Co-oto Teams – Auftragsverarbeitungsvertrag (AVV)

Version 1.1. Gültig ab: 19. November 2026.

Diese deutsche Fassung ist eine Übersetzung des englischen „Data Processing Agreement“. Bei Abweichungen ist die englische Fassung maßgebend.

Präambel

(A) Die Co-oto Sàrl, eine Gesellschaft mit beschränkter Haftung nach Schweizer Recht, eingetragen im Handelsregister des Kantons Waadt unter der UID CHE-414.102.270, mit Sitz am Chemin des Tines 5b, 1260 Nyon, Schweiz („**Co-oto**“), stellt die Anwendung Co-oto bereit, ein Werkzeug zur Koordination der gemeinsamen Nutzung von Fahrzeugen und zur Aufteilung ihrer Kosten innerhalb eines Vertrauenskreises, verfügbar für iOS, Android und im Web (der „**Dienst**“).

(B) Dieser Auftragsverarbeitungsvertrag („**AVV**“) ist integraler Bestandteil der Nutzungsbedingungen von Co-oto (die „**Nutzungsbedingungen**“) und durch Verweis in diese einbezogen. Er gilt ohne Unterschrift, sobald ein Kunde den Teams-Tarif abonniert, sei es über den Apple App Store, Google Play oder die Website von Co-oto. Mit dem Abschluss des Abonnements nimmt der Kunde diesen AVV an, und die Person, die das Abonnement abschließt, bestätigt, dass sie befugt ist, ihn im Namen des Kunden anzunehmen.

(C) Dieser AVV enthält die Bestimmungen, die Artikel 28 der Verordnung (EU) 2016/679 („**DSGVO**“) und Artikel 9 des Schweizer Bundesgesetzes über den Datenschutz vom 25. September 2020 („**DSG**“) verlangen. Er orientiert sich an den Standardvertragsklauseln zwischen Verantwortlichen und Auftragsverarbeitern gemäß dem Durchführungsbeschluss (EU) 2021/915 der Kommission.

1. Begriffsbestimmungen

1.1 „**Kunde**“ bezeichnet das Unternehmen, den Verein, die Genossenschaft, die öffentliche Stelle oder die in beruflicher oder vereinsbezogener Eigenschaft handelnde Einzelperson, die den Teams-Tarif abonniert und einen oder mehrere Kreise im Dienst verwaltet.

1.2 „**Personenbezogene Kundendaten**“ bezeichnet personenbezogene Daten, die Co-oto im Auftrag des Kunden innerhalb der Kreise des Kunden verarbeitet, wie in Anhang I beschrieben.

1.3 „**Datenschutzrecht**“ bezeichnet, soweit auf die jeweilige Verarbeitung anwendbar: das DSG und die Schweizer Datenschutzverordnung vom 31. August 2022 („**DSV**“); die DSGVO und das sie ergänzende Recht der EU-/EWR-Mitgliedstaaten; sowie die UK GDPR und den UK Data Protection Act 2018.

1.4 „**Verletzung des Schutzes personenbezogener Daten**“ bezeichnet eine Verletzung der Sicherheit, die zur unbeabsichtigten oder unrechtmäßigen Vernichtung, zum Verlust, zur Veränderung, zur unbefugten Offenlegung von oder zum unbefugten Zugang zu Personenbezogenen Kundendaten führt, einschließlich einer Verletzung der Datensicherheit im Sinne von Art. 5 lit. h DSG.

1.5 „**Unterauftragsverarbeiter**“ bezeichnet jeden von Co-oto beauftragten Dritten, der Personenbezogene Kundendaten im Auftrag des Kunden verarbeitet.

1.6 „**Aufsichtsbehörde**“ bezeichnet je nach Anwendbarkeit den Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten („**EDÖB**“), eine Aufsichtsbehörde im Sinne von Artikel 51 DSGVO oder den britischen Information Commissioner.

1.7 „**SCC**“ bezeichnet die Standardvertragsklauseln für die Übermittlung personenbezogener Daten in Drittländer gemäß dem Durchführungsbeschluss (EU) 2021/914 der Kommission, einschließlich der nach Schweizer Recht erforderlichen Anpassungen, wie sie der EDÖB am 27. August 2021 anerkannt hat, und gegebenenfalls des UK International Data Transfer Addendum.

2. Geltungsbereich

2.1 Dieser AVV gilt für die Verarbeitung Personenbezogener Kundendaten durch Co-oto bei der Bereitstellung des Teams-Tarifs, einschließlich Teams-Tarifen, die im Rahmen eines individuellen Angebots in mehreren Blöcken erworben werden, und unentgeltlich gewährter Teams-Zugänge. Er umfasst die mobilen Apps, das Web-Dashboard, Statistiken und Exporte.

2.2 Dieser AVV gilt, soweit der Kunde als Verantwortlicher handelt, der dem Datenschutzrecht unterliegt. Wird ein Kreis von einer natürlichen Person ausschließlich zu persönlichen oder familiären Zwecken genutzt, verarbeitet Co-oto die Daten gemäß seiner Datenschutzerklärung und wendet die in Anhang II beschriebenen Maßnahmen an.

2.3 Endet ein Teams-Abonnement, fallen die Kreise des Kunden auf den kostenlosen Tarif zurück, und ihre Daten bleiben erhalten (Nutzungsbedingungen, Artikel 18). Dieser AVV gilt für diese Daten weiter, solange Co-oto sie im Auftrag des Kunden verarbeitet.

2.4 Dieser AVV gilt nicht für: (a) das Gerät Co-oto Link und sonstige Hardware-Erweiterungen; (b) Integrationen für den Fahrzeugzugang oder für Fahrzeugdaten, die Teams-Kunden nicht angeboten werden, wie Co-oto Access oder Connected-Car-Dienste; (c) Verträge mit öffentlichen Stellen, die zu besonderen Bedingungen geschlossen werden; (d) Verarbeitungen, für die Co-oto gemäß Ziffer 3.3 eigenständiger Verantwortlicher ist.

3. Rollen der Parteien

3.1 **Kunde als Verantwortlicher.** Der Kunde bestimmt die Zwecke der Verarbeitung Personenbezogener Kundendaten, insbesondere die Organisation der Fahrzeugnutzung, Buchungen, Fahrtenaufzeichnungen, die Kostenaufteilung und die Erfassung von Ausgaben innerhalb seiner Kreise. Er entscheidet, wen er einlädt, welche Rollen er vergibt und welche Daten er von den Mitgliedern erfassen lässt.

3.2 **Co-oto als Auftragsverarbeiter.** Co-oto verarbeitet Personenbezogene Kundendaten ausschließlich im Auftrag des Kunden und gemäß diesem AVV.

3.3 **Co-oto als eigenständiger Verantwortlicher.** Co-oto handelt gemäß seiner Datenschutzerklärung und außerhalb dieses AVV als eigenständiger Verantwortlicher für:

1. Benutzerkonten als solche (Erstellung, Anmeldedaten und Anmeldung per E-Mail-Code, Apple oder Google), da ein Konto mehreren Kreisen und Tarifen angehören kann. Name, E-Mail-Adresse und Rolle, die innerhalb der Kreise des Kunden angezeigt werden, sowie die auf diese Kreise angewandte Zugriffskontrolle bleiben Personenbezogene Kundendaten;
2. Abonnements, Abrechnung, Zahlungen und Buchhaltungsunterlagen;

3. die Sicherheit des Dienstes, einschließlich der Abwehr von Bots und Missbrauch (App Check) und der App-Konfiguration (Remote Config);
4. die Produktmessung anhand von Nutzungsereignissen, die in der eigenen Datenbank von Co-oto gespeichert, bei Kontolöschung vom Namen des Nutzers getrennt und nach 13 Monaten gelöscht werden, sowie daraus abgeleitete anonymisierte Aggregate, einschließlich anonymisierter Aktivitäten, die auf der Website von Co-oto angezeigt werden;
5. die Kommunikation mit dem Kunden über sein Konto und den Dienst;
6. die Erfüllung rechtlicher Verpflichtungen sowie die Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.

Co-oto verwendet Personenbezogene Kundendaten für keinen anderen eigenen Zweck, verkauft sie nicht und nutzt sie nicht für Werbung.

3.4 **Verantwortlichkeiten des Kunden.** Der Kunde ist verantwortlich für:

1. die Rechtmäßigkeit der Verarbeitung, einschließlich einer geeigneten Rechtsgrundlage;
2. die Information der betroffenen Personen in seinen Kreisen gemäß den Artikeln 13 und 14 DSGVO und Artikel 19 DSG, auch über optionale Felder wie die Kontakttelefonnummer, Zahlungsangaben für Rückerstattungen und Fahrerangaben (Angaben zu Führerschein und Versicherung);
3. die Richtigkeit der von ihm erfassten Daten sowie die von ihm vergebenen Rollen und Zugriffsrechte;
4. die Anweisung an die Mitglieder, keine besonderen Kategorien personenbezogener Daten (Artikel 9 DSGVO) oder besonders schützenswerten Personendaten (Art. 5 lit. c DSG) in Freitextfelder, Nachrichten oder Fotos einzugeben;
5. sofern er Arbeitgeber ist, seine Pflichten aus dem Arbeits- und Datenschutzrecht, einschließlich der Information der Beschäftigten, der Beteiligung der Arbeitnehmervertretung, soweit erforderlich, und der Einhaltung von Artikel 328b des Schweizer Obligationenrechts, Artikel 26 der Verordnung 3 zum Schweizer Arbeitsgesetz, Artikel 88 DSGVO und des nationalen Rechts.

Der Kunde darf den Dienst nicht nutzen, um das Verhalten von Beschäftigten oder anderen Fahrern über das Maß hinaus zu überwachen, das zur Organisation der Fahrzeugnutzung und zur Kostenaufteilung erforderlich ist.

4. Weisungen

4.1 Co-oto verarbeitet Personenbezogene Kundendaten nur auf dokumentierte Weisung des Kunden, auch in Bezug auf Übermittlungen in Drittländer, es sei denn, Co-oto ist nach Schweizer Recht oder nach dem Recht der EU oder eines Mitgliedstaats, dem Co-oto unterliegt, dazu verpflichtet. In diesem Fall informiert Co-oto den Kunden vorab, sofern das betreffende Recht dies nicht aus wichtigen Gründen des öffentlichen Interesses untersagt.

4.2 Die dokumentierten Weisungen des Kunden sind: (a) dieser AVV und die Nutzungsbedingungen; (b) die Konfiguration und Nutzung des Dienstes durch den Kunden, einschließlich der von den Inhabern und Verwaltern seiner Kreise gewählten Einstellungen; (c) jede weitere schriftliche Weisung an info@co-oto.app, die mit den Nutzungsbedingungen und dem Funktionsumfang des Dienstes vereinbar ist.

4.3 Co-oto informiert den Kunden unverzüglich, wenn eine Weisung nach seiner Auffassung gegen Datenschutzrecht verstößt, und kann die Ausführung dieser Weisung aussetzen, bis der Kunde sie bestätigt oder ändert.

5. Pflichten von Co-oto

5.1 Co-oto verarbeitet Personenbezogene Kundendaten nur, soweit dies zur Bereitstellung des Dienstes erforderlich ist, und nur so, wie der Kunde selbst sie verarbeiten dürfte (Art. 9 Abs. 1 lit. a DSG).

5.2 Co-oto unterstützt den Kunden unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Einhaltung der Artikel 32 bis 36 DSGVO und der Artikel 7, 8, 22, 23 und 24 DSG, wie in den Ziffern 11 und 12 beschrieben.

5.3 Co-oto führt ein Verzeichnis der Verarbeitungen, die es im Auftrag seiner Kunden durchführt, soweit Artikel 30 Abs. 2 DSGVO oder Artikel 12 DSG dies verlangen.

5.4 Co-oto stellt dem Kunden die Informationen zur Verfügung, die zum Nachweis der Einhaltung dieses AVV erforderlich sind, wie in Ziffer 13 beschrieben.

6. Vertraulichkeit

6.1 Co-oto stellt sicher, dass sich jede Person, die es zur Verarbeitung Personenbezogener Kundendaten ermächtigt, zur Vertraulichkeit verpflichtet hat oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegt.

6.2 Der Zugang zu Personenbezogenen Kundendaten ist auf die in Anhang II beschriebenen Personen beschränkt und erfolgt nur, soweit er für deren Aufgaben erforderlich ist.

7. Sicherheit der Verarbeitung

7.1 Co-oto setzt die in Anhang II aufgeführten technischen und organisatorischen Maßnahmen um und erhält sie aufrecht, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten, gemäß Artikel 32 DSGVO, Artikel 8 DSG und den Artikeln 1 bis 5 DSV.

7.2 Co-oto kann diese Maßnahmen an die Entwicklung von Technik und Risiken anpassen, sofern das Schutzniveau insgesamt nicht verringert wird. Wesentliche Änderungen werden in der veröffentlichten Fassung von Anhang II nachgeführt.

7.3 Der Kunde ist für die Sicherheitsmaßnahmen in seinem eigenen Einflussbereich verantwortlich, insbesondere für den Schutz des Zugangs zu Inhaber- und Verwalterkonten, die angemessene Vergabe von Rollen, das Entfernen von Mitgliedern, die keinen Zugang mehr benötigen, und den sicheren Umgang mit exportierten Dateien nach dem Herunterladen.

8. Unterauftragsverarbeiter

8.1 **Allgemeine Genehmigung.** Der Kunde erteilt Co-oto die allgemeine Genehmigung, Unterauftragsverarbeiter im Sinne von Artikel 28 Abs. 2 DSGVO und Artikel 9 Abs. 3 DSG einzusetzen. Die zum Zeitpunkt des Inkrafttretens genehmigten Unterauftragsverarbeiter sind in Anhang III, Teil A aufgeführt.

8.2 **Liste und Mitteilung.** Co-oto führt eine aktuelle Liste seiner Unterauftragsverarbeiter mit deren Standort, Tätigkeit und Übermittlungsmechanismus in Abschnitt 6 seiner Datenschutzerklärung unter https://www.co-oto.app/privacy-policy/. Co-oto informiert den Kunden über jede beabsichtigte Hinzuziehung oder Ersetzung eines Unterauftragsverarbeiters mindestens dreißig (30) Tage im Voraus per E-Mail an den Inhaber des Kreises und durch Aktualisierung dieser Liste.

8.3 **Widerspruch.** Der Kunde kann innerhalb der Mitteilungsfrist schriftlich aus berechtigten datenschutzrechtlichen Gründen widersprechen. Die Parteien erörtern den Widerspruch nach Treu und Glauben. Kann Co-oto dem Widerspruch nicht in zumutbarer Weise Rechnung tragen, kann der Kunde sein Teams-Abonnement kündigen, bevor die Änderung wirksam wird. Hat der Kunde direkt über die Website an Co-oto gezahlt, erstattet Co-oto die im Voraus gezahlten Entgelte für die verbleibende Laufzeit anteilig. Wurde das Abonnement über den Apple App Store oder Google Play erworben, kündigt der Kunde es über den jeweiligen Store, und für Erstattungen gelten dessen Richtlinien. Widerspricht der Kunde nicht innerhalb der Mitteilungsfrist, gilt die Änderung als genehmigt.

8.4 **Dringende Ersetzung.** Muss ein Unterauftragsverarbeiter aus Gründen der Sicherheit, der Verfügbarkeit oder der Rechtskonformität, die außerhalb des Einflussbereichs von Co-oto liegen, dringend ersetzt werden, kann Co-oto die Änderung mit kürzerer Frist vornehmen und informiert den Kunden so bald wie möglich. Das Widerspruchsrecht nach Ziffer 8.3 läuft dann ab dieser Mitteilung.

8.5 **Weitergabe der Pflichten und Haftung.** Co-oto erlegt jedem Unterauftragsverarbeiter vertraglich Datenschutzpflichten auf, die im Wesentlichen dasselbe Schutzniveau bieten wie dieser AVV, einschließlich hinreichender Garantien für technische und organisatorische Maßnahmen. Co-oto haftet gegenüber dem Kunden weiterhin für die Erfüllung der Pflichten seiner Unterauftragsverarbeiter (Artikel 28 Abs. 4 DSGVO), vorbehaltlich Ziffer 14. Einige Unterauftragsverarbeiter sind große Cloud-Anbieter, die ausschließlich Standardbedingungen anbieten; Co-oto stellt die betreffenden Bedingungen auf Anfrage zur Verfügung.

9. Internationale Datenübermittlungen

9.1 **Standorte.** Personenbezogene Kundendaten werden im Europäischen Wirtschaftsraum gespeichert; ein Teil des E-Mail-Verkehrs wird in der Schweiz abgewickelt, wie in Anhang III beschrieben. Bestimmte technische Dienste (Authentifizierung und Push-Benachrichtigungen) sowie die vom Co-oto-Team genutzten KI-Werkzeuge sind mit einer Verarbeitung in den Vereinigten Staaten verbunden.

9.2 **EU/EWR in die Schweiz.** Übermittlungen aus der EU bzw. dem EWR an Co-oto stützen sich auf den Angemessenheitsbeschluss der Europäischen Kommission für die Schweiz (Entscheidung 2000/518/EG), dessen Fortgeltung die Kommission am 15. Januar 2024 bestätigt hat.

9.3 **Aus der Schweiz.** Übermittlungen durch Co-oto in Staaten, die in Anhang 1 DSV aufgeführt sind, einschließlich der EU-/EWR-Mitgliedstaaten, stützen sich auf diese Angemessenheitsfeststellung (Art. 16 Abs. 1 DSG).

9.4 **Vereinigte Staaten.** Co-oto übermittelt Personenbezogene Kundendaten an einen Unterauftragsverarbeiter in den Vereinigten Staaten nur: (a) wenn der Empfänger unter dem EU-U.S. Data Privacy Framework (Durchführungsbeschluss (EU) 2023/1795 der Kommission), dem Swiss-U.S. Data Privacy Framework (Anhang 1 DSV, in Kraft seit dem 15. September 2024) und

gegebenenfalls der UK Extension zertifiziert ist; oder (b) andernfalls auf der Grundlage der SCC, mit den Schweizer Anpassungen und gegebenenfalls dem UK Addendum, zusammen mit etwaigen zusätzlichen Maßnahmen, die nach einer Transfer-Folgenabschätzung erforderlich sind.

9.5 **Rückfallregelung.** Wird ein Angemessenheitsbeschluss, auf den sich eine Übermittlung stützt, für ungültig erklärt, ausgesetzt oder aufgehoben, stützt sich Co-oto unverzüglich auf die SCC oder eine andere geeignete Garantie, die der Unterauftragsverarbeiter anbietet, oder ergreift andere Maßnahmen, um die Übermittlung rechtskonform zu gestalten, und informiert den Kunden. Eine Änderung dieses AVV ist dafür nicht erforderlich.

9.6 **Schweizer Anpassungen.** Soweit die SCC für Übermittlungen gelten, die dem DSG unterliegen: (a) ist der EDÖB die zuständige Aufsichtsbehörde für diese Übermittlungen; (b) sind Verweise auf die DSGVO insoweit als Verweise auf das DSG zu verstehen; (c) hindert der Begriff „Mitgliedstaat“ betroffene Personen in der Schweiz nicht daran, ihre Rechte an ihrem gewöhnlichen Aufenthaltsort geltend zu machen.

9.7 **Vereinigtes Königreich.** Für Personenbezogene Kundendaten, die der UK GDPR unterliegen und in ein Land ohne britische Angemessenheitsregelung übermittelt werden, gilt das UK International Data Transfer Addendum zu den SCC.

10. Integrationen von KI-Assistenten und Sprachassistenten

10.1 **Kontrolle durch den Kunden.** Integrationen mit KI-Assistenten (etwa die Co-oto-Konnektoren für Claude oder ChatGPT) stehen in den Kreisen des Kunden zur Verfügung, und der Kunde kann sie jederzeit in den Einstellungen des Kreises deaktivieren. Lässt der Kunde sie aktiviert, gilt dies als Weisung des Kunden.

10.2 **Eigener Assistent des Mitglieds.** Ein Mitglied, das einen Assistenten nutzen möchte, verbindet seinen eigenen Assistenten mit seinem eigenen Konto beim KI-Anbieter und bestätigt die Verbindung mit einem per E-Mail zugesandten Code. Co-oto sendet Daten nur auf Anforderung eines verbundenen Mitglieds an einen KI-Anbieter, nie aus eigener Initiative. Der KI-Anbieter handelt auf der Grundlage seiner eigenen Bedingungen mit dem Mitglied und ist kein Unterauftragsverarbeiter von Co-oto.

10.3 **Begrenzte Daten.** Ein verbundener Assistent erhält nur den Namen und die Rolle des Mitglieds, die Fahrzeuge des Kreises und deren Regeln sowie die eigenen Buchungen des Mitglieds. Andere Mitglieder erscheinen nur als „der Inhaber“ oder „ein anderes Mitglied“, und von Mitgliedern verfasster Freitext wird vor dem Senden gefiltert. Verbindungstoken werden gehasht gespeichert; Zugriffstoken verfallen nach 1 Stunde, Aktualisierungstoken nach 60 Tagen.

10.4 **Sprachassistenten.** Sprachfunktionen des Betriebssystems auf dem Gerät des Mitglieds, etwa Siri unter iOS, werden auf Initiative des Mitglieds im Rahmen seiner Beziehung zum Geräteanbieter genutzt. Der Kunde kann sie in den Einstellungen des Kreises deaktivieren.

11. Unterstützung

11.1 **Anträge betroffener Personen.** Co-oto unterstützt den Kunden mit geeigneten technischen und organisatorischen Maßnahmen, soweit dies möglich ist, bei der Beantwortung von Anträgen betroffener Personen nach Kapitel III DSGVO und den Artikeln 25 bis 32 DSG. Inhaber und Verwalter können die Daten ihrer Kreise im Dienst einsehen, berichtigen und exportieren. Erhält Co-oto einen solchen Antrag direkt, leitet es ihn unverzüglich an den Kunden

weiter und beantwortet ihn nicht selbst, außer um die betroffene Person an den Kunden zu verweisen, sofern keine anderslautende Weisung vorliegt oder das Gesetz nichts anderes verlangt.

11.2 **Folgenabschätzungen.** Co-oto leistet angemessene Unterstützung bei Datenschutz-Folgenabschätzungen und vorherigen Konsultationen einer Aufsichtsbehörde (Artikel 35 und 36 DSGVO; Artikel 22 und 23 DSG), in erster Linie durch Bereitstellung der Informationen in diesem AVV und seinen Anhängen.

11.3 **Kosten.** Die Unterstützung ist unentgeltlich, soweit sie über den Dienst oder die veröffentlichte Dokumentation erbracht werden kann. Für Unterstützung, die erheblichen Aufwand erfordert, kann Co-oto angemessene Kosten berechnen, die es vorab mitteilt.

12. Verletzung des Schutzes personenbezogener Daten

12.1 Co-oto meldet dem Kunden jede Verletzung des Schutzes personenbezogener Daten, die Personenbezogene Kundendaten betrifft, unverzüglich und, soweit möglich, spätestens achtundvierzig (48) Stunden, nachdem sie Co-oto bekannt geworden ist (Artikel 33 Abs. 2 DSGVO; Art. 24 Abs. 3 DSG). Die Meldung erfolgt per E-Mail an den Inhaber des Kreises.

12.2 Die Meldung enthält, soweit verfügbar: die Art der Verletzung, nach Möglichkeit mit den Kategorien und der ungefähren Zahl der betroffenen Personen und Datensätze; die Kontaktstelle bei Co-oto; die wahrscheinlichen Folgen; sowie die ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung und zur Abmilderung ihrer Auswirkungen. Informationen, die nicht sofort verfügbar sind, können ohne weitere unangemessene Verzögerung schrittweise nachgereicht werden.

12.3 Co-oto ergreift angemessene Maßnahmen, um die Verletzung einzudämmen und ihre Auswirkungen abzumildern, und arbeitet mit dem Kunden zusammen, damit dieser seine eigenen Meldepflichten erfüllen kann. Die Meldung einer Verletzung stellt kein Anerkenntnis eines Verschuldens oder einer Haftung dar.

12.4 Co-oto dokumentiert jede Verletzung des Schutzes personenbezogener Daten, einschließlich des Sachverhalts, der Auswirkungen und der ergriffenen Abhilfemaßnahmen.

13. Prüfungen (Audits)

13.1 Auf Anfrage stellt Co-oto die Informationen zur Verfügung, die zum Nachweis der Einhaltung von Artikel 28 DSGVO, Artikel 9 DSG und dieses AVV erforderlich sind, darunter: einen ausgefüllten Sicherheitsfragebogen (einmal pro Jahr); eine Beschreibung seiner aktuellen technischen und organisatorischen Maßnahmen; sowie die Zertifizierungen und Prüfberichte seiner wichtigsten Unterauftragsverarbeiter, insbesondere das ISO/IEC-27001-Zertifikat und die SOC-Berichte von Google für Firebase und Google Cloud. Co-oto verfügt selbst über keine Sicherheitszertifizierung.

13.2 Reichen diese Informationen vernünftigerweise nicht aus oder wird eine Prüfung von einer Aufsichtsbehörde verlangt oder folgt sie auf eine Verletzung des Schutzes personenbezogener Daten, kann der Kunde eine Prüfung selbst oder durch einen unabhängigen, zur Vertraulichkeit verpflichteten Prüfer durchführen, der kein Wettbewerber von Co-oto ist, unter folgenden Bedingungen: (a) schriftliche Ankündigung dreißig (30) Tage im Voraus, außer wenn eine Aufsichtsbehörde die Prüfung verlangt oder sie auf eine Verletzung folgt; (b) höchstens eine

Prüfung je Zeitraum von zwölf Monaten; (c) ein im Voraus vereinbarter Umfang und eine im Voraus vereinbarte Dauer, beschränkt auf die eigene Verarbeitung von Co-oto; (d) Durchführung nach Möglichkeit aus der Ferne, während der Geschäftszeiten und ohne Zugang zu Daten anderer Kunden; (e) der Kunde trägt seine eigenen Kosten und erstattet Co-oto dessen angemessene Kosten, es sei denn, die Prüfung ergibt einen wesentlichen Verstoß von Co-oto gegen diesen AVV.

14. Haftung

14.1 Die Gesamthaftung jeder Partei aus oder im Zusammenhang mit diesem AVV ist auf die Entgelte beschränkt, die der Kunde in den zwölf (12) Monaten vor dem anspruchsbegründenden Ereignis für den Teams-Tarif gezahlt hat. Für Sachverhalte, die dieser AVV regelt, geht diese Ziffer der Haftungsbeschränkung und dem Haftungsausschluss in den Nutzungsbedingungen vor.

14.2 Dieser AVV beschränkt oder schließt nicht aus: (a) die Haftung für rechtswidrige Absicht oder grobe Fahrlässigkeit (Artikel 100 des Schweizer Obligationenrechts) oder jede andere Haftung, die gesetzlich nicht beschränkt werden kann; (b) die Rechte betroffener Personen nach Artikel 82 DSGVO oder nach dem DSG sowie die Haftungsverteilung zwischen Verantwortlichem und Auftragsverarbeiter nach Artikel 82 Abs. 4 und 5 DSGVO.

15. Aufbewahrung, Rückgabe und Löschung

15.1 **Während des Abonnements.** Fahrten, Buchungen, Ausgaben, Fotos und Nachrichten des Kreises werden aufbewahrt, solange der Kreis besteht. Co-oto wendet auf sie keine kürzere Aufbewahrungsfrist an. Der Kunde kann jederzeit die Löschung bestimmter Daten verlangen.

15.2 **Wenn ein Mitglied sein Konto löscht.** Das Profilfoto des Mitglieds wird automatisch gelöscht. Fahrten, Buchungen und Ausgaben bleiben im Kreis erhalten, wobei der Name des Mitglieds ersetzt wird (Pseudonymisierung). Nachrichten bleiben für den Kreis mit dem beim Senden angezeigten Namen sichtbar und werden auf Anfrage gelöscht.

15.3 **Rückgabe.** Während des Abonnements und nach dessen Ende können Inhaber und Verwalter Statistiken und die Kostenabrechnung aus dem Dienst exportieren. Auf schriftliche Anfrage stellt Co-oto innerhalb von dreißig (30) Tagen einen Export der Kreisdaten des Kunden in einem gängigen elektronischen Format bereit.

15.4 **Löschung.** Auf schriftliche Anfrage des Kunden, insbesondere nach Ende der Leistungserbringung, löscht Co-oto die Kreise des Kunden und die zugehörigen Personenbezogenen Kundendaten einschließlich der Fotos innerhalb von dreißig (30) Tagen aus seinen aktiven Systemen, sofern nicht Schweizer Recht oder das Recht der EU oder eines Mitgliedstaats die Speicherung verlangt. Gelöschte Daten verbleiben bis zu sieben (7) Tage in der Point-in-Time-Wiederherstellung und bis zu achtundneunzig (98) Tage in den wöchentlichen Sicherungen; danach werden sie überschrieben. Bis dahin bleiben die Sicherungen durch diesen AVV geschützt und werden zu keinem anderen Zweck verwendet. Authentifizierungsdaten bei Firebase Authentication werden innerhalb der von Google angegebenen Frist (derzeit bis zu 180 Tage) aus den Systemen von Google entfernt.

15.5 Daten, die Co-oto als eigenständiger Verantwortlicher gemäß Ziffer 3.3 verarbeitet, etwa Buchhaltungsunterlagen, die zehn Jahre aufbewahrt werden (Artikel 958f des Schweizer Obligationenrechts), unterliegen der Datenschutzerklärung von Co-oto.

16. Laufzeit, Rangfolge und Änderungen

16.1 Dieser AVV gilt, solange Co-oto Personenbezogene Kundendaten im Auftrag des Kunden verarbeitet. Bestimmungen, die ihrer Natur nach über die Beendigung hinaus gelten, bleiben in Kraft.

16.2 Bei Widersprüchen gilt folgende Rangfolge: (a) die SCC, soweit anwendbar; (b) dieser AVV; (c) die Nutzungsbedingungen.

16.3 Co-oto kann diesen AVV ändern, um Änderungen des Datenschutzrechts, Entscheidungen von Gerichten oder Aufsichtsbehörden oder Änderungen des Dienstes Rechnung zu tragen, sofern das Schutzniveau für Personenbezogene Kundendaten nicht wesentlich verringert wird. Co-oto teilt wesentliche Änderungen mindestens dreißig (30) Tage im Voraus per E-Mail an den Inhaber des Kreises mit. Frühere Fassungen sind auf Anfrage erhältlich.

17. Anwendbares Recht und Gerichtsstand

17.1 Dieser AVV unterliegt Schweizer Recht unter Ausschluss seiner Kollisionsnormen.

17.2 Ausschließlich zuständig sind die Gerichte in Nyon, Kanton Waadt, Schweiz, vorbehaltlich der Beschwerde an das Schweizerische Bundesgericht.

17.3 Die Ziffern 17.1 und 17.2 gelten unbeschadet: (a) zwingender Bestimmungen der DSGVO und des Rechts der EU-/EWR-Mitgliedstaaten, einschließlich der Rechte betroffener Personen nach den Artikeln 77 bis 79 DSGVO; (b) der Rechtswahl- und Gerichtsstandsklauseln der SCC, soweit anwendbar; (c) zwingender Verbraucherschutzvorschriften.

18. EU-Vertreter und Kontakt

18.1 Co-oto hat die VGS Datenschutzpartner GmbH, Am Kaiserkai 69, 20457 Hamburg, Deutschland, als Vertreter in der Europäischen Union gemäß Artikel 27 DSGVO benannt. Deren E-Mail-Adresse ist in Abschnitt 1 der Datenschutzerklärung von Co-oto angegeben.

18.2 Fragen, Weisungen, Anträge und Mitteilungen im Rahmen dieses AVV: Co-oto Sàrl, Deniz Ates, Chemin des Tines 5b, 1260 Nyon, Schweiz, info@co-oto.app.

Anhang I: Einzelheiten der Verarbeitung

Parteien. Verantwortlicher: der Kunde, erreichbar über die E-Mail-Adresse des Inhabers seines Kreises. Auftragsverarbeiter: Co-oto Sàrl, Nyon, Schweiz, info@co-oto.app; EU-Vertreter: VGS Datenschutzpartner GmbH, Hamburg.

Gegenstand. Bereitstellung des Teams-Tarifs: Software zur Koordination der gemeinsamen Nutzung von Fahrzeugen innerhalb eines Kreises und zur Aufteilung der damit verbundenen Kosten.

Dauer. Solange Co-oto Personenbezogene Kundendaten im Auftrag des Kunden verarbeitet, zuzüglich der Löschfristen nach Ziffer 15.

Art der Verarbeitung. Erheben, Erfassen, Organisieren, Speichern, Abrufen, Abfragen, Berechnen (Kosten, Salden, Statistiken), Anzeigen, Übermitteln (Synchronisierung, Nachrichten, Push-Benachrichtigungen, Transaktions-E-Mails), Exportieren, Einschränken und Löschen.

Zwecke, im Auftrag des Kunden. Verwaltung der Mitgliedschaft und der Rollen im Kreis; Buchung von Fahrzeugen und Führung eines gemeinsamen Kalenders; Aufzeichnung von Fahrten; Berechnung von Kosten und Salden zwischen den Mitgliedern (Zahlungen erfolgen außerhalb des Dienstes); Erfassung von Ausgaben und Belegfotos; optional die Erfassung des letzten Abstellorts eines Fahrzeugs; Nachrichten zwischen den Mitgliedern des Kreises; Benachrichtigungen über Aktivitäten im Kreis; Statistiken, Web-Dashboard und Exporte.

Betroffene Personen. Inhaber und Verwalter der Kreise des Kunden; Fahrer und Entleiher; weitere vom Kunden eingeladene Mitglieder, etwa Beschäftigte, Kollegen, Vereinsmitglieder oder Bewohner.

Kategorien personenbezogener Daten.

Kategorie	Inhalt	Pflichtangabe
Identität	Vorname, E-Mail-Adresse; Nachname nur, wenn er aus der Anmeldung über Apple oder Google stammt	Vorname und E-Mail: ja
Profil	Profilfoto; Kontakttelefonnummer (nur in Teams-Kreisen, mit Einwilligung)	Nein
Angaben zur Rückerstattung	TWINT-Nummer oder Vergleichbares, E-Mail, Benutzername oder Zahlungslink	Nein
Fahrerangaben	Land, Führerscheinklassen und Gültigkeit, Versicherungsangaben (keine Dokumentkopien)	Nein
Kreis	Mitgliedschaft, Rolle, Einladungsstatus, Ein- und Austrittsdatum	Ja
Buchungen	Fahrzeug, Daten, Uhrzeiten, Kommentare	Ja
Fahrten	Fahrer, Datum und Uhrzeit, Kilometerstand bei Start und Ende oder Strecke	Ja
Kosten und Ausgaben	Beträge, Kostenregeln, Salden zwischen Mitgliedern, Angaben zu Ausgaben	Ja

Kategorie	Inhalt	Pflichtangabe
Fotos	Kilometerzähler, Quittungen, Belege, Fahrzeugschäden; Fahrzeugfoto	Nein
Fahrzeug	Marke, Modell, Kategorie; Kennzeichen optional	Marke und Modell: ja
Standort	Letzter Abstellort, als einzelner Punkt	Nein
Nachrichten	Nachrichten im Kreis, Absender, Zeitpunkt	Nein
Technische Daten	Interne Kennung, Push-Token, Sprache, Zeitzone	Ja

Co-oto erhebt keine Postanschriften der Nutzer. Von einem Mitglied aufgezeichnete GPS-Spuren verbleiben 90 Tage auf dem Telefon des Mitglieds und werden nie an Co-oto übermittelt.

Besondere Kategorien. Keine vorgesehen (Ziffer 3.4).

Anhang II: Technische und organisatorische Maßnahmen

Diese Maßnahmen geben den Betrieb des Dienstes am 17. November 2026 wieder. Co-oto stützt sich auf die zertifizierte Infrastruktur von Google Cloud und Firebase und verfügt selbst über keine Sicherheitszertifizierung.

1. Hosting und Verschlüsselung

- Die Daten werden in der Infrastruktur des Google-Cloud-Projekts in Europa gehostet: Cloud Firestore in der Multi-Region eur3 (Belgien und Niederlande), Cloud Storage in einer europäischen Multi-Region, Cloud Functions in europe-west1 (Belgien).
- Nach Angaben von Google haben alle Firebase-Dienste die Prüfungen nach ISO/IEC 27001 sowie SOC 1, 2 und 3 abgeschlossen; Firestore, Cloud Functions, Cloud Storage und Firebase Authentication verfügen zudem über Zertifizierungen nach ISO/IEC 27017 und 27018.
- Verschlüsselung bei der Übertragung (TLS) zwischen Apps, Web-Dashboard und Backend; standardmäßige Verschlüsselung der gespeicherten Daten durch Google.

2. Administrativer Zugang

- Der administrative Zugang zur Produktionsumgebung ist auf zwei Personen beschränkt: den Geschäftsführer und einen Entwickler des Co-oto-Teams, die beide zur Vertraulichkeit verpflichtet sind.
- Für beide ist die Mehr-Faktor-Authentifizierung bei allen Verwaltungsdiensten aktiviert: Google Cloud, Firebase, GitHub, Stripe, Mailjet, RevenueCat und Hostpoint.
- Die Audit-Logs für Administratoraktivitäten von Google Cloud zeichnen administrative Vorgänge auf und können nicht deaktiviert werden. Audit-Logs zum Datenzugriff sind nicht aktiviert.

3. Zugriffskontrolle innerhalb des Dienstes

- Anmeldung über Firebase Authentication (E-Mail-Code, Sign in with Apple, Google Sign-In). Co-oto speichert keine Benutzerpasswörter.
- Die Sicherheitsregeln von Firestore und Cloud Storage trennen die Daten nach Kreis: Ein Nutzer liest und schreibt nur in den Kreisen, denen er angehört, und nur entsprechend seiner Rolle.
- Firebase App Check (im Web mit reCAPTCHA) beschränkt den Zugriff auf das Backend auf echte App-Instanzen.

4. Datenminimierung

- Keine Postanschriften; Kennzeichen und Abstellort optional; kein Hochladen von Führerschein- oder Versicherungsdokumenten.
- GPS-Spuren verbleiben auf dem Telefon des Mitglieds und werden nie an Co-oto übermittelt.
- Keine Analyse-, Absturzbericht- oder Werbewerkzeuge Dritter in den Apps (kein Firebase Analytics, Crashlytics oder Performance Monitoring). Die Produktmessung erfolgt intern, und ihre Ereignisse werden nach 13 Monaten gelöscht.
- KI-Assistenten erhalten nur die in Ziffer 10.3 beschriebenen begrenzten Daten.

5. Verfügbarkeit und Sicherungen

- Verwaltete Firestore-Sicherungen jede Woche, Aufbewahrung 98 Tage, gespeichert zusammen mit der Datenbank in Google Cloud.
- Point-in-Time-Wiederherstellung über 7 Tage aktiviert.

6. Entwicklung und lokale Kopien

- Der Quellcode liegt in einem privaten GitHub-Repository mit Mehr-Faktor-Authentifizierung. Es enthält keine Kundendaten und keine Sicherungen. Automatisierte Tests laufen gegen die Produktionsumgebung ausschließlich mit einem internen Testkonto; Bildschirmaufnahmen dieses Kontos werden 90 Tage aufbewahrt.
- Administrative Exporte (zum Beispiel vor einem Wechsel des Kreisinhabers) werden in einen lokalen Ordner außerhalb des Repositorys geschrieben, auf einem mit FileVault verschlüsselten Datenträger.

7. Umgang mit Vorfällen

- Verletzungen werden in den Schritten Erkennung, Eindämmung, Bewertung, Meldung nach Ziffer 12 und Behebung bearbeitet und in einem internen Vorfallregister festgehalten.
- Sicherheitsmeldungen: info@co-oto.app.

8. Löschung

- Beim Löschen eines Profils oder eines Fahrzeugs wird das zugehörige Foto automatisch gelöscht. Wird ein Kreis auf Anfrage gelöscht, werden seine Daten und Fotos gelöscht (Ziffer 15).
- Gelöschte Daten verschwinden innerhalb der Fristen nach Ziffer 15.4 aus den Sicherungen.

9. Organisation

- Vertraulichkeitsverpflichtung jeder Person mit Zugang; Auswahl der Unterauftragsverarbeiter anhand ihrer dokumentierten Garantien; Überprüfung dieser Maßnahmen mindestens einmal jährlich und nach jedem erheblichen Vorfall.

Anhang III: Unterauftragsverarbeiter und weitere Anbieter

Die aktuelle Liste wird in Abschnitt 6 der Datenschutzerklärung von Co-oto geführt (Ziffer 8.2). Stand zum Zeitpunkt des Inkrafttretens:

Teil A: Unterauftragsverarbeiter für Personenbezogene Kundendaten (Ziffer 8)

Unternehmen	Dienst	Zweck	Datenstandort	Grundlage der Übermittlung
Google Cloud EMEA Ltd / Google LLC	Cloud Firestore, verwaltete Sicherungen	Speicherung der Kreisdaten	eur3: Belgien und Niederlande	EWR
Google (wie oben)	Cloud Storage for Firebase	Speicherung von Fotos	Europäische Multi-Region	EWR
Google (wie oben)	Cloud Functions, Cloud Scheduler, Secret Manager	Backend-Logik, Berechnungen, geplante Aufgaben, Endpunkt des KI-Konnektors	europe-west1 (Belgien)	EWR
Google (wie oben)	Firebase Hosting	Auslieferung der Web-App und der Adresse des KI-Konnektors	Globales Netzwerk	EU-U.S. und Swiss-U.S. DPF; ersatzweise SCC
Google (wie oben)	Firebase Authentication	Zugriffskontrolle für die Kreise des Kunden (von Co-oto auch als Verantwortlicher für Benutzerkonten genutzt)	Vereinigte Staaten	EU-U.S. und Swiss-U.S. DPF; ersatzweise SCC
Google (wie oben)	Firebase Cloud Messaging	Push-Benachrichtigungen	Weltweit, einschließlich der Vereinigten Staaten	EU-U.S. und Swiss-U.S. DPF; ersatzweise SCC
Apple Inc. / Apple Distribution International Ltd	Apple Push Notification service	Zustellung von Push-Benachrichtigungen an iOS-Geräte	Weltweit, einschließlich der Vereinigten Staaten	SCC
Mailjet SAS (Sinch-Gruppe), Frankreich	E-Mail-API, Unterkonto für Transaktions-E-Mails	Einladungen, Anmeldecodes, Benachrichtigungen	EU (Google Cloud, Frankfurt und Saint-Ghislain)	EWR
Hostpoint AG, Schweiz	E-Mail (SMTP) und Postfächer	Ersatzweg für E-Mails, erster Weg für E-Mails mit QR-Code, Support-Postfach	Schweiz	Nicht erforderlich
Anthropic Ireland, Limited / Anthropic, PBC	Claude, nach den kommerziellen Bedingungen von Anthropic	KI-Werkzeuge, die das Co-oto-Team für Entwicklung, Wartung und Support nutzt; punktuelle Verarbeitung nur der Daten, die eine bestimmte Aufgabe erfordert; keine Nutzung dieser Daten zum Training von Modellen	Vereinigte Staaten	SCC (Data Processing Addendum von Anthropic)

Karten. Die Apps zeigen Karten über die Google Maps Platform an. Öffnet ein Mitglied eine Karte, erhält Google den angezeigten Standort (etwa den letzten Abstellort eines Fahrzeugs) und technische Daten des Geräts. Google handelt für diese Daten als eigenständiger Verantwortlicher gemäß den Google Maps Controller-Controller Data Protection Terms und ist kein Unterauftragsverarbeiter.

Teil B: Anbieter, die Co-oto als eigenständiger Verantwortlicher einsetzt (zur Transparenz aufgeführt)

Unternehmen	Dienst	Zweck	Datenstandort
Apple	App Store, Sign in with Apple	Kauf von iOS-Abonnements; Anmeldeoption	Weltweit, einschließlich der Vereinigten Staaten
Google	Google Play Billing, Google Sign-In	Kauf von Android-Abonnements; Anmeldeoption	Weltweit, einschließlich der Vereinigten Staaten
RevenueCat, Inc.	Abonnementverwaltung	Validierung von In-App-Abonnements	Vereinigte Staaten (SCC)
Stripe Payments Europe Ltd / Stripe, LLC	Web-Zahlungen	Zahlung von Abonnements, die über die Website erworben werden	Irland und Vereinigte Staaten (DPF, SCC)
Google	App Check mit reCAPTCHA; Remote Config, A/B Testing, Installations	Sicherheit und App-Konfiguration	Weltweit, einschließlich der Vereinigten Staaten
Mailjet SAS	Newsletter-Konto	Newsletter an Abonnenten	EU
Matomo (selbst gehostet)	Website-Analyse	Reichweitenmessung von co-oto.app	Schweiz
Hostpoint AG	Webhosting	Hosting der Website co-oto.app	Schweiz
Web3Forms	Kontaktformular	Kontaktformular der Website	Indien, Server in den Vereinigten Staaten
Healthchecks.io	Überwachung	Überwachung geplanter Aufgaben	Lettland

Teil C: Nicht Bestandteil des Teams-Tarifs

Teltonika (Co-oto-Link-Geräte) und der Google-Compute-Engine-Server für diese Geräte, flinkey und Tapkey (Co-oto Access) sowie Smartcar werden Teams-Kunden nicht angeboten und verarbeiten keine Personenbezogenen Kundendaten im Rahmen dieses AVV. Sie werden gemäß Ziffer 8.2 aufgenommen, bevor ein solcher Dienst angeboten wird.

Unterschriften

Dieser AVV gilt ohne Unterschrift, sobald der Kunde den Teams-Tarif abonniert (Präambel (B)). Diese Seite dient Kunden, die für ihre Unterlagen ein unterzeichnetes Exemplar aufbewahren möchten.

Co-oto hat unten unterzeichnet. Der Kunde kann seinen Teil ergänzen, unterzeichnen und dieses Exemplar aufbewahren; eine Rücksendung an Co-oto ist nicht erforderlich.

Co-oto Sàrl (Auftragsverarbeiter)

Name	Deniz Ates
Funktion	Geschäftsführer
Ort und Datum	Nyon, 19. November 2026
Unterschrift	

Kunde (Verantwortlicher)

Unternehmen	
Anschrift	
Name	
Funktion	
Ort und Datum	
Unterschrift	