

Auftragsverarbeitungsvertrag (AVV)

Die Anlagen 1 bis 3 sind Bestandteil dieses Vertrags; die Anlagen 2 und 3 werden als eigenständige Dokumente geführt.

1 Parteien, Vertragsgegenstand und Rangfolge

Auftraggeber / Verantwortlicher: das im Hauptvertrag bezeichnete Kundenunternehmen (nachfolgend „Auftraggeber“). Auftragsverarbeiter: LavaLoft UG (haftungsbeschränkt), Am Kirchweg 29, 06188 Landsberg, Deutschland; Amtsgericht Stendal, HRB 36977; USt-IdNr. DE460693748. Geschäftsführer: Matthias Maier und Christopher Gansert. Datenschutz- und Sicherheitskontakt: teams@lavaloft.de. Operativer Ansprechpartner: Christopher Gansert, Co-Founder & COO. Dieser Vertrag ergänzt den SaaS- oder Pilotvertrag. Er regelt die Verarbeitung personenbezogener Daten durch LavaLoft im Auftrag des Kunden. Im Fall von Widersprüchen gehen zwingende datenschutzrechtliche Bestimmungen dieser AVV vor. Die Rollenverteilung ist für jede konkrete Verarbeitung anhand der tatsächlichen Zwecke zu beurteilen; eigene Verantwortlichkeit von LavaLoft etwa für Vertrags- und Abrechnungsdaten bleibt unberührt.

2 Dauer, Art und Zweck der Verarbeitung

Die Auftragsverarbeitung beginnt mit der Bereitstellung der vereinbarten Leistungen und dauert bis zur Beendigung des Hauptvertrags einschließlich der geregelten Rückgabe- und Löschvorgänge. LavaLoft ruft CRM-Daten ab, strukturiert, verknüpft, analysiert und zeigt sie an, speichert erforderliche Daten, protokolliert technische Vorgänge und verarbeitet diese zur algorithmischen Erkennung und Bearbeitung von Vertriebsprozessfehlern, Pipeline- und Forecast-Analysen, Aufgaben- und Callback-Management sowie Nutzerverwaltung und Betrieb. LavaLoft setzt nach der aktuellen Produktangabe für die Fehlererkennung keine KI-Modelle ein.

Nur bei entsprechender Freigabe durch den Auftraggeber können CRM-Datensätze im vereinbarten Funktionsumfang erstellt oder verändert werden. Umfang und konkrete Integrationen ergeben sich aus Anlage 1 und den dokumentierten Kundeneinstellungen.

3 Betroffene Personen

Beschäftigte und autorisierte Nutzer des Auftraggebers, Vertriebsmitarbeiter, Teamleiter und Administratoren; bestehende und potenzielle Geschäftskontakte sowie deren Ansprechpartner; Teilnehmer aktivierter Kalenderintegrationen; Absender und Empfänger geschäftlicher E-Mails bei aktivierter Mailintegration; weitere Personen, die in CRM-Datensätzen oder Freitextfeldern des Auftraggebers erfasst sind.

4 Kategorien personenbezogener Daten

- a) Deal-/Opportunity-Stammdaten: Name, Stage, Pipeline, Wert, Erstell- und Abschlussdatum, Wahrscheinlichkeit, Status, Datensatz-ID und Owner-ID.
- b) Deal-Verlauf: letzte Aktivität, nächster Schritt, Änderungen des Abschlussdatums, Stage-Wechsel und Zeitstempel.
- c) Kontakte: Name, geschäftliche E-Mail, Kontakt-ID und Unternehmenszuordnung.
- d) Unternehmen: Firmenname und ID, soweit personenbezogen.

- e) Aufgaben: Betreff, Beschreibung, Status, Priorität, Typ, Fälligkeit, Zeitstempel und Zuständigkeit.
- f) Meetings: Titel, Zeiten, Ort, Beschreibung, Outcome, Teilnehmer, zuständiger Benutzer und interne Meeting-Notizen (u. a. `hs_internal_meeting_notes`).
- g) Calls: Titel, Zeitstempel, Status, Dauer, zuständiger Benutzer und vorhandene Protokollfelder; keine pauschale Zusage zum Ausschluss von Aufzeichnungen ohne gesonderte technische Prüfung.
- h) Notizen: Text, Zeitstempel, Ersteller und Zuordnung (u. a. `hs_note_body`).
- i) CRM-Benutzer: Name, geschäftliche E-Mail, Benutzer-ID, Rolle und Aktivstatus.
- j) Kalender bei Aktivierung: Titel, Beginn/Ende, Ort, Teilnehmer, Beschreibung, Antwortstatus und Termin-ID.
- k) E-Mail bei Aktivierung: Absender, Betreff, Header-/Metadaten, Zeitstempel, Lesestatus, Thread-ID und gegebenenfalls Vorschau/Snippet (Outlook `bodyPreview`; Gmail Metadatenmodus nach aktueller Beschreibung).
- l) LavaLoft-Callbacks: Prospect-Name, Unternehmen, Grund, Notizen, Termin und Zusatzfelder.
- m) LavaLoft-Konten und Integration: Name, geschäftliche E-Mail, Firebase UID, Team, Rolle, Login-/Nutzungszeitpunkte und OAuth-Tokens.
- n) Nutzung und Interaktionen: Deal-Öffnungen, Callback-Ergebnisse, Nutzeraktionen, Reaktionszeiten und Aggregatwerte, soweit personenbezogen.

5 Berechtigungen und dokumentierte Weisungen

LavaLoft verarbeitet die für den vereinbarten Funktionsumfang erforderlichen CRM-Daten mit lesendem Zugriff. Bei der Verbindung können Kunden optionale OAuth-Schreibberechtigungen auswählen oder weglassen. Zusätzlich kann der Kunde Schreibfunktionen innerhalb der LavaLoft-Anwendung ein- oder ausschalten. Ohne aktivierte Schreibfunktionen werden keine CRM-Datensätze durch LavaLoft verändert. Bereits erteilte OAuth-Scopes werden durch eine Deaktivierung innerhalb der Anwendung nicht zwingend technisch widerrufen; die Anwendung unterbindet dann die entsprechenden Schreiboperationen. Der Hauptvertrag, die aktivierten Integrationen, gespeicherte Funktionseinstellungen und weitere dokumentierte Anweisungen bilden die Weisungsgrundlage. LavaLoft informiert den Auftraggeber, wenn eine Weisung nach eigener Auffassung gegen Datenschutzrecht verstößt, soweit gesetzlich zulässig.

6 Freitexte und besondere Datenkategorien

LavaLoft wertet Freitexte (z. B. Notizen, Meeting- und Aufgabenbeschreibungen sowie Callback-Notizen) nach der Produktbeschreibung nicht gezielt inhaltlich für die algorithmische Fehlererkennung aus. Die Prüfungen erfolgen primär auf Metadatenebene; Freitexte können dennoch in autorisierten Oberflächen angezeigt und gespeichert werden. Eine automatische Filterung besonderer Kategorien personenbezogener Daten nach Art. 9 DSGVO beim CRM-Import findet derzeit nicht statt. Die gezielte Verarbeitung solcher Daten ist nicht Gegenstand der vereinbarten Leistung. Der Auftraggeber stellt die Rechtmäßigkeit seiner Eingaben und Weisungen sicher und weist seine Nutzer entsprechend an. Die Schutz-, Vertraulichkeits- und Unterstützungspflichten von LavaLoft bleiben bestehen. Eine generelle Pseudonymisierung sämtlicher angezeigter Freitexte wird nicht zugesichert.

7 Pflichten des Auftragsverarbeiters

LavaLoft verarbeitet personenbezogene Daten nur auf dokumentierte Weisung des Auftraggebers, außer bei zwingender gesetzlicher Verpflichtung; in diesem Fall informiert LavaLoft den Auftraggeber vorab, soweit rechtlich zulässig. Befugte Personen sind auf Vertraulichkeit verpflichtet. LavaLoft trifft die in Anlage 2 beschriebenen angemessenen Maßnahmen gemäß Art. 32 DSGVO, unterstützt den Auftraggeber bei der

Einhaltung der Art. 32 bis 36 DSGVO unter Berücksichtigung der verfügbaren Informationen und weist auf nach eigener Auffassung rechtswidrige Weisungen hin. Eine Verarbeitung für eigene Zwecke ist von diesem Vertrag nicht gedeckt.

8 Datenschutzverletzungen und Betroffenenrechte

LavaLoft informiert den Auftraggeber unverzüglich nach Bekanntwerden einer Verletzung des Schutzes personenbezogener Daten gemäß Art. 33 Abs. 2 DSGVO und stellt verfügbare Angaben zur Art des Vorfalls, betroffenen Daten und ergriffenen Maßnahmen bereit; fehlende Informationen werden nachgereicht. Kontakt: teams@lavaloft.de. Betroffenenanfragen, die sich auf die Auftragsverarbeitung beziehen und unmittelbar an LavaLoft gerichtet werden, werden unverzüglich an den Auftraggeber weitergeleitet; eine eigenständige inhaltliche Antwort erfolgt vorbehaltlich gesetzlicher Pflichten nicht. LavaLoft unterstützt auf dokumentierte Anforderung durch CSV-Export von Teamdaten oder JSON-Export von Einzelprofilen grundsätzlich innerhalb von 10 Arbeitstagen; Datensatz-/Einzelbenutzerlöschungen nach Weisung grundsätzlich innerhalb von 30 Kalendertagen; ferner durch angemessene Auskunft zu Zugriffen und Unterstützung bei Berichtigung oder Einschränkung. Gesetzliche Dringlichkeiten bleiben unberührt.

9 Unterauftragsverarbeiter und internationale Übermittlungen

Der Auftraggeber erteilt eine allgemeine Genehmigung für die in Anlage 3 aufgeführten Unterauftragsverarbeiter, soweit diese tatsächlich personenbezogene Daten im Auftrag von LavaLoft verarbeiten. LavaLoft informiert über beabsichtigte Hinzuziehungen oder Ersetzungen rechtzeitig vor deren Wirksamwerden und ermöglicht begründete Einwände. Bei Einwänden bemühen sich die Parteien um eine angemessene Lösung; zwingende Rechte bleiben unberührt. LavaLoft verpflichtet Unterauftragsverarbeiter zu den nach Art. 28 Abs. 4 DSGVO erforderlichen Pflichten und bleibt dem Auftraggeber gegenüber verantwortlich. Die eingesetzten Unterauftragsverarbeiter der SaaS-Leistung sind in Anlage 3 aufgeführt: Google Cloud/Firebase, Cloudflare, Brevo und Resend. Drittlandtransfers sind nur unter Beachtung von Kapitel V DSGVO zulässig; konkrete Empfänger, Standorte und Transfergrundlagen sind in Anlage 3 festzuhalten. Die Verbindung eines CRM-Anbieters durch den Auftraggeber begründet nicht automatisch dessen Stellung als Unterauftragsverarbeiter von LavaLoft.

10 Nachweise und Audits

LavaLoft stellt dem Auftraggeber die zur Überprüfung der Einhaltung der datenschutzrechtlichen Verpflichtungen erforderlichen Informationen zur Verfügung. Hierzu gehören insbesondere die technischen und organisatorischen Maßnahmen sowie die relevanten Sicherheits- und Datenschutzunterlagen. Überprüfungen erfolgen grundsätzlich zunächst anhand der bereitgestellten Dokumentation. Soweit weitergehende Prüfungen erforderlich sind, ermöglicht LavaLoft diese einschließlich Inspektionen durch den Auftraggeber oder einen von ihm beauftragten Prüfer. Die Durchführung wird grundsätzlich mit angemessener Vorankündigung abgestimmt. Dabei sind die Vertraulichkeit, die Sicherheit der Systeme sowie die Rechte anderer Kunden zu berücksichtigen. Die gesetzlichen Kontrollrechte gemäß Art. 28 Abs. 3 lit. h DSGVO bleiben unberührt.

11 Rückgabe, Löschung und Aufbewahrung

Nach Beendigung der Verarbeitung gibt LavaLoft die im Auftrag verarbeiteten personenbezogenen Daten nach Wahl des Auftraggebers zurück oder löscht diese, sofern keine gesetzliche Aufbewahrungspflicht entgegensteht. Rückgabe erfolgt nach abgestimmtem Verfahren in geeignetem maschinenlesbarem Format, insbesondere CSV und für Einzelprofile gegebenenfalls JSON. Die Löschung aus aktiven Kundensystemen erfolgt grundsätzlich spätestens innerhalb von 30 Kalendertagen nach Vertragsende, sofern keine zulässige abweichende Weisung besteht. Die Löschung aktiver Mandantendaten kann administrativ ausgelöst werden.

Auf Anfrage bestätigt LavaLoft die Löschung. Bei Trennung einer CRM-, Kalender- oder Mailintegration werden die zugehörigen OAuth-Tokens unverzüglich aus der aktiven Firestore-Datenbank entfernt. Die Löschung in Sicherungskopien folgt den technischen Rotationsfristen: Point-in-Time-Recovery 7 Tage, tägliche Firestore-Backups 98 Tage. Backups dienen der Wiederherstellung; im Wiederherstellungsfall sind bereits gelöschte Datensätze erneut zu entfernen. Anwendungslogs im Bucket _Default werden 30 Tage und Logs im Bucket _Required 400 Tage aufbewahrt. Für weitere Log-Buckets gelten die jeweils konfigurierten Fristen; das interne Incident-Register wird nach Bereinigung oder spätestens 12 Monate nach Resolve-Status gelöscht. Soweit gesetzliche Aufbewahrungspflichten bestehen, bleiben nur die betroffenen Daten im erforderlichen Umfang gespeichert.

12 Schlussbestimmungen

Dieser Vertrag gilt ab beidseitiger Unterzeichnung und ergänzt den Hauptvertrag. Änderungen und Ergänzungen bedürfen der Textform, soweit keine strengere gesetzliche Form gilt. Unwirksame Einzelbestimmungen lassen die Wirksamkeit der übrigen Bestimmungen unberührt. Es gilt deutsches Recht; zwingende datenschutzrechtliche Vorschriften bleiben unberührt. Gerichtsstand ist, soweit gesetzlich zulässig, der Sitz der LavaLoft UG (haftungsbeschränkt). Auftraggeber: _____ Ort/Datum:

_____ Unterschrift: _____ LavaLoft UG (haftungsbeschränkt):
_____ Ort/Datum: _____ Unterschrift: _____

Anlage 1 – Integrationen und Verarbeitungsvorgänge

HubSpot: Deals, Kontakte, Unternehmen, Aufgaben, Meetings, Calls und Notizen; optionale Schreibfunktionen nach kundenseitiger Autorisierung. Salesforce, Pipedrive und Microsoft Dynamics 365: CRM-Objekte, Aktivitäten, Benutzer- und Pipelineinformationen nach aktivierter Integration; Schreibaktionen ausschließlich im freigegebenen Funktionsumfang. Weitreichende technische OAuth-Scopes, insbesondere Microsoft Dynamics user_impersonation, begründen keine pauschale Erlaubnis zu beliebigen Änderungen. Google Calendar und Outlook Calendar: Kalendertermine und Teilnehmerdaten nur bei aktivierter Integration. Gmail und Outlook Mail: E-Mail-Metadaten, gegebenenfalls Snippets und Vorschautexte nur bei aktivierter Integration.

LavaLoft-Funktionen: CRM-Fehlerprüfung, Aufgaben- und Callback-Verwaltung, Analyse, Nutzerkonten und Autorisierung. Firestore und Cloud Functions werden in europe-west3 (Frankfurt) betrieben; für die produktive Verarbeitung ist europe-west3 (Frankfurt) konfiguriert. Firebase Authentication kann abweichende technische Verarbeitungsorte haben.

Technische Zugriffsrechte sind jeweils durch die tatsächlich erteilten OAuth-Berechtigungen und die kundenseitig aktivierten Funktionen begrenzt. Die vollständige, aktuelle technische Scope-Liste ist als operative Dokumentation zu führen.

Anlage 2 – Technische und organisatorische Maßnahmen (separates Dokument)

Die verbindlichen TOMs werden als eigenständige Anlage beigelegt. Dokumentierte Maßnahmen: Google-Cloud-Verschlüsselung gespeicherter Daten (AES-256), TLS 1.2 oder höher, IAM-Service-Accounts für serverseitige Zugriffe, Firestore Security Rules für Client-SDK-Zugriffe, beschränkter Adminzugriff mit 2FA, Cloud Audit Logs, Firestore PITR und tägliche Backups sowie Cloudflare als vorgeschaltete Schutzschicht. OAuth-Refresh-Tokens werden derzeit nicht zusätzlich durch eine LavaLoft-eigene Application-Layer-Verschlüsselung geschützt; Google Cloud entschlüsselt berechtigten Zugriff transparent. Cloudflare cached nach aktueller Konfiguration ausschließlich statische, nicht personenbezogene Inhalte. Das Monitoring erfolgt derzeit manuell, nicht als zugesicherte 24/7-Alarmierung.

Anlage 3 – Unterauftragsverarbeiter (separates Dokument)

Die aktuelle Liste der Unterauftragsverarbeiter mit jeweiligem Vertragsunternehmen, Zweck, Verarbeitungsort und gegebenenfalls Drittlandtransfergrundlage wird als gesonderte Anlage beigelegt. Erfasste Anbieter: Google Cloud/Firebase, Cloudflare, Brevo und Resend. IONOS wird ausschließlich für die Website und Domainverwaltung genutzt und ist kein Unterauftragsverarbeiter der SaaS-Leistung.