

COREFLOW-AI ROUTENPLANER

Vertrag zur Auftragsverarbeitung (AVV)

Fassung vom 2026-10-09

Coreflow-Ai UG (haftungsbeschränkt)

Tassilostraße 14, 94327 Bogen Amtsgericht Straubing, HRB 13861

Geschäftsführer: Matthias Amann, Daniel Hirschmann USt-IdNr. DE463329986 support@coreflow-ai.de

Präambel/Parteien

- (1) Dieser Vertrag zur Auftragsverarbeitung („**AVV**“) besteht zwischen dem Kunden, der den Coreflow-Ai Routenplaner („**Routenplaner**“) bestellt hat, als Verantwortlichem im Sinne des Art. 4 Nr. 7 DSGVO („**Kunde**“), und der Coreflow-Ai UG (haftungsbeschränkt), Tassilostraße 14, 94327 Bogen, eingetragen im Handelsregister des Amtsgerichts Straubing unter HRB 13861, vertreten durch die Geschäftsführer Matthias Amann und Daniel Hirschmann, als Auftragsverarbeiter im Sinne des Art. 4 Nr. 8 DSGVO („**Coreflow**“).
- (2) Der AVV konkretisiert die datenschutzrechtlichen Rechte und Pflichten der Parteien aus dem Nutzungsvertrag über den Routenplaner, der auf Grundlage der Allgemeinen Geschäftsbedingungen von Coreflow („**AGB**“) geschlossen wurde („**Hauptvertrag**“). Begriffe, die in § 1 Abs. 3 AGB bestimmt sind — insbesondere „Nutzer“, „Inhaber-Konto“, „Mandantendaten“, „Abrechnungszeitraum“ und „Textform“ —, haben in diesem AVV dieselbe Bedeutung.
- (3) Der AVV wird elektronisch zusammen mit dem Hauptvertrag geschlossen: Der Hinweis an der Bestellschaltfläche verweist auf die AGB und diesen AVV in der jeweils verlinkten Fassung (§ 3 Abs. 3 AGB). Coreflow stellt diesen AVV vor der Bestellung ohne Anmeldung abrufbar und zusätzlich als speicherbares PDF-Dokument bereit, das beide Parteien bezeichnet (Art. 28 Abs. 9 DSGVO). Coreflow speichert die Kennung der bei der Bestellung geltenden Fassung.

§ 1 Gegenstand, Dauer, Datenarten, Zweck, betroffene Personen

- (1) **Gegenstand.** Coreflow stellt dem Kunden den Routenplaner als webbasierte Software bereit und verarbeitet dabei personenbezogene Mandantendaten im Auftrag des Kunden.
- (2) **Dauer.** Der AVV gilt für die Laufzeit des Hauptvertrags. Er endet nicht vor Abschluss der Löschung nach § 7.
- (3) **Art der Verarbeitung.** Erheben und Erfassen, Speichern, Ordnen, Abfragen, Auslesen, Verändern, Verknüpfen, Verwenden (insbesondere Berechnen von Routen und Touren), Übermitteln an die in Anlage 2 Teil A genannten Unterauftragsverarbeiter, Bereitstellen zum

Export sowie Löschen.

- (4) **Zweck.** Die Verarbeitung dient ausschließlich dem Betrieb des Routenplaners für den Kunden: Verwaltung von Nutzerkonten, Verwaltung von Geschäftskontakten und Besuchsadressen, Geokodierung von Anschriften, Tourenplanung und Streckenberechnung, Hotelsuche, Dokumentation von Besuchen, Terminen, Fahrten und Arbeitstagen sowie Versand von Anmelde- und Einladungs-E-Mails.
- (5) **Kategorien betroffener Personen.**
1. Nutzer des Kunden, insbesondere seine Mitarbeiter im Außendienst und deren Vorgesetzte;
 2. Geschäftskontakte des Kunden, insbesondere Kunden und Interessenten, deren Anschriften als Besuchsadressen importiert oder erfasst werden, sowie deren Ansprechpartner, soweit der Kunde sie erfasst.
- (6) **Datenarten zu den Nutzern:** E-Mail-Adresse, Anzeigename, Rolle und Kontostatus; Passwort ausschließlich als kryptografischer Hash; Einladungen (E-Mail-Adresse, Name, Rolle); persönliche Einstellungen wie Heimat- oder Startadresse mit Koordinaten, Arbeitsregeln und Fahrzeugprofile; Tourenpläne, Routen und Termine; Besuchsberichte mit Plan- und Ist-Zeiten, Ergebnis, Themen und Notizen; Arbeitszeitrachweise mit Beginn, Ende, Pausen und gefahrenen Kilometern; Kennungen für Kalender-Abonnements; Verbindungsdaten wie IP-Adresse und Zeitpunkt in Server-Protokollen.
- (7) **Datenarten zu den Geschäftskontakten:** Firma, Kundennummer, Anschrift, Koordinaten, Telefonnummer, Website; Einstufungen wie Kategorie, Klasse, Priorität, Besuchsrhythmus und Erreichbarkeitszeiten; Datum des letzten Besuchs; Termine; Besuchsberichte und Notizen einschließlich darin erfasster Namen von Ansprechpartnern.
- (8) Besondere Kategorien personenbezogener Daten (Art. 9 DSGVO) sind nicht Gegenstand der Verarbeitung (§ 7 Abs. 2 AGB).
- (9) Vertrags-, Abrechnungs- und Zahlungsdaten des Kunden verarbeitet Coreflow in eigener Verantwortung; sie sind nicht Gegenstand dieses AVV.
- (10) **Ort der Verarbeitung.** Datenbank und Serverfunktionen stehen in der Europäischen Union. Eine Übermittlung in ein Drittland oder ein Zugriff aus einem Drittland erfolgt nur, soweit in Anlage 2 angegeben, und nur, wenn die Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind. Jede weitere Verlagerung in ein Drittland bedarf einer Weisung des Kunden oder einer Änderung nach § 3.

§ 2 Pflichten des Auftragsverarbeiters

- (1) **Weisungen.** Coreflow verarbeitet personenbezogene Mandantendaten nur auf dokumentierte Weisung des Kunden — auch in Bezug auf die Übermittlung in ein Drittland —, es sei denn, Coreflow ist nach dem Recht der Union oder eines Mitgliedstaats zur Verarbeitung verpflichtet; in diesem Fall teilt Coreflow dem Kunden diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet (Art. 28 Abs. 3 Satz 2 lit. a DSGVO). Die Weisungen sind bei Vertragsschluss durch den Hauptvertrag und diesen AVV festgelegt; die Nutzung der Funktionen des Routenplaners durch den Kunden und seine Nutzer gilt als Weisung.
- (2) Weitere Weisungen erteilt der Kunde von der dem Inhaber-Konto zugeordneten E-Mail-Adresse in Textform an support@coreflow-ai.de. Mündliche Weisungen bestätigt der Kunde unverzüglich in Textform. Coreflow dokumentiert erteilte Weisungen und bewahrt sie für die Laufzeit des AVV und drei weitere Kalenderjahre auf. Weisungen, die über den vertraglichen Leistungsumfang hinausgehen, kann Coreflow von einer gesonderten Vereinbarung über Aufwand und Vergütung abhängig machen.
- (3) Ist Coreflow der Ansicht, dass eine Weisung gegen die DSGVO oder andere Datenschutzvorschriften der Union oder der Mitgliedstaaten verstößt, informiert Coreflow den Kunden unverzüglich (Art. 28 Abs. 3 Satz 3 DSGVO) und darf die Ausführung aussetzen, bis der Kunde die Weisung bestätigt oder ändert.
- (4) Coreflow nutzt die personenbezogenen Mandantendaten nicht für eigene Zwecke und gibt sie nicht an Dritte weiter, außer an Unterauftragsverarbeiter nach § 3 oder auf Weisung des Kunden. Kopien werden nur erstellt, soweit sie für den Betrieb, die Datensicherheit oder die Erfüllung dieses AVV erforderlich sind.
- (5) Coreflow stellt sicher, dass die zur Verarbeitung befugten Personen zur Vertraulichkeit verpflichtet sind oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen (Art. 28 Abs. 3 Satz 2 lit. b DSGVO) und dass sie Zugriff nur erhalten, soweit dies für die Erfüllung des Hauptvertrags erforderlich ist. Die Pflicht zur Vertraulichkeit besteht über das Vertragsende hinaus fort.
- (6) Coreflow trifft die technischen und organisatorischen Maßnahmen nach Art. 32 DSGVO (§ 4, Anlage 1).
- (7) Coreflow unterstützt den Kunden unter Berücksichtigung der Art der Verarbeitung und der ihr zur Verfügung stehenden Informationen bei der Einhaltung der Pflichten aus Art. 32 bis 36 DSGVO, insbesondere bei Datenschutz-Folgenabschätzungen und vorherigen

Konsultationen der Aufsichtsbehörde, und bei der Erstellung seines Verzeichnisses von Verarbeitungstätigkeiten.

- (8) Coreflow informiert den Kunden unverzüglich, wenn personenbezogene Mandantendaten durch Maßnahmen Dritter (etwa Pfändung oder Beschlagnahme), durch ein Insolvenzverfahren oder durch sonstige Ereignisse gefährdet sind, sowie über Kontrollhandlungen und Maßnahmen einer Aufsichtsbehörde, soweit sie diesen AVV betreffen.
- (9) Ansprechstelle für Datenschutzfragen ist support@coreflow-ai.de. Benennt Coreflow einen Datenschutzbeauftragten, teilt Coreflow dem Kunden dessen Kontaktdaten in Textform mit.
- (10) **Rechte und Pflichten des Kunden.** Der Kunde ist für die Rechtmäßigkeit der Verarbeitung und die Wahrung der Rechte der betroffenen Personen verantwortlich (§ 7 Abs. 2 AGB). Er hat das Recht, Weisungen nach den Absätzen 1 und 2 zu erteilen und die Einhaltung dieses AVV nach § 8 zu überprüfen. Er informiert Coreflow unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Verarbeitung feststellt.

§ 3 Unterauftragnehmer — Anlage: Unterauftragsverarbeiter-Tabelle

- (1) Der Kunde genehmigt die in Anlage 2 Teil A genannten Unterauftragsverarbeiter. Zugleich erteilt er die allgemeine schriftliche Genehmigung (Art. 28 Abs. 2 DSGVO), weitere Unterauftragsverarbeiter hinzuzuziehen oder bestehende zu ersetzen, nach Maßgabe der folgenden Absätze.
- (2) Coreflow informiert den Kunden über jede beabsichtigte Hinzuziehung oder Ersetzung eines unmittelbaren Unterauftragsverarbeiters mindestens vier Wochen vorher in Textform und nennt Namen, Anschrift, Tätigkeit, Ort der Verarbeitung und gegebenenfalls die Garantien nach Art. 44 ff. DSGVO. Muss ein Unterauftragsverarbeiter kurzfristig ersetzt werden, um die Sicherheit oder Verfügbarkeit des Routenplaners zu wahren, informiert Coreflow unverzüglich, spätestens mit dem Wechsel; das Widerspruchsrecht nach Absatz 3 gilt dann ab Zugang der Information.
- (3) Der Kunde kann einer Änderung aus berechtigten datenschutzrechtlichen Gründen bis zu ihrem Wirksamwerden in Textform widersprechen. Coreflow wird sich dann um eine Lösung bemühen. Finden die Parteien keine Lösung, kann der Kunde den Hauptvertrag ohne Einhaltung einer Frist auf den Zeitpunkt des Wirksamwerdens der Änderung kündigen; für bereits gezahlte Entgelte über diesen Zeitpunkt hinaus erhält der Kunde eine anteilige Erstattung.
- (4) Coreflow legt jedem Unterauftragsverarbeiter durch Vertrag oder ein anderes Rechtsinstrument im Wesentlichen dieselben Datenschutzpflichten auf, die in diesem AVV festgelegt sind, insbesondere hinreichende Garantien für geeignete technische und

organisatorische Maßnahmen (Art. 28 Abs. 4 DSGVO). Coreflow wählt Unterauftragsverarbeiter sorgfältig aus und stellt dem Kunden auf Anfrage eine Kopie des jeweiligen Auftragsverarbeitungsvertrags zur Verfügung; Geschäftsgeheimnisse darf Coreflow dabei schwärzen. Coreflow haftet gegenüber dem Kunden für die Einhaltung der Pflichten des Unterauftragsverarbeiters wie für eigenes Handeln.

- (5) Die Unterauftragsverarbeiter setzen ihrerseits weitere Unterauftragsverarbeiter ein, die sie in öffentlich abrufbaren Listen führen; die Fundstellen nennt Coreflow dem Kunden auf Anfrage. Über Änderungen in diesen Listen, die Coreflow mitgeteilt werden, informiert Coreflow den Kunden unverzüglich in Textform; Absatz 3 gilt entsprechend.
- (6) Keine Unterauftragsverarbeitung im Sinne dieses AVV sind Leistungen, bei denen der Dienstleister keine Mandantendaten im Auftrag des Kunden verarbeitet. Sie sind aus Gründen der Transparenz in Anlage 2 Teil B genannt.

§ 4 TOMs (Anlage 1)

- (1) Die technischen und organisatorischen Maßnahmen sind in Anlage 1 beschrieben. Sie sind Bestandteil dieses AVV.
- (2) Die Maßnahmen unterliegen dem technischen Fortschritt. Coreflow darf sie durch gleichwertige oder bessere Maßnahmen ersetzen; das Schutzniveau darf dabei nicht sinken. Wesentliche Änderungen dokumentiert Coreflow und teilt sie dem Kunden auf Anfrage mit.
- (3) Coreflow überprüft die Wirksamkeit der Maßnahmen bei gegebenem Anlass, mindestens einmal jährlich, und dokumentiert das Ergebnis (Art. 32 Abs. 1 lit. d DSGVO).

§ 5 Betroffenenrechte

- (1) Coreflow unterstützt den Kunden mit geeigneten technischen und organisatorischen Maßnahmen bei der Beantwortung von Anträgen auf Wahrnehmung der Rechte nach Art. 12 bis 22 DSGVO (Art. 28 Abs. 3 Satz 2 lit. e DSGVO). Dies betrifft beide Gruppen betroffener Personen nach § 1 Abs. 5.
- (2) Wendet sich eine betroffene Person unmittelbar an Coreflow und ist sie dem Kunden zuzuordnen, leitet Coreflow das Anliegen unverzüglich an die E-Mail-Adresse des Inhaber-Kontos weiter. Coreflow beantwortet es nicht selbst, es sei denn, der Kunde weist Coreflow dazu an.
- (3) Soweit der Kunde personenbezogene Mandantendaten nicht selbst im Routenplaner berichtigen, löschen, in ihrer Verarbeitung einschränken oder auslesen kann, führt Coreflow dies auf Weisung des Kunden durch.

§ 6 Meldepflicht bei Datenpannen

- (1) Coreflow meldet dem Kunden jede Verletzung des Schutzes personenbezogener Daten, die personenbezogene Mandantendaten des Kunden betrifft, unverzüglich, nachdem sie Coreflow bekannt geworden ist, möglichst innerhalb von 24 Stunden (Art. 33 Abs. 2 DSGVO). Die Meldung geht in Textform an die E-Mail-Adresse des Inhaber-Kontos.
- (2) Die Meldung enthält, soweit bekannt, die Angaben nach Art. 33 Abs. 3 DSGVO: eine Beschreibung der Art der Verletzung, soweit möglich mit den Kategorien und der ungefähren Zahl der betroffenen Personen und Datensätze, eine Ansprechstelle, die wahrscheinlichen Folgen und die ergriffenen oder vorgeschlagenen Maßnahmen. Informationen, die noch nicht vorliegen, reicht Coreflow unverzüglich nach.
- (3) Coreflow ergreift unverzüglich die erforderlichen Maßnahmen, um die Verletzung einzudämmen und nachteilige Folgen zu mindern, und unterstützt den Kunden bei dessen Pflichten nach Art. 33 und 34 DSGVO. Meldungen an die Aufsichtsbehörde und Benachrichtigungen betroffener Personen nimmt der Kunde vor; Coreflow nimmt sie nur auf Weisung des Kunden vor.
- (4) Absatz 1 gilt entsprechend für schwerwiegende Störungen der Verarbeitung und für Verstöße von Coreflow oder von bei Coreflow beschäftigten Personen gegen diesen AVV.

§ 7 Löschung/Rückgabe nach Vertragsende

- (1) Nach Ende des Hauptvertrags gibt Coreflow die personenbezogenen Mandantendaten nach Wahl des Kunden zurück oder löscht sie (Art. 28 Abs. 3 Satz 2 lit. g DSGVO). Rückgabe bedeutet die Bereitstellung eines Exports; Frist, Form und Umfang des Exports sowie die Löschfrist richten sich nach § 5 Abs. 4 bis 7 AGB. Verlangt der Kunde innerhalb der dort genannten Frist keinen Export, gilt dies als Wahl der Löschung.
- (2) Coreflow macht die Bereitstellung eines Exports nicht von der Begleichung offener Entgelte abhängig; ein Zurückbehaltungsrecht an den personenbezogenen Mandantendaten ist ausgeschlossen.
- (3) Die Löschung umfasst auch die Daten bei den Unterauftragsverarbeitern. Soweit Daten in Datensicherungen enthalten sind, werden sie mit dem Ablauf der dort geltenden Aufbewahrungszyklen gelöscht und bis dahin nicht weiter verarbeitet.
- (4) Eine Aufbewahrung über die Löschfrist hinaus erfolgt nur, soweit das Recht der Union oder eines Mitgliedstaats Coreflow zur Speicherung verpflichtet. Aufbewahrungspflichten des Kunden selbst erfüllt der Kunde (§ 5 Abs. 7 AGB).
- (5) Coreflow bestätigt die Löschung auf Verlangen in Textform unter Angabe des Datums.

§ 8 Nachweise/Kontrollen

- (1) Coreflow stellt dem Kunden auf Anfrage alle Informationen zur Verfügung, die zum Nachweis der Einhaltung der Pflichten aus Art. 28 DSGVO und diesem AVV erforderlich sind (Art. 28 Abs. 3 Satz 2 lit. h DSGVO).
- (2) Den Nachweis erbringt Coreflow vorrangig durch Unterlagen, insbesondere eine aktuelle Beschreibung der technischen und organisatorischen Maßnahmen, die Dokumentation nach § 4 Abs. 3, die Auftragsverarbeitungsverträge sowie Zertifikate und Prüfberichte der Unterauftragsverarbeiter, soweit deren Weitergabe zulässig ist.
- (3) Der Kunde kann in angemessenen Abständen oder bei konkreten Anhaltspunkten für einen Verstoß Überprüfungen einschließlich Inspektionen selbst durchführen oder durch einen zur Verschwiegenheit verpflichteten Prüfer durchführen lassen, der kein Wettbewerber von Coreflow ist; Coreflow ermöglicht solche Überprüfungen und trägt zu ihnen bei. Eine Überprüfung ist mindestens 14 Tage vorher in Textform anzukündigen, es sei denn, ein konkreter Anlass erfordert eine kürzere Frist; sie findet während der üblichen Geschäftszeiten statt und darf den Betrieb nicht unverhältnismäßig stören. Coreflow betreibt keine eigenen Rechenzentren; Überprüfungen bei Unterauftragsverarbeitern richten sich nach deren Verträgen mit Coreflow. Jede Partei trägt ihre eigenen Kosten einer Überprüfung; ergibt die Überprüfung einen erheblichen Verstoß von Coreflow gegen diesen AVV, trägt Coreflow die angemessenen Kosten des Kunden.
- (4) Coreflow stellt der zuständigen Aufsichtsbehörde auf Anfrage die Informationen nach Absatz 1 zur Verfügung.

§ 9 Schlussbestimmungen

- (1) Bei Widersprüchen zwischen diesem AVV und dem Hauptvertrag geht dieser AVV in Fragen des Datenschutzes vor.
- (2) Änderungen der Anlage 2 richten sich nach § 3. Andere Änderungen dieses AVV teilt Coreflow mindestens sechs Wochen vor ihrem Wirksamwerden in Textform mit. Änderungen, die durch eine Änderung der Rechtslage, durch eine Anordnung oder Empfehlung einer Aufsichtsbehörde oder durch eine Änderung der technischen und organisatorischen Maßnahmen nach § 4 Abs. 2 veranlasst sind, gelten als genehmigt, wenn der Kunde nicht bis zu ihrem Wirksamwerden in Textform widerspricht; § 12 Abs. 2 Satz 3 bis 5 AGB gilt entsprechend. Alle übrigen Änderungen bedürfen der Zustimmung des Kunden in Textform.

- (3) Der Kunde kann den Hauptvertrag ohne Einhaltung einer Frist kündigen, wenn Coreflow schwerwiegend gegen diesen AVV oder gegen Datenschutzvorschriften verstößt, eine rechtmäßige Weisung nicht ausführen kann oder will oder Kontrollrechte nach § 8 vertragswidrig verweigert.
- (4) Die Haftung gegenüber betroffenen Personen richtet sich nach Art. 82 DSGVO. Im Verhältnis der Parteien gilt § 8 AGB; Art. 82 Abs. 5 DSGVO bleibt unberührt.
- (5) Es gilt das Recht der Bundesrepublik Deutschland. Der Gerichtsstand richtet sich nach § 13 Abs. 2 AGB.
- (6) Sollte eine Bestimmung dieses AVV unwirksam sein oder werden, bleibt die Wirksamkeit der übrigen Bestimmungen unberührt. An ihre Stelle tritt die gesetzliche Regelung, insbesondere Art. 28 DSGVO.

ANLAGE 1

TOMs

Coreflow betreibt kein eigenes Rechenzentrum. Alle Systeme laufen bei den in Anlage 2 Teil A genannten Unterauftragsverarbeitern; deren Maßnahmen ergänzen die folgenden eigenen Maßnahmen von Coreflow.

1. Zutrittskontrolle

- Server und Datenbanken stehen ausschließlich in Rechenzentren der Unterauftragsverarbeiter; der physische Zutritt richtet sich nach deren Maßnahmen und Nachweisen.
- Coreflow unterhält keine eigenen Serverräume.

2. Zugangskontrolle

- Nutzerkonten entstehen nur über eine Bestellung oder eine Einladung; eine offene Selbstregistrierung besteht nicht.
- Einladungs- und Wiederherstellungslinks sind zeitlich begrenzt gültig und nur einmal verwendbar.
- Passwörter müssen eine Mindestlänge und mehrere Zeichenklassen erfüllen; bekannt gewordene Passwörter werden abgewiesen. Passwörter werden nur als Hash gespeichert.
- Das Inhaberkonto der Datenbankplattform ist mit Zwei-Faktor-Authentifizierung geschützt.
- Zugangsschlüssel für Dienste werden nicht im Quellcode gespeichert, sondern getrennt verwaltet und nur zur Laufzeit geladen.

3. Zugriffskontrolle

- Mandantentrennung auf Datenbankebene: Jede Tabelle der Anwendung ist mit Row Level Security geschützt, und zwar aktiviert und erzwungen; ein Nutzer sieht und ändert nur Daten seines eigenen Mandanten.
- Diese Trennung wird bei jeder Freigabe einer neuen Version automatisiert geprüft; ein Test weist nach, dass ein Konto in einem fremden Mandanten nicht schreiben kann.
- Rollen innerhalb eines Mandanten (Inhaber, Nutzer); die Teamübersicht und die Abo-Verwaltung sind der Inhaber-Rolle vorbehalten.
- Die Anzahl der Nutzerkonten je Mandant ist technisch auf die gebuchte Sitzzahl begrenzt.
- Schlüssel mit Sonderrechten werden nur serverseitig verwendet, nie im Browser.

4. Weitergabekontrolle

- Alle Verbindungen zur Anwendung sind per TLS (HTTPS) verschlüsselt; der Browser wird per HSTS auf verschlüsselte Verbindungen festgelegt.
- An den Geokodierungsdienst wird nur die Anschrift ohne Namen, Kundennummer, Nutzerkennung oder IP-Adresse des Nutzers übermittelt, mit der Vorgabe, die Anfrage nicht zu speichern.
- Anfragen an den Routing- und Planungsserver laufen über verschlüsselte Verbindungen (TLS). Der Planungsserver hält keinen Schlüssel mit Sonderrechten; er greift auf Daten ausschließlich mit dem Zugangstoken des anfragenden Nutzers und damit unter der Mandantentrennung zu.
- Die Anfrage an den Hotelpreisdienst enthält nur Ort, Datum und Nächtezahl.

5. Eingabekontrolle

- Datensätze der Fachtabellen tragen die Kennung des Mandanten, soweit erforderlich des anlegenden Nutzers, sowie Zeitstempel.
- Kauf- und Abo-Ereignisse werden in einem Journal festgehalten.

6. Auftragskontrolle

- Mit allen Unterauftragsverarbeitern nach Anlage 2 Teil A bestehen Auftragsverarbeitungsverträge; sie werden in einem zentralen Verzeichnis geführt.
- Keine Verwendung von Mandantendaten für eigene Zwecke; Tests laufen in einem gesonderten Test-Mandanten mit fiktiven Daten.
- Mandantendaten gelangen nicht in das Quellcode-Repository; eine automatisierte Prüfung vor jeder Übernahme von Änderungen weist echte Daten und Zugangsschlüssel ab.

7. Verfügbarkeitskontrolle

- Neue Versionen gehen nur über einen festgelegten Freigabeweg in Betrieb, der zuvor eine automatisierte Prüfung gegen die neue Version ausführt; schlägt sie fehl, wird die Version nicht freigeschaltet. Frühere Versionen der Anwendung können wiederhergestellt werden.
- Der Hauptzweig des Quellcodes ist serverseitig gegen Löschen und Überschreiben geschützt.
- Anfragebegrenzungen an öffentlich erreichbaren Schnittstellen erschweren Missbrauch und Überlastung.

8. Trennungsgebot

- Die Daten aller Kunden liegen in einer gemeinsamen Datenbank, sind aber über eine Mandantenkennung und die unter Nr. 3 beschriebene erzwungene Row Level Security logisch getrennt.

9. Verschlüsselung und Standort

- Übertragung: TLS (Nr. 4).
- Ruhende Daten: Verschlüsselung der Datenträger durch die Anbieter von Datenbank und Hosting nach deren Angaben.
- Datenbank und Serverfunktionen laufen in der Region Frankfurt am Main, der Routing- und Planungsserver in Falkenstein (Deutschland).

10. Überprüfung

- Coreflow überprüft die Wirksamkeit dieser Maßnahmen nach § 4 Abs. 3.

ANLAGE 2**Unterauftragsverarbeiter-Tabelle****Teil A — Unterauftragsverarbeiter mit Zugriff auf personenbezogene Mandantendaten**

Unterauftragsverarbeiter	Leistung	Ort der Verarbeitung	Drittlandbezug / Garantie
Supabase Pte. Ltd., 65 Chulia Street #38-02/03, OCBC Centre, Singapur 049513	Datenbank und Anmeldung (Kontoverwaltung)	Amazon Web Services, Frankfurt am Main	Vertragspartner in Singapur, Unternehmensgruppe mit Sitz in den USA; möglicher Zugriff aus Drittländern: EU-Standardvertragsklauseln
Vercel Inc., 440 N Barranca Ave #4133, Covina, CA 91723, USA	Hosting der Anwendung und der Serverfunktionen	Serverfunktionen in Frankfurt am Main; Auslieferung über ein weltweites Netz	USA: EU-US Data Privacy Framework, ergänzend EU-Standardvertragsklauseln
Hetzner Online GmbH, Industriestr. 25, 91710 Gunzenhausen	Rechenzentrum des Routing- und Planungsservers (Streckenberechnung, Tourenplanung) sowie Speicher der Kartendaten (beim Abruf wird die IP-Adresse des Nutzers übertragen, keine Mandantendaten)	Falkenstein, Deutschland	keiner
OpenCage GmbH, Pappelallee 78/79, 10437 Berlin	Umwandlung von Anschriften in Koordinaten (nur Anschrift, ohne Namen)	Deutschland und Finnland	keiner
Heinlein Hosting GmbH (mailbox.org), Schwedter Straße 8/9, 10119 Berlin	Versand von E-Mails, insbesondere Einladungs- und Anmelde-E-Mails an Nutzer	Deutschland	keiner

Teil B — Dienste ohne Verarbeitung von Mandantendaten im Auftrag des Kunden (keine Unterauftragsverarbeitung, § 3 Abs. 6)

Dienst	Leistung	Übermittelte Daten	Einordnung
Nuitée (LiteAPI)	Hotelpreise für die Hotelsuche	ausschließlich Ort, Datum und Nächtezahl; keine Buchung	keine personenbezogenen Daten
Stripe Payments Europe, Ltd., Dublin, Irland	Zahlungsabwicklung und Abo-Verwaltung	Vertrags- und Zahlungsdaten des Kunden, keine Daten aus dem Routenplaner	Verarbeitung in eigener Verantwortung von Coreflow (§ 1 Abs. 9); Einzelheiten in der Datenschutzerklärung

Coreflow-Ai UG (haftungsbeschränkt)