CANLIO LEGAL CENTER

Canlio Security Whitepaper

Technische und organisatorische Sicherheitsuebersicht fuer Canlio.

VERSION	GÜLTIG AB	AKTUALISIERT
1.0	**2026-07-13**	**2026-07-13**

Version 1.0

Stand: Juli 2026

Einleitung

Dieses Security Whitepaper beschreibt die Sicherheitsarchitektur der Plattform **Canlio** sowie die organisatorischen und technischen Maßnahmen der **Can Lead GmbH** zum Schutz von Kunden-, Unternehmens- und Systemdaten.

Es richtet sich insbesondere an

- IT-Abteilungen,
- Informationssicherheitsbeauftragte,
- Datenschutzbeauftragte,
- Compliance-Verantwortliche,
- Enterprise-Kunden,
- Auditoren,
- sowie technische Ansprechpartner.

Dieses Dokument ergänzt insbesondere die

- Security Policy,
- Privacy Policy,
- Data Processing Agreement (AVV),
- Service Level Agreement,
- Responsible AI Policy,
- sowie sämtliche weiteren Sicherheitsdokumente der Can Lead GmbH.

Sicherheitsphilosophie

Informationssicherheit ist Bestandteil sämtlicher Entwicklungs- und Betriebsprozesse der Plattform Canlio.

Unsere Sicherheitsstrategie basiert insbesondere auf den Grundprinzipien

- Security by Design
- Privacy by Design
- Least Privilege
- Zero Trust
- Defense in Depth
- Secure Defaults
- Continuous Monitoring
- Continuous Improvement

Sicherheitsmaßnahmen werden bereits während der Planung neuer Funktionen berücksichtigt und kontinuierlich an neue technische sowie regulatorische Anforderungen angepasst.

Plattformarchitektur

Canlio wird als cloudbasierte Enterprise-SaaS-Plattform betrieben.

Die Architektur besteht aus logisch voneinander getrennten Komponenten, insbesondere

- Web Frontend
- Kundenportal
- API-Ebene
- Authentifizierungsdienste
- Backend-Services
- KI-Komponenten
- Datenbanken
- Hintergrundprozessen (Worker)
- Speicherlösungen
- Monitoring
- Logging
- Backup-Infrastruktur
- Administrationssystemen

Die einzelnen Komponenten können unabhängig voneinander aktualisiert, überwacht und skaliert werden.

Mandantentrennung

Canlio ist mandantenfähig entwickelt.

Die Daten verschiedener Kunden werden logisch voneinander getrennt verarbeitet.

Zugriffe erfolgen ausschließlich nach erfolgreicher Authentifizierung sowie einer Berechtigungsprüfung.

Administratoren erhalten ausschließlich diejenigen Rechte, die für ihre jeweilige Aufgabe erforderlich sind.

Eine unberechtigte Einsicht in Daten anderer Kunden ist durch technische und organisatorische Maßnahmen ausgeschlossen.

Sichere Softwareentwicklung

Die Entwicklung von Canlio folgt einem strukturierten Softwareentwicklungsprozess.

Hierzu gehören insbesondere

- Code Reviews,
- Versionskontrolle,
- Freigabeprozesse,
- Testumgebungen,
- Qualitätssicherung,
- automatisierte Tests,
- Regressionstests,
- Sicherheitsprüfungen,
- Dependency Management,
- sowie dokumentierte Release-Prozesse.

Vor der Bereitstellung produktiver Änderungen erfolgen angemessene technische Prüfungen entsprechend der Art und Komplexität der jeweiligen Änderung.

Authentifizierung

Der Zugriff auf Canlio erfolgt ausschließlich über authentifizierte Benutzerkonten.

Je nach Leistungsumfang können unter anderem eingesetzt werden

- sichere Passwortrichtlinien,
- Multi-Faktor-Authentifizierung,
- rollenbasierte Berechtigungen,
- Sitzungsverwaltung,
- Gerätevalidierung,
- Token-basierte Authentifizierung,
- API-Schlüssel,
- OAuth-Verfahren,
- sowie weitere moderne Authentifizierungsmechanismen.

Authentifizierungsverfahren werden regelmäßig überprüft und an den Stand der Technik angepasst.

Autorisierung

Der Zugriff auf Funktionen und Daten erfolgt ausschließlich auf Grundlage eines rollenbasierten Berechtigungskonzepts.

Hierbei gilt der Grundsatz:

So viele Rechte wie erforderlich – so wenige Rechte wie möglich.

Administrative Berechtigungen werden ausschließlich autorisierten Personen gewährt.

Berechtigungen können jederzeit angepasst, eingeschränkt oder entzogen werden.

Netzwerk- und Infrastruktursicherheit

Zum Schutz der Plattform setzt die Can Lead GmbH geeignete technische Sicherheitsmaßnahmen ein.

Hierzu können insbesondere gehören

- Firewalls,
- Netzwerksegmentierung,
- verschlüsselte Kommunikation,
- Zugriffsbeschränkungen,
- DDoS-Schutz,
- Sicherheitsfilter,
- Intrusion Detection,

- Anomalieerkennung,
- Netzwerkmonitoring,
- Infrastrukturüberwachung,
- sowie weitere dem Stand der Technik entsprechende Schutzmechanismen.

Die konkrete technische Ausgestaltung wird kontinuierlich überprüft und bei Bedarf angepasst.

Verschlüsselung und Schlüsselmanagement

Der Schutz vertraulicher Informationen erfolgt durch den Einsatz zeitgemäßer kryptographischer Verfahren entsprechend dem Stand der Technik.

Canlio verfolgt das Ziel, personenbezogene Daten, Unternehmensinformationen und sicherheitsrelevante Systemdaten sowohl während der Übertragung als auch während der Speicherung angemessen gegen unbefugte Zugriffe zu schützen.

Datenübertragung

Die Kommunikation zwischen

- Browser und Plattform,
- API und Backend,
- internen Diensten,
- Integrationen,
- mobilen Anwendungen,
- sowie weiteren Systemkomponenten

erfolgt grundsätzlich ausschließlich über verschlüsselte Verbindungen.

Nicht verschlüsselte Verbindungen können – soweit technisch möglich – automatisch auf sichere Kommunikationswege umgeleitet oder blockiert werden.

Speicherung von Daten

Je nach Art der gespeicherten Informationen können insbesondere verschlüsselt gespeichert werden:

- personenbezogene Daten,
- Zugangsinformationen,
- Authentifizierungstoken,

- API-Schlüssel,
- Systemkonfigurationen,
- Sicherungskopien,
- Protokolldaten,
- vertrauliche Projektdaten,
- sowie weitere sicherheitsrelevante Informationen.

Passwörter werden grundsätzlich nicht im Klartext gespeichert.

Schlüsselmanagement

Kryptographische Schlüssel werden getrennt von den eigentlichen Nutzdaten verwaltet.

Die Can Lead GmbH verfolgt hierbei insbesondere folgende Grundsätze:

- Zugriff ausschließlich für autorisierte Systeme,
- Least-Privilege-Prinzip,
- dokumentierte Verwaltungsprozesse,
- regelmäßige Überprüfung,
- kontrollierte Rotation sicherheitsrelevanter Schlüssel,
- sowie Schutz vor unberechtigtem Zugriff.

Backup- und Wiederherstellungsstrategie

Datensicherung ist ein zentraler Bestandteil der Sicherheitsarchitektur von Canlio.

Zur Minimierung möglicher Datenverluste werden geeignete Sicherungsverfahren eingesetzt.

Hierzu können insbesondere gehören:

- regelmäßige Datenbanksicherungen,
- Systembackups,
- Konfigurationssicherungen,
- Infrastrukturbackups,
- Versionshistorien,
- Snapshot-Technologien,
- sowie weitere Sicherungsverfahren.

Die Wiederherstellbarkeit wird regelmäßig überprüft.

Backups dienen ausschließlich der Wiederherstellung produktiver Systeme und werden nicht für andere Zwecke verwendet.

Business Continuity und Disaster Recovery

Die Can Lead GmbH verfolgt das Ziel, den Geschäftsbetrieb auch bei außergewöhnlichen Ereignissen möglichst schnell wiederherzustellen.

Hierzu bestehen organisatorische und technische Prozesse für den Umgang mit

- Hardwareausfällen,
- Infrastrukturstörungen,
- Cloud-Ausfällen,
- Netzwerkproblemen,
- Cyberangriffen,
- Datenverlusten,
- Stromausfällen,
- Softwarefehlern,
- sowie weiteren außergewöhnlichen Ereignissen.

Je nach Art des Vorfalls können insbesondere folgende Maßnahmen eingeleitet werden:

- Aktivierung interner Notfallprozesse,
- Wiederherstellung aus Sicherungskopien,
- Infrastrukturmigration,
- Fehlerbehebung,
- temporäre Ausweichlösungen,
- Priorisierung kritischer Systeme,
- sowie weitere Maßnahmen zur Wiederaufnahme des Betriebs.

Logging und Monitoring

Zur Sicherstellung eines sicheren Plattformbetriebs werden sicherheits- und betriebsrelevante Ereignisse protokolliert.

Hierzu können insbesondere gehören:

- Anmeldungen,
- fehlgeschlagene Anmeldungen,
- Berechtigungsänderungen,

- API-Zugriffe,
- Systemfehler,
- Performanceereignisse,
- Sicherheitswarnungen,
- Infrastrukturereignisse,
- Änderungen administrativer Einstellungen,
- sowie weitere sicherheitsrelevante Vorgänge.

Die Protokollierung dient insbesondere

- der Fehleranalyse,
- der Angriffserkennung,
- der Missbrauchsprävention,
- der Nachvollziehbarkeit,
- der IT-Sicherheit,
- sowie der kontinuierlichen Verbesserung unserer Plattform.

Schwachstellenmanagement

Die Can Lead GmbH überprüft ihre Plattform regelmäßig auf mögliche Sicherheitsrisiken.

Hierzu gehören insbesondere

- Sicherheitsupdates,
- Dependency-Prüfungen,
- Codeanalysen,
- Sicherheitsbewertungen,
- Schwachstellenanalysen,
- Konfigurationsprüfungen,
- sowie kontinuierliche technische Verbesserungen.

Bekannte Sicherheitslücken werden entsprechend ihrer jeweiligen Risikobewertung priorisiert und im Rahmen definierter interner Prozesse bearbeitet.

Sicherheitsrelevante Aktualisierungen können kurzfristig außerhalb regulärer Release-Zyklen bereitgestellt werden, sofern dies zum Schutz der Plattform erforderlich ist.

Sicherheitsvorfälle (Incident Response)

Die Can Lead GmbH verfügt über strukturierte Prozesse zur Behandlung sicherheitsrelevanter Ereignisse.

Hierzu gehören insbesondere:

- Erkennung,
- Bewertung,
- Priorisierung,
- Dokumentation,
- Eindämmung,
- Ursachenanalyse,
- Wiederherstellung,
- Nachbereitung,
- sowie kontinuierliche Verbesserung der Sicherheitsmaßnahmen.

Je nach Art und Schwere des Vorfalls arbeiten technische, organisatorische und – soweit erforderlich – rechtliche Verantwortliche zusammen, um Auswirkungen möglichst gering zu halten und den ordnungsgemäßen Betrieb der Plattform schnellstmöglich wiederherzustellen.

Soweit gesetzlich erforderlich oder vertraglich vereinbart, werden betroffene Kunden über relevante Sicherheitsvorfälle informiert.

Kontinuierliche Sicherheitsentwicklung

Informationssicherheit ist kein abgeschlossener Zustand, sondern ein fortlaufender Entwicklungsprozess.

Die Can Lead GmbH überprüft regelmäßig ihre Sicherheitsarchitektur, Entwicklungsprozesse, Infrastruktur und organisatorischen Maßnahmen, um neue technische Entwicklungen, regulatorische Anforderungen und aktuelle Bedrohungslagen angemessen zu berücksichtigen.

Unser Ziel besteht darin, Canlio dauerhaft als sichere, vertrauenswürdige und moderne Enterprise-Plattform für Unternehmen zu betreiben und den Schutz der uns anvertrauten Daten kontinuierlich weiterzuentwickeln.

Unternehmensdaten

Can Lead GmbH
Leerer Landstraße 29
26629 Großefehn
Deutschland
Geschäftsführer: Necati Can
Registergericht: Amtsgericht Aurich
HRB: 208028
Website: www.canlio.de