Vertrag zur Auftragsverarbeitung (AVV)

Stand: 06.11.2026

Dieser AVV gilt für alle Verarbeitungsvorgänge, bei denen Locitup personenbezogene Daten von Endkunden oder Store-Mitarbeitern im Auftrag der jeweiligen Organisation verarbeitet. Verarbeitungsvorgänge, bei denen CoaSoft eigenständiger Verantwortlicher ist (z. B. B2B-Dashboard-Kontoführung, Stripe-Abrechnung, eigene Marketing-Website), werden durch unsere allgemeine Datenschutzerklärung geregelt.

Präambel und Vertragsschluss

(1) Dieser Vertrag zur Auftragsverarbeitung („AVV“) wird zwischen der CoaSoft - Consulting & Software UG (haftungsbeschränkt), Am Wäldchen 24, 66424 Homburg, Deutschland („Auftragsverarbeiter“, „Locitup“) und dem jeweiligen gewerblichen Kunden („Verantwortlicher“ oder „Kunde“) geschlossen.

(2) Der AVV konkretisiert die datenschutzrechtlichen Verpflichtungen der Parteien im Rahmen der Nutzung der mobilen Stempelkarten-Plattform Locitup (einschließlich Händler-Dashboard, Store-Staff-Modus und API) und ergänzt den bestehenden Hauptvertrag bzw. die Allgemeinen Geschäftsbedingungen (AGB).

(3) Der AVV kann rechtswirksam elektronisch abgeschlossen werden, insbesondere durch Bestätigung im Registrierungs- und Onboarding-Prozess des Händler-Dashboards oder durch elektronische Annahme eines entsprechenden Vertragsangebots.

§ 1 Gegenstand, Dauer und Rangfolge

(1) Gegenstand dieses AVV ist die Bereitstellung der Softwareplattform Locitup zur Ausgabe, Verwaltung und Entwertung digitaler Stempelkarten, Einlöse-Prämien, städteweiter Rallyes sowie der Zuweisung von Store-Personal zur Abwicklung von Scans vor Ort im Auftrag des Kunden.

(2) Die Laufzeit richtet sich nach der Dauer des Hauptvertrages. Gesetzliche oder vertraglich vereinbarte Aufbewahrungs- und Nachweispflichten bleiben über das Vertragsende hinaus unberührt.

(3) Bei Widersprüchen zwischen diesem AVV und sonstigen Vereinbarungen der Parteien gehen die Bestimmungen dieses AVV in datenschutzrechtlichen Fragen vor.

§ 2 Rollenabgrenzung

(1) Der Kunde ist Verantwortlicher im Sinne von Art. 4 Nr. 7 DSGVO für die im Rahmen des Treueprogramms verarbeiteten Daten seiner Endkunden und seines Filialpersonals. Locitup verarbeitet diese Daten als Auftragsverarbeiter gemäß Art. 28 DSGVO streng weisungsgebunden.

(2) Handelt CoaSoft für eigene Zwecke (z. B. Verifikation von Unternehmensstammdaten, Rechnungslegung gegenüber dem Händler, systemübergreifende Missbrauchsüberwachung oder Auslieferung der Marketing-Landingpage), agiert CoaSoft als eigenständiger Verantwortlicher.

(3) Die Einbindung des Zahlungsdienstleisters Stripe dient der Begleichung von Händlergebühren (B2B) und unterliegt gesonderten Bedingungen von Stripe; Transaktionszahlungen von Endkunden finden über Locitup nicht statt.

§ 3 Einzelheiten der Verarbeitung

Umfang, Art und Zweck der Datenverarbeitung, die Kategorien personenbezogener Daten sowie die Kreise betroffener Personen sind verbindlich in Anlage 1 festgelegt.

§ 4 Weisungsgebundenheit

(1) Locitup verarbeitet Daten ausschließlich auf dokumentierte Weisung des Kunden, einschließlich hinsichtlich etwaiger Datenübermittlungen in Drittländer, es sei denn, Locitup ist durch Unionsrecht oder nationales Recht hierzu verpflichtet.

(2) Die Weisungen werden primär durch die Konfiguration und Aktionen autorisierter Händler-Accounts im Dashboard (z. B. Anlegen von Stempelkarten, Einladen von Scannern, Entwerten von Prämien) erteilt.

(3) Ist Locitup der Ansicht, dass eine erteilte Weisung gegen Datenschutzvorschriften verstößt, wird der Kunde unverzüglich informiert. Locitup ist berechtigt, die Ausführung auszusetzen, bis der Kunde die Weisung bestätigt oder anpasst.

§ 5 Pflichten des Auftragsverarbeiters

Locitup gewährleistet:

- die Einhaltung des Grundsatzes der Vertraulichkeit durch alle zur Verarbeitung befugten Personen;
- die Umsetzung und fortlaufende Überprüfung angemessener technischer und organisatorischer Maßnahmen (TOM);
- die Unterstützung des Kunden bei Anfragen betroffener Personen nach Kapitel III DSGVO;
- die unverzügliche Meldung von Datenschutzverletzungen nach Kenntnisnahme;
- die Unterstützung bei Datenschutz-Folgenabschätzungen (Art. 35 DSGVO) und behördlichen Konsultationen;
- die vertragsgemäße Rückgabe oder Löschung aller Auftragsdaten nach Vertragsbeendigung.

§ 6 Pflichten des Kunden

(1) Der Kunde ist allein verantwortlich für die Rechtmäßigkeit der Datenerhebung gegenüber seinen Store-Kunden und Filialmitarbeitern sowie für die Erfüllung der Informationspflichten (Art. 13, 14 DSGVO).

(2) Besondere Kategorien personenbezogener Daten (Art. 9 DSGVO) dürfen über Locitup nicht verarbeitet werden.

§ 7 Technische und organisatorische Maßnahmen (TOM)

Locitup trifft alle erforderlichen Sicherheitsmaßnahmen nach Art. 32 DSGVO. Die konkreten Maßnahmen sind in Anlage 2 verbindlich geregelt. Sicherheitsrelevante Anpassungen sind zulässig, sofern das vertraglich vereinbarte Schutzniveau nicht unterschritten wird.

§ 8 Unterauftragsverarbeiter (Subprozessoren)

(1) Der Kunde erteilt die allgemeine schriftliche Genehmigung zum Einsatz von Unterauftragsverarbeitern. Die bei Vertragsschluss genehmigten Dienstleister sind in Anlage 3 aufgeführt.

(2) Locitup informiert den Kunden mindestens 14 Tage vor dem beabsichtigten Wechsel oder der Hinzuziehung eines Unterauftragsverarbeiters in Textform. Der Kunde kann aus sachlichen datenschutzrechtlichen Gründen innerhalb der Frist widersprechen.

(3) Den Unterauftragsverarbeitern werden dieselben Pflichten auferlegt, die für Locitup nach diesem AVV gelten.

§ 9 Drittlandübermittlungen

Finden Übermittlungen an Empfänger außerhalb der EU/des EWR statt, stellt Locitup sicher, dass die Garantien der Art. 44 ff. DSGVO (insbesondere das EU-U.S. Data Privacy Framework oder EU-Standardvertragsklauseln) eingehalten werden.

§ 10 Audits und Nachweise

Locitup stellt dem Kunden alle erforderlichen Nachweise zur Einhaltung von Art. 28 DSGVO bereit. Vor-Ort-Audits sind mit einer Frist von mindestens 14 Tagen während üblicher Betriebszeiten anzukündigen und dürfen Geschäftsgeheimnisse sowie Daten Dritter nicht

gefährden.

§ 11 Meldung von Datenschutzverletzungen

Locitup informiert den Kunden unverzüglich über bekannt gewordene Verletzungen des Schutzes personenbezogener Auftragsdaten und liefert die für Meldungen nach Art. 33, 34 DSGVO erforderlichen Angaben (Art des Vorfalls, Kategorien Betroffener, Gegenmaßnahmen).

§ 12 Beendigung, Löschung und Backups

(1) Nach Vertragsende löscht Locitup die im Auftrag verarbeiteten Kundendaten innerhalb von 30 Tagen aus den aktiven Systemen, sofern keine gesetzlichen Aufbewahrungsfristen entgegenstehen.

(2) Daten in automatisierten Sicherungskopien werden im Rahmen des rollierenden Backup-Zyklus nach spätestens 90 Tagen endgültig überschrieben.

§ 13 Schlussbestimmungen

Es gilt deutsches Recht. Sollten einzelne Klauseln unwirksam sein, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt.

Anlage 1 Beschreibung der Datenverarbeitung

Gegenstand & Zweck

Bereitstellung des digitalen Treue- und Stempelprogramms Locitup, Ausgabe von Stempeln via QR-Code, Einlösung von Belohnungen, Gamification-Fortschritte (XP, Badges) sowie Verwaltung von Filialpersonal.

Dauer

Laufzeit des Hauptvertrages zuzüglich der technisch vorgesehenen Löschfristen (30 Tage / Backups 90 Tage).

Kategorien betroffener Personen

Endkunden und App-Nutzer der Stores; Filialpersonal, Scanner und Shop-Mitarbeiter des Händlers.

Kategorien personenbezogener Daten

Kunden-ID (userId), Karten-ID (cardId), Stempelzähler, Einlöse-Tokens (gehasht via tokenHash), E-Mail-Adressen (bei Gast-Stempeln GuestStampClaim), Mitarbeiter-Rollen (SCANNER, STAFF, MANAGER) sowie flüchtige Store-Standortzuordnungen.

Anlage 2 Technische und organisatorische Maßnahmen (TOM)

- Verschlüsselung: Durchgehende HTTPS/TLS-Transportverschlüsselung aller API-Routen sowie Ruhedatenverschlüsselung (AES-256) der Datenbank.
- Mandantentrennung: Logische Trennung aller Händlerdaten auf Datenbankebene über Row Level Security (RLS) in PostgreSQL/Supabase.
- Zugriffskontrollen: Strikte rollenbasierte Autorisierung (RBAC) – Scanner-Accounts haben keinen Zugriff auf Abrechnungs- oder Vorlagendaten.
- Token-Sicherheit: Gültigkeitsbegrenzung von Einlöse-QR-Tokens auf maximal 10 Minuten und sofortige serverseitige Entwertung gegen Replay-Angriffe.
- Logging-Hygiene: Vollständige Maskierung sensibler Anfragedaten vor der Protokollierung in Cloud Logging.

Anlage 3 Unterauftragsverarbeiter (Subprozessoren)

Supabase, Inc. | PostgreSQL-Datenbank, Identitätsverwaltung, Session-Tokens (JWT) | Frankfurt am Main (Deutschland / EU) | AVV nach Art. 28 DSGVO; Standardvertragsklauseln (SCCs)

Google Cloud Platform / Firebase (Google Cloud EMEA Ltd. / Google Ireland Ltd.) | Cloud Run Hosting der API, Firebase Hosting (Dashboard, Staff-Portal), Server-Logging | Europäische Union (Belgien); weltweites CDN für Firebase Hosting | Cloud Data Processing Addendum; zertifiziert nach EU-U.S. Data Privacy Framework (DPF)

Cloudflare, Inc. (Turnstile) | Bot- und Missbrauchsschutz bei Login, Registrierung und Code-Anforderung im Dashboard und Staff-Portal | USA | AVV; EU-U.S. Data Privacy Framework (DPF) sowie Standardvertragsklauseln (SCCs)

Brevo (Sendinblue SAS) | Versand transaktionaler E-Mails (Anmeldecodes, Einladungen von Mitarbeitern, Benachrichtigungen) | Frankreich / Europäische Union | AVV; Serverstandort innerhalb der EU

Hinweis zur Rollenabgrenzung von Zahlungsdiensten: Stripe Payments Europe, Ltd. wird für die Abrechnung von B2B-Händlergebühren eingesetzt und agiert bezüglich der Zahlungsvorgänge als eigenständiger Verantwortlicher. Da über Locitup keine Zahlungen der Store-Endkunden abgewickelt werden, ist Stripe nicht als Unterauftragsverarbeiter für Endkundendaten einzuordnen.