendung Camtly. **Wichtig:** Die Inhalte der vom Verantwortlichen konvertierten Umsatzdateien (Transaktions-/Mandantendaten) werden ausschließlich lokal im Browser des Verantwortlichen verarbeitet und erreichen die Systeme des Auftragsverarbeiters nicht; sie sind nicht Gegenstand dieser Auftragsverarbeitung.

1.2 Auftragsverarbeitung im Sinne dieses Vertrags betrifft die serverseitig im Auftrag des Verantwortlichen gespeicherten Daten, insbesondere die vom Verantwortlichen angelegten Mandanten-Stammdaten (z. B. Mandantenname, Mandantennummer, Karten-Zuordnungen) sowie Nutzerdaten von Teammitgliedern, die der Verantwortliche anlegt. Konto-, Organisations- und Abrechnungsdaten verarbeitet der Auftragsverarbeiter als eigener Verantwortlicher (siehe Datenschutzerklärung).

1.3 Die Dauer entspricht der Laufzeit des Nutzungsvertrags.

1.4 Sollten Inhalte der Umsatzdateien im Einzelfall dennoch an den Auftragsverarbeiter gelangen (z. B. versehentlich im Rahmen des Supports oder durch eine Fehlfunktion), gelten die Pflichten dieses AVV und der Verschwiegenheitsvereinbarung für diese Daten entsprechend; der Auftragsverarbeiter wird solche Daten unverzüglich löschen und den Verantwortlichen informieren.

2. Art, Zweck, Datenkategorien, betroffene Personen

Zweck: Bereitstellung, Betrieb und Support der Anwendung.

Art der Verarbeitung: Speicherung, Anzeige, Übermittlung an den berechtigten Nutzer, Löschung.

Datenkategorien: Stammdaten (Name, E-Mail), Zugangsdaten (Passwort-Hash, Session-Daten), Organisationsdaten, Mandanten-Stammdaten, Abrechnungsdaten.

Betroffene Personen: Mitarbeiter des Verantwortlichen; Mandanten des Verantwortlichen (nur Stammdaten, keine Transaktionsdaten).

3. Weisungsrecht

Der Auftragsverarbeiter verarbeitet die Daten ausschließlich auf dokumentierte Weisung des Verantwortlichen (regelmäßig: durch Nutzung der Anwendung), sofern nicht Unionsrecht oder deutsches Recht die Verarbeitung verlangen; in diesem Fall informiert er den Verantwortlichen vor der Verarbeitung, sofern rechtlich zulässig. Hält der Auftragsverarbeiter eine Weisung für rechtswidrig, informiert er den Verantwortlichen unverzüglich.

4. Vertraulichkeit

Zur Verarbeitung befugte Personen sind zur Vertraulichkeit verpflichtet und über die besonderen Pflichten (einschließlich § 203 StGB, siehe [Verschwiegenheitsvereinbarung](#)) belehrt.

5. Technische und organisatorische Maßnahmen (Art. 32 DSGVO)

Architektur-Maßnahme (zentral): Client-seitige Verarbeitung der Umsatzdaten — die sensibelsten Daten verlassen das Endgerät des Verantwortlichen nicht (Datenminimierung by design, Art. 25 DSGVO).

Transportverschlüsselung (TLS) für sämtliche Verbindungen; HSTS.

Verschlüsselung der Datenbank im Ruhezustand (AES-256, EU-Rechenzentrum Frankfurt).

Zugriffskonzept nach dem Prinzip der geringsten Berechtigung (dedizierte Dienstkonten, Secret-Management, rollenbasierte Zugriffe in der Anwendung).

Passwort-Speicherung ausschließlich als kryptografischer Hash; Session-Ablauf.

Hosting ausschließlich in EU-Rechenzentren (Google Cloud EU, AWS Frankfurt).

Protokollierung sicherheitsrelevanter Ereignisse; regelmäßige Sicherheitsupdates und automatisierte Tests inkl. Prüfung, dass kein Upload-Endpunkt für Umsatzdaten existiert.

Trennung der Kundendaten (Mandantenfähigkeit auf Organisationsebene).

Backups der serverseitigen Datenbank; Wiederherstellungsverfahren.

6. Subauftragsverarbeiter

6.1 Der Verantwortliche erteilt die allgemeine Genehmigung zum Einsatz der folgenden Subauftragsverarbeiter:

Subauftragsverarbeiter	Leistung	Ort der Verarbeitung
Google Cloud EMEA Limited (Irland)	Hosting/Betrieb der Anwendung	EU (Region Belgien)
Supabase Pte. Ltd. (Singapur; US-Konzerngesellschaft Supabase, Inc.)	Datenbank	AWS Frankfurt am Main (DE); Support ggf. Drittland (SCC)
Scaleway SAS (Frankreich)	Versand von Konto-E-Mails (z. B. E-Mail-Bestätigung, Passwort zurücksetzen)	EU (Frankreich)

Hinweis: Die Zahlungsabwicklung über Stripe erfolgt in eigener datenschutzrechtlicher Verantwortung des Anbieters (siehe Datenschutzerklärung Ziffer 6) und ist nicht Gegenstand dieses AVV.

6.2 Über beabsichtigte Änderungen (Hinzuziehen/Ersetzen) informiert der Auftragsverarbeiter mindestens vier Wochen vorab in Textform; der Verantwortliche kann aus wichtigem Grund widersprechen. Mit jedem Subauftragsverarbeiter bestehen Verträge mit gleichwertigen Datenschutzpflichten; bei Drittlandbezug bestehen geeignete Garantien (Art. 44 ff. DSGVO).

7. Unterstützungspflichten

Der Auftragsverarbeiter unterstützt den Verantwortlichen mit geeigneten Maßnahmen bei der Erfüllung von Betroffenenrechten (Art. 12-23 DSGVO) sowie bei den Pflichten aus Art. 32-36 DSGVO (Sicherheit, Meldung von Verletzungen, Datenschutz-Folgenabschätzung), soweit ihm dies möglich ist.

8. Meldung von Verletzungen

Verletzungen des Schutzes personenbezogener Daten, die die Auftragsdaten betreffen, meldet der Auftragsverarbeiter dem Verantwortlichen unverzüglich und stellt die nach Art. 33 Abs. 3 DSGVO erforderlichen Informationen bereit.

9. Löschung und Rückgabe

Nach Vertragsende werden die Auftragsdaten nach Wahl des Verantwortlichen herausgegeben (Datenexport) und anschließend gelöscht, soweit keine gesetzliche Aufbewahrungspflicht besteht. Die Löschung wird auf Verlangen bestätigt.

10. Nachweise und Kontrollen

Der Auftragsverarbeiter stellt dem Verantwortlichen alle erforderlichen Informationen zum Nachweis der Einhaltung dieses Vertrags zur Verfügung (insbesondere Beschreibungen der TOMs und vorhandene Zertifikate/Testate der Rechenzentrums-Anbieter) und ermöglicht — nach rechtzeitiger Ankündigung, während üblicher Geschäftszeiten, ohne unverhältnismäßige Betriebsstörung — Überprüfungen einschließlich Inspektionen.

11. Haftung; Schlussbestimmungen

Für die Haftung gilt Ziffer 12 der [AGB](#); Art. 82 DSGVO bleibt unberührt. Bei Widersprüchen zwischen diesem AVV und den AGB geht in Bezug auf die Verarbeitung personenbezogener Daten dieser AVV vor. Es gilt deutsches Recht.