CANLIO LEGAL CENTER

Encryption Policy

Grundsaetze zur Verschluesselung von Daten bei Uebertragung und Speicherung.

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

1. Zweck

Die **Encryption Policy** beschreibt die Grundsätze der Can Lead GmbH für den Einsatz kryptographischer Verfahren innerhalb der Plattform **Canlio**.

Verschlüsselung ist ein wesentlicher Bestandteil unserer Informationssicherheitsstrategie und dient dem Schutz der Vertraulichkeit, Integrität und Authentizität von Daten während ihrer Übertragung, Speicherung und Verarbeitung.

Diese Richtlinie ergänzt insbesondere die **Security Policy**, das **Security Whitepaper**, das **Data Processing Agreement (AVV)** sowie die **Privacy Policy**.

2. Sicherheitsgrundsätze

Die Can Lead GmbH verfolgt bei der Auswahl und dem Einsatz kryptographischer Verfahren insbesondere folgende Grundsätze:

- Einsatz etablierter kryptographischer Verfahren
- Orientierung am Stand der Technik
- regelmäßige Überprüfung kryptographischer Verfahren
- Schutz kryptographischer Schlüssel
- Trennung von Daten und Schlüsseln
- kontrollierte Schlüsselverwaltung
- regelmäßige Aktualisierung sicherheitsrelevanter Verfahren

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

3. Verschlüsselung bei der Datenübertragung

Die Kommunikation zwischen Clients, APIs, Backend-Systemen und weiteren technischen Komponenten erfolgt grundsätzlich über verschlüsselte Kommunikationsverbindungen.

Dies betrifft insbesondere:

- Website
- Kundenportal
- API-Schnittstellen
- Administratorenzugänge
- Integrationen
- interne Dienste
- Systemkommunikation
- Authentifizierungsdienste

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

4. Verschlüsselung gespeicherter Daten

Je nach Art der Daten können geeignete Verschlüsselungsverfahren für gespeicherte Informationen eingesetzt werden.

Hierzu gehören insbesondere:

- Datenbanken
- Dateispeicher
- Sicherungskopien
- Konfigurationsdaten
- API-Schlüssel
- Zugangsinformationen
- Authentifizierungstoken
- Sitzungsinformationen
- vertrauliche Unternehmensdaten
- personenbezogene Daten

Nicht sämtliche Daten unterliegen denselben Verschlüsselungsverfahren.

Die eingesetzten Maßnahmen richten sich nach Schutzbedarf, technischen Anforderungen und gesetzlichen Vorgaben.

5. Passwortschutz

Passwörter werden grundsätzlich nicht im Klartext gespeichert.

Für die Speicherung von Authentifizierungsinformationen werden geeignete Verfahren eingesetzt, die eine Wiederherstellung des ursprünglichen Passworts verhindern sollen.

Der Zugriff auf Authentifizierungsdaten ist auf autorisierte technische Prozesse beschränkt.

6. Schlüsselmanagement

Kryptographische Schlüssel stellen besonders schützenswerte Informationen dar.

Die Can Lead GmbH verfolgt daher insbesondere folgende Grundsätze:

- getrennte Verwaltung von Schlüsseln und Nutzdaten,
- eingeschränkte Zugriffsrechte,
- dokumentierte Verwaltungsprozesse,
- regelmäßige Überprüfung,
- Rotation sicherheitsrelevanter Schlüssel, soweit erforderlich,
- sowie Schutz vor unbefugter Offenlegung.

Der Zugriff auf kryptographische Schlüssel erfolgt ausschließlich für autorisierte Systeme oder Personen im Rahmen ihrer jeweiligen Aufgaben.

7. Kontinuierliche Weiterentwicklung

Die Can Lead GmbH überprüft regelmäßig die eingesetzten kryptographischen Verfahren unter Berücksichtigung

- neuer wissenschaftlicher Erkenntnisse,
- technischer Entwicklungen,
- gesetzlicher Anforderungen,
- regulatorischer Vorgaben,
- sowie aktueller Bedrohungslagen.

Soweit erforderlich, werden eingesetzte Verfahren, Algorithmen oder Sicherheitsmechanismen angepasst oder ersetzt, um ein angemessenes Schutzniveau dauerhaft sicherzustellen.

Die Verschlüsselung bildet einen wesentlichen Bestandteil unserer Sicherheitsarchitektur und wird kontinuierlich an den Stand der Technik angepasst, um die Vertraulichkeit und Integrität der innerhalb von Canlio verarbeiteten Informationen bestmöglich zu schützen.

Unternehmensdaten

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