CANLIO LEGAL CENTER

# Security Policy

Sicherheitsgrundsaetze und organisatorische Kontrollen fuer Canlio.

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

## 1. Informationssicherheit als Unternehmensgrundsatz

Die Sicherheit der Plattform **Canlio**, der verarbeiteten Daten sowie der technischen Infrastruktur besitzt für die Can Lead GmbH höchste Priorität. Informationssicherheit ist kein isolierter technischer Bestandteil der Plattform, sondern ein grundlegendes Unternehmensprinzip, das sämtliche Entwicklungs-, Betriebs- und Geschäftsprozesse begleitet.

Die Can Lead GmbH verfolgt das Ziel, Vertraulichkeit, Integrität, Verfügbarkeit und Nachvollziehbarkeit der bereitgestellten Systeme und Daten dauerhaft zu gewährleisten. Hierzu werden organisatorische, technische und vertragliche Maßnahmen eingesetzt, die regelmäßig überprüft und an den Stand der Technik angepasst werden.

Die Sicherheitsarchitektur von Canlio orientiert sich an den Grundprinzipien moderner Cloud-Plattformen und verfolgt insbesondere die Ziele,

- unberechtigte Zugriffe zu verhindern,
- Datenverluste zu vermeiden,
- Manipulationen zu erkennen,
- Systeme vor Angriffen zu schützen,
- Ausfälle frühzeitig zu erkennen,
- Sicherheitsvorfälle nachvollziehbar zu dokumentieren,
- sowie Risiken kontinuierlich zu reduzieren.

Informationssicherheit wird bei der Entwicklung neuer Funktionen von Beginn an berücksichtigt ("Security by Design") und bildet einen festen Bestandteil sämtlicher Entwicklungs- und Betriebsprozesse.

## 2. Organisatorische Sicherheitsmaßnahmen

Die Can Lead GmbH trifft angemessene organisatorische Maßnahmen, um die Sicherheit der Plattform dauerhaft sicherzustellen.

Hierzu gehören insbesondere

- klar definierte Zugriffsberechtigungen,
- rollenbasierte Berechtigungskonzepte,
- dokumentierte Sicherheitsprozesse,
- geregelte Freigabeverfahren,
- Änderungsmanagement,
- Incident-Management,
- Backup-Strategien,
- Wiederherstellungsprozesse,
- interne Sicherheitsrichtlinien,
- sowie regelmäßige Überprüfung sicherheitsrelevanter Prozesse.

Zugriffe auf produktive Systeme werden ausschließlich autorisierten Personen gewährt, soweit dies zur Erfüllung ihrer jeweiligen Aufgaben erforderlich ist.

Die Vergabe administrativer Berechtigungen erfolgt nach dem Grundsatz der minimal erforderlichen Rechte ("Least Privilege Principle").

---

## 3. Technische Sicherheitsmaßnahmen

Zur Sicherstellung eines sicheren Plattformbetriebs können insbesondere folgende technische Maßnahmen eingesetzt werden:

- verschlüsselte Datenübertragung,
- verschlüsselte Datenspeicherung,
- Authentifizierungsverfahren,
- rollenbasierte Zugriffskontrollen,
- Multi-Faktor-Authentifizierung,
- Firewalls,
- Netzwerksegmentierung,
- Intrusion Detection,
- Anomalieerkennung,
- Sicherheitsprotokollierung,
- automatisierte Angriffserkennung,
- DDoS-Schutz,
- Malware-Erkennung,
- Sicherheitsupdates,

- Schwachstellenmanagement,
- Sicherheitsmonitoring,
- sowie weitere dem Stand der Technik entsprechende Schutzmaßnahmen.

Die konkrete technische Umsetzung kann sich im Rahmen der kontinuierlichen Weiterentwicklung der Plattform ändern.

---

## 4. Sicherheitsvorfälle

Die Can Lead GmbH unterhält organisatorische Prozesse zur Erkennung, Bewertung und Bearbeitung sicherheitsrelevanter Ereignisse.

Hierzu gehören insbesondere

- Untersuchung gemeldeter Sicherheitsvorfälle,
- Bewertung möglicher Auswirkungen,
- Einleitung geeigneter Gegenmaßnahmen,
- Wiederherstellung des ordnungsgemäßen Betriebs,
- Ursachenanalysen,
- Dokumentation,
- sowie kontinuierliche Verbesserung der Sicherheitsmaßnahmen.

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

---

## 5. Gemeinsame Verantwortung

Informationssicherheit ist eine gemeinsame Verantwortung der Can Lead GmbH und ihrer Kunden.

Der Kunde verpflichtet sich insbesondere,

- Zugangsdaten vertraulich zu behandeln,
- sichere Passwörter zu verwenden,
- Mehr-Faktor-Authentifizierung zu aktivieren, soweit verfügbar,
- Endgeräte aktuell zu halten,
- Sicherheitsupdates zeitnah einzuspielen,
- unbefugte Zugriffe unverzüglich zu melden,
- sowie sämtliche Sicherheitsrichtlinien der Can Lead GmbH einzuhalten.

Die Can Lead GmbH überprüft ihre Sicherheitsmaßnahmen kontinuierlich und entwickelt diese fortlaufend weiter, um Canlio auch künftig als sichere, vertrauenswürdige und moderne Enterprise-Plattform betreiben zu können.

---

## Unternehmensdaten

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