

# Technische und organisatorische Maßnahmen

Auftragsverarbeiter: LavaLoft UG (haftungsbeschränkt), Am Kirchweg 29, 06188 Landsberg, Deutschland · Amtsgericht Stendal, HRB 36977 · Geschäftsführer: Matthias Maier und Christopher Gansert · Datenschutz- und Sicherheitskontakt: teams@lavaloft.de.

Diese Anlage beschreibt die nach Angaben von LavaLoft eingerichteten technischen und organisatorischen Maßnahmen gemäß Art. 32 DSGVO für die Verarbeitung personenbezogener Kundendaten im Rahmen der LavaLoft-Leistungen. Die Maßnahmen werden risikobasiert überprüft und bei Bedarf angepasst. Diese Anlage ist gemeinsam mit der AVV und ihren übrigen Anlagen zu lesen.

## 1 Zutritts- und Endgerätesicherheit

Geschäftsräume sind abschließbar; Zutritt erhalten nur berechtigte Personen. Jeder Geschäftsführer nutzt ein eigenes persönliches macOS-Benutzerkonto. Geschäftliche Endgeräte sind mit Passwort oder PIN, automatischer Bildschirmsperre und Festplattenverschlüsselung geschützt. Die integrierten macOS-Sicherheitsfunktionen, insbesondere XProtect und Gatekeeper, werden eingesetzt. Betriebssysteme, Browser und sicherheitsrelevante Software werden regelmäßig aktualisiert; Sicherheitsupdates werden zeitnah installiert.

## 2 Zugangs- und Berechtigungskontrolle

Administrative Zugriffe auf Google Cloud, Firebase und GitHub erfolgen über individuelle Konten mit Zwei-Faktor-Authentifizierung (2FA). Das GitHub-Repository ist privat. Zugriffsberechtigungen werden regelmäßig auf Erforderlichkeit überprüft und nicht mehr benötigte Rechte entzogen. Die beiden Geschäftsführer verfügen derzeit jeweils über administrative Berechtigungen und können im Rahmen ihrer Rolle auf Kundendaten zugreifen. Die serverseitige Anwendungslogik nutzt Google-Cloud-Service-Accounts und Identity and Access Management (IAM); für Client-SDK-Zugriffe werden Firestore Security Rules eingesetzt.

Bei Ausscheiden einer berechtigten Person werden geschäftliche Zugänge spätestens zum Ende des letzten Arbeitstages deaktiviert, persönliche Tokens widerrufen, aktive Sitzungen beendet und Berechtigungen entfernt. Ein Geschäftsführer überprüft und dokumentiert die Durchführung. Bei Verdacht auf eine Kompromittierung können betroffene Konten sofort gesperrt und Tokens/Sitzungen widerrufen werden.

## 3 Mandantentrennung und Vertraulichkeit

Kundendaten werden anwendungsseitig logisch nach Mandanten getrennt. Die Trennung wird für kundenseitige Zugriffe, serverseitige Cloud Functions, Exporte und Cache-Zugriffe berücksichtigt. Dedizierte automatisierte Negativtests zur Überprüfung mandantenübergreifender Zugriffsmöglichkeiten sind derzeit nicht als eigenständige Kontrollmaßnahme eingerichtet. Beide Geschäftsführer haben schriftliche Vertraulichkeits- und Datenschutzverpflichtungen unterzeichnet.

## 4 Verschlüsselung und geschützte Übertragung

Für die Übertragung von Daten werden verschlüsselte Verbindungen mit TLS 1.2 oder höher eingesetzt. Daten in Google Cloud werden im Rahmen der eingesetzten Cloud-Dienste standardmäßig verschlüsselt gespeichert (Google-verwaltete Schlüssel; AES-256). OAuth-Zugriffs- und Refresh-Tokens werden serverseitig in Firestore gespeichert. Eine zusätzliche, von LavaLoft selbst implementierte anwendungsseitige Verschlüsselung der

Refresh-Tokens ist derzeit nicht eingerichtet. Zugriffe werden durch IAM, Authentifizierung und Berechtigungen beschränkt.

## **5 Netzwerk- und Anwendungsschutz**

Cloudflare ist als vorgeschaltete Schutzschicht für öffentliche Webdomains und die Anwendung eingebunden, unter anderem für TLS-Terminierung, DDoS-Schutz und die Blockierung bekannter schädlicher IP-Adressen. Nach aktueller Konfiguration werden ausschließlich statische, nicht personenbezogene Inhalte gecacht. Als Reverse Proxy kann Cloudflare jedoch technische Verbindungsdaten und übertragene Anfragen verarbeiten; dies ist bei der Unterauftragsverarbeiter- und Drittlandbewertung zu berücksichtigen.

## **6 Entwicklungs-, Test- und Freigabeprozess**

Produktive Kundendaten werden ausschließlich in der Produktivumgebung verarbeitet. Für die getrennte Staging-Umgebung werden nur Testdaten verwendet. Vor Produktiv-Releases erfolgen Code-Review und Tests. Zusätzlich wird die Anwendung mindestens einmal monatlich intern manuell auf Sicherheitsprobleme geprüft; Abhängigkeiten und Schwachstellen werden manuell kontrolliert und erforderliche Sicherheitskorrekturen vorgenommen. Automatisierte Schwachstellenscans und externe Penetrationstests sind derzeit nicht als bestehende Maßnahmen ausgewiesen.

## **7 Sicherung, Verfügbarkeit und Wiederherstellung**

Für Firestore sind tägliche Backups mit einer Aufbewahrungsdauer von 98 Tagen sowie eine Point-in-Time-Recovery (PITR) über sieben Tage eingerichtet. Die Wiederherstellung erfolgt im Bedarfsfall manuell. Die erfolgreiche Wiederherstellung aus einem Backup wurde getestet. Ein gesonderter schriftlicher Disaster-Recovery- bzw. Wiederherstellungsplan besteht derzeit nicht; konkrete Wiederanlaufzeiten oder Wiederherstellungspunkte werden durch diese Anlage nicht zugesichert.

## **8 Protokollierung, Kontrolle und Monitoring**

Google Cloud Logging wird für technische Anwendungs- und Fehlermeldungen verwendet (reguläre Aufbewahrung nach interner Angabe: 30 Tage). Cloud Audit Logs dokumentieren administrative und technische Aktivitäten. Die Aufbewahrung beträgt für den Log-Bucket \_Default 30 Tage und für den Log-Bucket \_Required 400 Tage. Für weitere Buckets gelten die jeweils konfigurierten Fristen. Ein internes Incident-Register in Firestore erfasst Sicherheitsereignisse und deren Bearbeitung; Einträge werden nach interner Regel spätestens zwölf Monate nach Abschluss entfernt. CRM-Nutzdaten werden nicht gezielt in Anwendungslogs protokolliert. Es besteht keine gesonderte lückenlose Protokollierung jedes lesenden Administratorzugriffs auf einzelne CRM-Datensätze. Die Kontrolle erfolgt derzeit durch manuelle Dashboard-Prüfungen, nicht durch zugesichertes automatisiertes 24/7-Sicherheitsmonitoring.

## **9 Behandlung von Sicherheits- und Datenschutzvorfällen**

LavaLoft verwendet einen internen Ablauf: (1) Vorfall erkennen und bewerten, (2) gegebenenfalls Zugänge sperren und Auswirkungen eindämmen, (3) Sachverhalt, Zeitpunkte, Auswirkungen und Maßnahmen im Incident-Register dokumentieren, (4) betroffene Auftraggeber bei einer Verletzung des Schutzes personenbezogener Daten unverzüglich nach Bekanntwerden gemäß Art. 33 Abs. 2 DSGVO informieren und bei deren Pflichten unterstützen, (5) Ursache beheben und vorbeugende Maßnahmen festhalten. Zuständig sind die Geschäftsführer Matthias Maier und Christopher Gansert; Kontakt: teams@lavaloft.de. Die behördliche Meldepflicht des Verantwortlichen bleibt unberührt.

## **10 Datenminimierung, Integrationen und Weisungsbindung**

LavaLoft verarbeitet CRM-Daten und gegebenenfalls aktivierte Kalender- bzw. E-Mail-Metadaten nur im für die vertraglichen Funktionen erforderlichen Umfang. Die Fehlererkennung erfolgt regel- bzw. algorithmusbasiert; hierfür werden nach aktuellem Produktstand keine externen KI-Modelle eingesetzt. Freitextfelder können im berechtigten Produktzugriff sichtbar sein und auch vom Kunden eingetragene sensible Inhalte enthalten; eine automatische Erkennung oder Filterung besonderer Datenkategorien findet nicht statt.

Der Pipeline-Check erfolgt lesend. Schreiboperationen in angeschlossene CRM-Systeme werden nur im kundenseitig autorisierten und in der Anwendung aktivierten Funktionsumfang ausgelöst. Aktivierte Funktionen und Entscheidungen werden gespeichert. Das Deaktivieren einer Funktion verhindert entsprechende Anwendungsaktionen, widerruft jedoch nicht zwingend bereits gewährte OAuth-Scopes beim jeweiligen Anbieter. Bei Trennung einer Integration werden die aktiven OAuth-Zugriffs- und Refresh-Tokens gelöscht; Sicherungskopien laufen entsprechend den Backup-Fristen aus.

## **11 Rückgabe, Löschung und Unterstützung von Betroffenenrechten**

Kunden können vorhandene Teamdaten als CSV exportieren; ein personenbezogener JSON-Export wird nach schriftlicher Anforderung innerhalb von zehn Arbeitstagen bereitgestellt. Die Löschung einzelner personenbezogener Daten auf dokumentierte Weisung erfolgt innerhalb von 30 Kalendertagen. Nach Vertragsende werden Kundendaten entsprechend der AVV aus aktiven Systemen grundsätzlich innerhalb von 30 Tagen gelöscht, soweit keine rechtliche Pflicht oder abweichende zulässige Weisung entgegensteht. Die vollständige Löschung eines Kundenkontos samt zugehörigen CRM-Daten aus aktiven Systemen wurde erfolgreich getestet.

In Sicherungen verbleibende Daten werden im regulären Sicherungszyklus spätestens nach 98 Tagen entfernt; PITR-Daten laufen nach sieben Tagen aus. Bei einer Wiederherstellung aus Sicherungen werden zwischenzeitlich ausgeführte Löschungen erneut berücksichtigt. Direkt bei LavaLoft eingehende Betroffenenanfragen werden dem zuständigen Auftraggeber zur Bearbeitung zugeordnet; LavaLoft unterstützt im Rahmen der AVV.

## **12 Dienstleister, Verarbeitungsorte und Überprüfung**

Die wesentliche Anwendungsdatenverarbeitung über Firestore und Cloud Functions erfolgt nach aktueller technischer Beschreibung in Google-Cloud-Region europe-west3 (Frankfurt). Für die produktive Verarbeitung ist europe-west3 (Frankfurt) konfiguriert. Für Firebase Authentication und weitere Dienstleister kann eine Verarbeitung außerhalb Deutschlands erfolgen. Die jeweils aktuelle Liste der eingesetzten Unterauftragsverarbeiter einschließlich Aufgaben, Standorten und gegebenenfalls Drittlandgarantien wird gesondert als Anlage 3 geführt.

LavaLoft überprüft die Angemessenheit seiner Sicherheitsmaßnahmen regelmäßig sowie bei wesentlichen Änderungen oder Sicherheitsvorfällen. Informationen zur Einhaltung der Maßnahmen werden dem Auftraggeber nach Maßgabe der AVV und Art. 28 Abs. 3 lit. h DSGVO zur Verfügung gestellt.

### **Hinweise zur abschließenden Freigabe**

Diese Fassung basiert auf den von LavaLoft beschriebenen technischen und organisatorischen Abläufen. Vor rechtsverbindlicher Veröffentlichung sind insbesondere die tatsächliche Konfiguration von Audit-Log-Aufbewahrungen, die bestätigte Region europe-west3 (Frankfurt) und die Datenverarbeitung bei Firebase Authentication, die Nachweise zur monatlichen Prüfung sowie die Übereinstimmung mit AVV, Datenschutzhinweisen und Unterauftragsverarbeiterliste zu verifizieren. Eine rechtliche Prüfung wird empfohlen.