

Data Processing Agreement

Auftragsverarbeitungsvereinbarung fuer Kunden, die Canlio als Auftragsverarbeiter einsetzen.

VERSION

1.0

GÜLTIG AB

2026-07-13

AKTUALISIERT

2026-07-13

Präambel

Dieser Auftragsverarbeitungsvertrag ("AVV" oder "Data Processing Agreement") ergänzt die zwischen der **Can Lead GmbH** und dem jeweiligen Kunden geschlossenen **Terms of Service**, individuelle Verträge sowie sämtliche weiteren Vertragsdokumente der Plattform **Canlio**.

Soweit die Can Lead GmbH im Rahmen der Nutzung von Canlio personenbezogene Daten im Auftrag des Kunden verarbeitet und der Kunde hierbei Verantwortlicher im Sinne von Art. 4 Nr. 7 DSGVO ist, schließen die Vertragsparteien diesen Auftragsverarbeitungsvertrag gemäß Art. 28 DSGVO.

Dieser Vertrag gilt automatisch für sämtliche Leistungen der Can Lead GmbH, bei denen eine Auftragsverarbeitung im Sinne der Datenschutz-Grundverordnung vorliegt, sofern keine abweichende schriftliche Vereinbarung getroffen wurde.

1. Vertragsparteien

Verantwortlicher (Controller)

Der jeweilige Kunde der Can Lead GmbH.

Der Kunde entscheidet eigenverantwortlich über Zwecke und Mittel der Verarbeitung personenbezogener Daten innerhalb seiner eigenen Geschäftsprozesse.

Auftragsverarbeiter (Processor)

Can Lead GmbH

Leerer Landstraße 29

26629 Großefehn

Deutschland

Geschäftsführer:

Necati Can

E-Mail:

<info@can-lead.de>

Website:

www.canlio.de

2. Gegenstand der Verarbeitung

Die Can Lead GmbH verarbeitet personenbezogene Daten ausschließlich zur Erbringung der vertraglich vereinbarten Leistungen der Plattform Canlio.

Hierzu gehören insbesondere

- Bereitstellung der SaaS-Plattform,
- Hosting,
- Benutzerverwaltung,
- Kundenportal,
- Projektverwaltung,
- KI-Funktionen,
- Datenverarbeitung,
- Datenspeicherung,
- Datensicherung,
- technische Administration,
- API-Dienste,
- Support,
- Fehleranalyse,
- Sicherheitsmaßnahmen,
- sowie weitere vertraglich vereinbarte Leistungen.

Die Verarbeitung erfolgt ausschließlich nach dokumentierten Weisungen des Kunden, soweit gesetzliche Vorschriften keine abweichende Verarbeitung verlangen.

3. Dauer der Verarbeitung

Die Verarbeitung erfolgt für die Dauer des zugrunde liegenden Vertragsverhältnisses.

Nach Vertragsbeendigung werden personenbezogene Daten entsprechend den vertraglichen Vereinbarungen sowie den gesetzlichen Aufbewahrungspflichten gelöscht oder zurückgegeben, soweit keine gesetzlichen Verpflichtungen einer sofortigen Löschung entgegenstehen.

4. Art der personenbezogenen Daten

Je nach Nutzung der Plattform können insbesondere verarbeitet werden

- Namen,
- E-Mail-Adressen,
- Telefonnummern,
- Unternehmensdaten,
- Rechnungsdaten,
- Ansprechpartner,
- Benutzerinformationen,
- Login-Daten,
- IP-Adressen,
- Nutzungsdaten,
- Kommunikationsdaten,
- Projektdaten,
- Dokumente,
- Dateien,
- Notizen,
- CRM-Daten,
- API-Daten,
- Protokolldaten,
- sowie weitere durch den Kunden innerhalb der Plattform gespeicherte Informationen.

Die konkrete Datenverarbeitung richtet sich ausschließlich nach der tatsächlichen Nutzung der Plattform durch den Kunden.

5. Kategorien betroffener Personen

Die Verarbeitung kann sich insbesondere beziehen auf

- Mitarbeitende des Kunden,
- Administratoren,
- Benutzer der Plattform,

- Interessenten,
 - Kunden,
 - Geschäftspartner,
 - Lieferanten,
 - Ansprechpartner,
 - Bewerber,
 - Websitebesucher,
 - sowie weitere Personen, deren Daten der Kunde innerhalb der Plattform verarbeitet.
-

6. Rechte und Pflichten des Verantwortlichen

Der Kunde bleibt Verantwortlicher im Sinne der DSGVO.

Er trägt insbesondere die Verantwortung dafür,

- dass eine gültige Rechtsgrundlage für die Verarbeitung besteht,
- dass Informationspflichten erfüllt werden,
- dass Betroffenenrechte beachtet werden,
- dass Weisungen rechtmäßig sind,
- sowie dass ausschließlich zulässige personenbezogene Daten verarbeitet werden.

Die Can Lead GmbH ist nicht verpflichtet, jede Weisung rechtlich zu überprüfen.

Erkennt sie jedoch offensichtlich rechtswidrige Weisungen, wird sie den Kunden hierauf hinweisen.

7. Weisungsrecht

Die Can Lead GmbH verarbeitet personenbezogene Daten ausschließlich auf dokumentierte Weisung des Kunden.

Weisungen können insbesondere erfolgen

- über die Funktionen der Plattform,
- schriftlich,
- per E-Mail,
- oder auf sonstigem dokumentierten Kommunikationsweg.

Mündliche Weisungen sind auf Verlangen der Can Lead GmbH unverzüglich in Textform zu bestätigen.

Soweit eine Weisung gegen geltendes Recht verstößt oder offensichtlich datenschutzwidrig erscheint, ist die Can Lead GmbH berechtigt, deren Ausführung bis zur Klärung auszusetzen.

8. Vertraulichkeit und Verpflichtung der Mitarbeitenden

Die Can Lead GmbH gewährleistet, dass sämtliche Personen, die Zugang zu personenbezogenen Daten erhalten, ausschließlich im Rahmen ihrer jeweiligen Aufgaben tätig werden und zur Wahrung der Vertraulichkeit verpflichtet sind.

Alle Mitarbeitenden sowie sonstige für die Can Lead GmbH tätige Personen mit Zugriff auf personenbezogene Daten werden vor Aufnahme ihrer Tätigkeit auf die Vertraulichkeit personenbezogener Daten verpflichtet und regelmäßig hinsichtlich Datenschutz, Informationssicherheit sowie der internen Sicherheitsrichtlinien sensibilisiert.

Der Zugriff auf personenbezogene Daten erfolgt ausschließlich nach dem Need-to-know-Prinzip. Personen erhalten nur diejenigen Berechtigungen, die zur Erfüllung ihrer jeweiligen Aufgaben erforderlich sind.

Die Verpflichtung zur Vertraulichkeit besteht auch nach Beendigung des jeweiligen Beschäftigungs- oder Vertragsverhältnisses fort.

9. Technische und organisatorische Maßnahmen (TOM)

Die Can Lead GmbH trifft geeignete technische und organisatorische Maßnahmen gemäß Art. 32 DSGVO, um personenbezogene Daten unter Berücksichtigung des Stands der Technik, der Implementierungskosten, der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere möglicher Risiken angemessen zu schützen.

Zu den eingesetzten Maßnahmen können insbesondere gehören:

Zutrittskontrolle

- Schutz der Rechenzentrumsinfrastruktur,
- physische Zugangskontrollen,
- Zutrittsberechtigungen,
- Besuchermanagement,
- Videoüberwachung durch Rechenzentrumsbetreiber, soweit eingesetzt.

Zugangskontrolle

- individuelle Benutzerkonten,
- starke Authentifizierungsverfahren,
- Multi-Faktor-Authentifizierung,
- Passwort-Richtlinien,
- Sperrmechanismen,
- Sitzungsverwaltung,
- rollenbasierte Berechtigungen.

Zugriffskontrolle

- Rollen- und Rechtekonzepte,
- Least-Privilege-Prinzip,
- Mandantentrennung,
- Berechtigungsprüfungen,
- administrative Zugriffsbeschränkungen.

Weitergabekontrolle

- verschlüsselte Datenübertragung,
- TLS-gesicherte Kommunikation,
- sichere API-Kommunikation,
- Authentifizierungsmechanismen,
- kontrollierte Exportfunktionen.

Eingabekontrolle

- Protokollierung administrativer Änderungen,
- Audit-Logs,
- Änderungsnachweise,
- Nachvollziehbarkeit sicherheitsrelevanter Aktionen.

Auftragskontrolle

- dokumentierte interne Prozesse,
- Auswahl geeigneter Auftragsverarbeiter,
- vertragliche Verpflichtung sämtlicher Unterauftragsverarbeiter,
- regelmäßige Überprüfung organisatorischer Maßnahmen.

Verfügbarkeitskontrolle

- Datensicherungen,
- Backup-Strategien,
- Wiederherstellungsprozesse,
- Infrastrukturmonitoring,
- Schutz vor Datenverlust,
- Notfallkonzepte.

Trennungsgebot

- logische Trennung von Kundendaten,
- Mandantenfähigkeit,
- getrennte Projektbereiche,
- rollenbasierte Zugriffsbeschränkungen.

Die Can Lead GmbH entwickelt ihre technischen und organisatorischen Maßnahmen kontinuierlich weiter.

Soweit neue Maßnahmen mindestens ein gleichwertiges Sicherheitsniveau gewährleisten, dürfen bestehende Maßnahmen durch technisch oder organisatorisch verbesserte Verfahren ersetzt werden.

10. Unterauftragsverarbeiter

Die Can Lead GmbH ist berechtigt, geeignete Unterauftragsverarbeiter zur Erfüllung ihrer vertraglichen Leistungen einzusetzen.

Hierzu können insbesondere gehören:

- Cloud-Infrastrukturanbieter,
- Hostinganbieter,

- Rechenzentrumsbetreiber,
- E-Mail-Dienstleister,
- Monitoring-Dienstleister,
- Sicherheitsdienstleister,
- Backup-Dienstleister,
- KI-Technologieanbieter,
- Supportsysteme,
- Kommunikationsplattformen,
- sowie weitere technische Dienstleister.

Die Can Lead GmbH verpflichtet sämtliche Unterauftragsverarbeiter vertraglich auf Datenschutz und Informationssicherheit entsprechend Art. 28 DSGVO.

Eine jeweils aktuelle Übersicht der eingesetzten Unterauftragsverarbeiter wird im **Trust Center** oder auf Anfrage zur Verfügung gestellt.

Beabsichtigt die Can Lead GmbH die Hinzunahme oder den Austausch wesentlicher Unterauftragsverarbeiter, wird sie ihre Kunden in angemessener Weise informieren, soweit dies datenschutzrechtlich erforderlich ist.

11. Unterstützung des Verantwortlichen

Die Can Lead GmbH unterstützt den Kunden im angemessenen Umfang bei der Erfüllung seiner gesetzlichen Verpflichtungen nach der DSGVO.

Dies umfasst insbesondere – soweit die jeweilige Verarbeitung betroffen ist –

- Unterstützung bei Betroffenenanfragen,
- Unterstützung bei Datenschutz-Folgenabschätzungen,
- Unterstützung bei der Erfüllung gesetzlicher Meldepflichten,
- Bereitstellung erforderlicher Informationen,
- Unterstützung bei datenschutzrechtlichen Prüfungen,
- sowie Zusammenarbeit mit Datenschutzaufsichtsbehörden, soweit gesetzlich erforderlich.

Die Unterstützung erfolgt unter Berücksichtigung der Art der Verarbeitung sowie der der Can Lead GmbH zur Verfügung stehenden Informationen.

Soweit Unterstützungsleistungen über die gewöhnliche Vertragserfüllung hinausgehen und erheblichen zusätzlichen Aufwand verursachen, ist die Can Lead GmbH berechtigt, hierfür eine angemessene Vergütung entsprechend der jeweils gültigen Preisliste oder einer individuellen Vereinbarung zu verlangen.

8. Vertraulichkeit und Verpflichtung der Mitarbeitenden

Die Can Lead GmbH gewährleistet, dass sämtliche Personen, die Zugang zu personenbezogenen Daten erhalten, ausschließlich im Rahmen ihrer jeweiligen Aufgaben tätig werden und zur Wahrung der Vertraulichkeit verpflichtet sind.

Alle Mitarbeitenden sowie sonstige für die Can Lead GmbH tätige Personen mit Zugriff auf personenbezogene Daten werden vor Aufnahme ihrer Tätigkeit auf die Vertraulichkeit personenbezogener Daten verpflichtet und regelmäßig hinsichtlich Datenschutz, Informationssicherheit sowie der internen Sicherheitsrichtlinien sensibilisiert.

Der Zugriff auf personenbezogene Daten erfolgt ausschließlich nach dem Need-to-know-Prinzip. Personen erhalten nur diejenigen Berechtigungen, die zur Erfüllung ihrer jeweiligen Aufgaben erforderlich sind.

Die Verpflichtung zur Vertraulichkeit besteht auch nach Beendigung des jeweiligen Beschäftigungs- oder Vertragsverhältnisses fort.

9. Technische und organisatorische Maßnahmen (TOM)

Die Can Lead GmbH trifft geeignete technische und organisatorische Maßnahmen gemäß Art. 32 DSGVO, um personenbezogene Daten unter Berücksichtigung des Stands der Technik, der Implementierungskosten, der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere möglicher Risiken angemessen zu schützen.

Zu den eingesetzten Maßnahmen können insbesondere gehören:

Zutrittskontrolle

- Schutz der Rechenzentrumsinfrastruktur,
- physische Zugangskontrollen,
- Zutrittsberechtigungen,
- Besuchermanagement,
- Videoüberwachung durch Rechenzentrumsbetreiber, soweit eingesetzt.

Zugangskontrolle

- individuelle Benutzerkonten,
- starke Authentifizierungsverfahren,

- Multi-Faktor-Authentifizierung,
 - Passwort-Richtlinien,
 - Sperrmechanismen,
 - Sitzungsverwaltung,
 - rollenbasierte Berechtigungen.
-

Zugriffskontrolle

- Rollen- und Rechtekonzepte,
 - Least-Privilege-Prinzip,
 - Mandantentrennung,
 - Berechtigungsprüfungen,
 - administrative Zugriffsbeschränkungen.
-

Weitergabekontrolle

- verschlüsselte Datenübertragung,
 - TLS-gesicherte Kommunikation,
 - sichere API-Kommunikation,
 - Authentifizierungsmechanismen,
 - kontrollierte Exportfunktionen.
-

Eingabekontrolle

- Protokollierung administrativer Änderungen,
 - Audit-Logs,
 - Änderungsnachweise,
 - Nachvollziehbarkeit sicherheitsrelevanter Aktionen.
-

Auftragskontrolle

- dokumentierte interne Prozesse,
- Auswahl geeigneter Auftragsverarbeiter,
- vertragliche Verpflichtung sämtlicher Unterauftragsverarbeiter,
- regelmäßige Überprüfung organisatorischer Maßnahmen.

Verfügbarkeitskontrolle

- Datensicherungen,
- Backup-Strategien,
- Wiederherstellungsprozesse,
- Infrastrukturmonitoring,
- Schutz vor Datenverlust,
- Notfallkonzepte.

Trennungsgebot

- logische Trennung von Kundendaten,
- Mandantenfähigkeit,
- getrennte Projektbereiche,
- rollenbasierte Zugriffsbeschränkungen.

Die Can Lead GmbH entwickelt ihre technischen und organisatorischen Maßnahmen kontinuierlich weiter.

Soweit neue Maßnahmen mindestens ein gleichwertiges Sicherheitsniveau gewährleisten, dürfen bestehende Maßnahmen durch technisch oder organisatorisch verbesserte Verfahren ersetzt werden.

10. Unterauftragsverarbeiter

Die Can Lead GmbH ist berechtigt, geeignete Unterauftragsverarbeiter zur Erfüllung ihrer vertraglichen Leistungen einzusetzen.

Hierzu können insbesondere gehören:

- Cloud-Infrastrukturanbieter,
- Hostinganbieter,
- Rechenzentrumsbetreiber,
- E-Mail-Dienstleister,
- Monitoring-Dienstleister,
- Sicherheitsdienstleister,
- Backup-Dienstleister,
- KI-Technologieanbieter,
- Supportsysteme,

- Kommunikationsplattformen,
- sowie weitere technische Dienstleister.

Die Can Lead GmbH verpflichtet sämtliche Unterauftragsverarbeiter vertraglich auf Datenschutz und Informationssicherheit entsprechend Art. 28 DSGVO.

Eine jeweils aktuelle Übersicht der eingesetzten Unterauftragsverarbeiter wird im **Trust Center** oder auf Anfrage zur Verfügung gestellt.

Beabsichtigt die Can Lead GmbH die Hinzunahme oder den Austausch wesentlicher Unterauftragsverarbeiter, wird sie ihre Kunden in angemessener Weise informieren, soweit dies datenschutzrechtlich erforderlich ist.

11. Unterstützung des Verantwortlichen

Die Can Lead GmbH unterstützt den Kunden im angemessenen Umfang bei der Erfüllung seiner gesetzlichen Verpflichtungen nach der DSGVO.

Dies umfasst insbesondere – soweit die jeweilige Verarbeitung betroffen ist –

- Unterstützung bei Betroffenenanfragen,
- Unterstützung bei Datenschutz-Folgenabschätzungen,
- Unterstützung bei der Erfüllung gesetzlicher Meldepflichten,
- Bereitstellung erforderlicher Informationen,
- Unterstützung bei datenschutzrechtlichen Prüfungen,
- sowie Zusammenarbeit mit Datenschutzaufsichtsbehörden, soweit gesetzlich erforderlich.

Die Unterstützung erfolgt unter Berücksichtigung der Art der Verarbeitung sowie der der Can Lead GmbH zur Verfügung stehenden Informationen.

Soweit Unterstützungsleistungen über die gewöhnliche Vertragserfüllung hinausgehen und erheblichen zusätzlichen Aufwand verursachen, ist die Can Lead GmbH berechtigt, hierfür eine angemessene Vergütung entsprechend der jeweils gültigen Preisliste oder einer individuellen Vereinbarung zu verlangen.

Unternehmensdaten

Can Lead GmbH

Leerer Landstraße 29

26629 Großefehn

Deutschland

Geschäftsführer: Necati Can

Registergericht: Amtsgericht Aurich

HRB: 208028

Website: www.canlio.de