

Informationen zur Datenverarbeitung und Datensicherheit

LavaLoft Security Center · Stand: 17. Oktober 2026

1 Zweck und Einordnung

LavaLoft unterstützt B2B-Vertriebsteams dabei, Fehler und versäumte Aktivitäten in bestehenden CRM-Systemen zu erkennen und zu bearbeiten. Dieses Dokument erläutert die Verarbeitung von Daten bei der Nutzung der LavaLoft-Anwendung. Es ergänzt den Auftragsverarbeitungsvertrag (AVV), die technischen und organisatorischen Maßnahmen (TOMs) und die Liste der Unterauftragsverarbeiter. Es ersetzt weder die AVV noch die Datenschutzerklärung für Verarbeitungen in eigener Verantwortlichkeit von LavaLoft.

2 Verantwortlichkeiten und Kontakt

Für die vom Kunden bereitgestellten CRM-Daten ist grundsätzlich das Kundenunternehmen Verantwortlicher im Sinne der DSGVO; LavaLoft verarbeitet diese Daten als Auftragsverarbeiter nach dokumentierten Weisungen. Für eigene Vertrags-, Abrechnungs- und gegebenenfalls eigenständige Sicherheits- und Kommunikationsverarbeitungen kann LavaLoft selbst Verantwortlicher sein. Die konkrete Rolle hängt vom jeweiligen Verarbeitungsvorgang ab.

Anbieter: LavaLoft UG (haftungsbeschränkt), Am Kirchweg 29, 06188 Landsberg, Deutschland.

Datenschutz- und Sicherheitskontakt: teams@lavaloft.de.

3 Welche Daten können verarbeitet werden?

Je nach CRM-Anbindung und aktivierten Funktionen verarbeitet LavaLoft insbesondere Deal- und Opportunity-Daten (z. B. Name, Phase, Wert, Abschlussdatum, Status, zuständige Person), Kontakte und Unternehmenszuordnungen, Aufgaben und Aktivitäten, Meeting- und Call-Metadaten, Notizen und Beschreibungen, Benutzer- und Rolleninformationen sowie technische Integrationsdaten einschließlich OAuth-Tokens. Bei aktivierten Kalender- oder E-Mail-Integrationen können Termin-, Teilnehmer-, Betreff-, Header- und sonstige in der AVV beschriebenen Metadaten hinzukommen. Die konkreten Kategorien sind in Anlage 1 der AVV aufgeführt.

Freitextfelder können personenbezogene oder vom Kunden eingegebene sensible Informationen enthalten.

LavaLoft filtert besondere Kategorien personenbezogener Daten nach Art. 9 DSGVO beim Import nicht automatisch heraus. Die Fehlererkennung erfolgt primär anhand von Regeln und Metadaten, nicht durch eine gezielte inhaltliche Auswertung sämtlicher Freitexte.

4 Pipeline-Scanner und vollständige Anwendung

Pipeline-Scanner: Der Pipeline-Scanner verwendet ausschließlich lesenden CRM-Zugriff. Die für die Analyse abgerufenen Daten werden temporär verarbeitet und anschließend gelöscht; durch den Scanner werden keine CRM-Datensätze verändert. Eine konkrete, technisch bestätigte Löschfrist für die temporären Scanner-Daten liegt für diese Information noch nicht vor. Daher wird keine feste Stunden- oder Tagesfrist zugesichert.

Vollständige LavaLoft-Anwendung: CRM-Daten können im vereinbarten Umfang gespeichert, analysiert und angezeigt werden. Schreiboperationen in verbundene CRM-Systeme erfolgen nur, wenn der Kunde entsprechende Berechtigungen erteilt und die Funktionen innerhalb von LavaLoft aktiviert hat. Das Deaktivieren einer Schreibfunktion innerhalb der Anwendung widerruft nicht automatisch zuvor beim CRM-Anbieter gewährte OAuth-Berechtigungen.

Integrationsberechtigungen: Der tatsächliche Umfang der OAuth-Scopes und Datenfelder hängt von Anbieter, Integration und Konfiguration ab. Eine vollständige technische Scope-Inventur für sämtliche Integrationen wurde zum Stand dieses Dokuments nicht bestätigt. Deshalb enthält dieses Dokument keine abschließende Liste aller produktiven OAuth-Berechtigungen.

5 Analyseverfahren und KI

Die Erkennung von Vertriebsprozessfehlern erfolgt nach der aktuellen Produktbeschreibung regel- bzw.

algorithmusbasiert. Für diese Fehlererkennung werden keine externen KI-Modelle eingesetzt. Aus den hier beschriebenen Verarbeitungsvorgängen wird keine generelle Aussage über sämtliche denkbaren zukünftigen Funktionen abgeleitet.

6 Hosting, Dienstleister und internationale Übermittlungen

Die wesentliche Verarbeitung und Speicherung von CRM-Anwendungsdaten erfolgt in Google Cloud, insbesondere über Cloud Firestore und Cloud Functions in der konfigurierten Region europe-west3 (Frankfurt). Firebase Authentication sowie Betriebs-, Support- und Sicherheitsfunktionen können abweichende Verarbeitungsorte aufweisen. Eine ausschließliche Verarbeitung sämtlicher Daten innerhalb Deutschlands oder der EU wird nicht zugesichert.

Als Unterauftragsverarbeiter werden Google Cloud/Firebase, Cloudflare, Brevo und Resend eingesetzt. Cloudflare schützt als Reverse Proxy die Anwendung und kann technisch durchgeleitete Anfragen und Inhalte verarbeiten.

Brevo versendet transaktionale Einladungs- und Bestätigungs-E-Mails, Resend technische E-Mails wie Passwortzurücksetzungen; an diese E-Mail-Dienste werden nach aktueller Produktangabe Name und E-Mail-Adresse, jedoch keine CRM-Inhalte übermittelt. IONOS wird nur für die öffentliche Website und Domain eingesetzt und gehört nicht zur CRM-Auftragsverarbeitung.

Internationale Datenübermittlungen werden nach den einschlägigen Vorgaben von Kapitel V DSGVO behandelt. Je nach Anbieter und Übermittlung kommen EU-Standardvertragsklauseln und – soweit die jeweilige Zertifizierung und der Übermittlungsvorgang erfasst sind – das EU-U.S. Data Privacy Framework zum Einsatz. Die Einzelheiten und offiziellen Anbieterquellen stehen in Anlage 3 der AVV.

7 Speicherdauer, Exporte und Löschung

Während der Vertragslaufzeit werden die für die vereinbarten Funktionen erforderlichen Daten verarbeitet. Nach Vertragsende werden Kundendaten grundsätzlich innerhalb von 30 Tagen aus aktiven Systemen gelöscht, sofern keine gesetzliche Pflicht oder zulässige abweichende Weisung entgegensteht. Einzelne personenbezogene Daten werden auf dokumentierte Weisung innerhalb von 30 Kalendertagen gelöscht. Vorhandene Teamdaten können als CSV exportiert werden; ein personenbezogener JSON-Export wird nach schriftlicher Anforderung innerhalb von zehn Arbeitstagen bereitgestellt.

Für Firestore besteht eine Point-in-Time-Recovery-Aufbewahrung (PITR) von sieben Tagen; tägliche Sicherungen werden regulär spätestens nach 98 Tagen entfernt. Google Cloud Logging verwendet für den Bucket _Default 30 Tage und für _Required 400 Tage; bei anderen Buckets gelten deren Konfigurationen. Ein

internes Incident-Register wird spätestens zwölf Monate nach Abschluss eines Vorfalls bereinigt. Diese Fristen betreffen unterschiedliche Datenarten und dürfen nicht als einheitliche Aufbewahrungsdauer aller CRM-Daten verstanden werden.

8 Technische und organisatorische Schutzmaßnahmen

LavaLoft setzt unter anderem rollenbasierte Zugriffssteuerung, Authentifizierung und Zwei-Faktor-Schutz für administrative Zugänge, Verschlüsselung bei Übertragung und Speicherung, logische Mandantentrennung, Backups, Protokollierung, einen Prozess für Sicherheitsvorfälle sowie interne Sicherheitsprüfungen ein. Der konkrete Stand, bestehende Einschränkungen und Wiederherstellungsmaßnahmen sind in Anlage 2 (TOMs) beschrieben. Eine ISO-27001-Zertifizierung oder ein automatisiertes 24/7-Sicherheitsmonitoring wird nicht behauptet.

9 Betroffenenrechte und Sicherheitsvorfälle

Anfragen zu personenbezogenen CRM-Daten sind grundsätzlich an das verantwortliche Kundenunternehmen zu richten. LavaLoft unterstützt den Kunden gemäß AVV bei der Bearbeitung von Betroffenenrechten und informiert ihn bei Verletzungen des Schutzes personenbezogener Daten unverzüglich nach Bekanntwerden entsprechend Art.

33 Abs. 2 DSGVO. Sicherheitsanfragen können an teams@lavaloft.de gerichtet werden.

10 Ergänzende Dokumente

Zum Security Center gehören der Auftragsverarbeitungsvertrag (AVV) einschließlich Anlage 1, die technischen und organisatorischen Maßnahmen (Anlage 2) und die Liste der Unterauftragsverarbeiter (Anlage 3). Diese Dokumente sind gemeinsam zu lesen. Die konkreten Downloadlinks werden im Security Center bereitgestellt.

Dokumentenstand und technische Grenzen

Dieses Informationsdokument basiert auf den von LavaLoft bestätigten Produkt- und Betriebsangaben zum 17.10.2026. Die vollständige produktive OAuth-Scope-Liste ist noch nicht technisch inventarisiert; eine exakte Frist für die Löschung temporärer Pipeline-Scanner-Daten ist nicht bestätigt. Die Angaben sollten bei Änderungen der Produktkonfiguration aktualisiert werden.

Maßgeblich für vertragliche Rechte und Pflichten sind die geschlossenen Vereinbarungen einschließlich AVV.