Co-oto Teams – Data Processing Agreement

Version 1.1. Effective date: 19 November 2026.

Preamble

(A) Co-oto Sàrl, a limited liability company under Swiss law, registered in the commercial register of the canton of Vaud under UID CHE-414.102.270, with its registered office at Chemin des Tines 5b, 1260 Nyon, Switzerland ("**Co-oto**"), provides the Co-oto application, a tool for coordinating the shared use of vehicles and sharing their costs within a circle of trust, available on iOS, Android and the web (the "**Service**").

(B) This Data Processing Agreement ("**DPA**") forms an integral part of the Co-oto Terms of Service (the "**Terms**") and is incorporated into them by reference. It applies without signature when a customer subscribes to the Teams plan, whether through the Apple App Store, Google Play or the Co-oto website. By subscribing, the customer accepts this DPA, and the person subscribing confirms that they are authorised to accept it on the customer's behalf.

(C) This DPA sets out the terms required by Article 28 of Regulation (EU) 2016/679 ("**GDPR**") and Article 9 of the Swiss Federal Act on Data Protection of 25 September 2020 ("**FADP**"). It is informed by the Standard Contractual Clauses between controllers and processors adopted by Commission Implementing Decision (EU) 2021/915.

1. Definitions

1.1 "**Customer**" means the company, association, cooperative, public body or individual acting in a professional or associative capacity that subscribes to the Teams plan and administers one or more circles in the Service.

1.2 "**Customer Personal Data**" means personal data processed by Co-oto on behalf of the Customer within the Customer's circles, as described in Annex I.

1.3 "**Data Protection Laws**" means, to the extent applicable to the processing concerned: the FADP and the Swiss Data Protection Ordinance of 31 August 2022 ("**DPO**"); the GDPR and the laws of EU/EEA Member States supplementing it; and the UK GDPR and the UK Data Protection Act 2018.

1.4 "**Personal Data Breach**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Customer Personal Data, including a data security breach within the meaning of Article 5(h) FADP.

1.5 "**Sub-processor**" means any third party engaged by Co-oto that processes Customer Personal Data on behalf of the Customer.

1.6 "**Supervisory Authority**" means the Swiss Federal Data Protection and Information Commissioner ("**FDPIC**"), a supervisory authority within the meaning of Article 51 GDPR, or the UK Information Commissioner, as applicable.

1.7 "**SCCs**" means the standard contractual clauses for transfers of personal data to third countries adopted by Commission Implementing Decision (EU) 2021/914, including the adaptations required under Swiss law as recognised by the FDPIC on 27 August 2021 and, where applicable, the UK International Data Transfer Addendum.

2. Scope

2.1 This DPA applies to the processing of Customer Personal Data by Co-oto in providing the Teams plan, including Teams plans purchased in several blocks under a custom offer and Teams access granted free of charge. It covers the mobile apps, the web dashboard, statistics and exports.

2.2 This DPA applies to the extent that the Customer acts as a controller subject to Data Protection Laws. Where a circle is used by a natural person for purely personal or household purposes, Co-oto processes the data under its Privacy Policy and applies the measures described in Annex II.

2.3 When a Teams subscription ends, the Customer's circles revert to the free plan and their data is kept (Terms, Article 18). This DPA continues to apply to that data for as long as Co-oto processes it on the Customer's behalf.

2.4 This DPA does not cover: (a) the Co-oto Link device and any other hardware add-on; (b) vehicle access or vehicle data integrations not offered to Teams customers, such as Co-oto Access or connected-car services; (c) contracts with public bodies concluded on specific terms; (d) processing for which Co-oto is an independent controller under Section 3.3.

3. Roles of the parties

3.1 **Customer as controller.** The Customer determines the purposes of processing Customer Personal Data, in particular the organisation of vehicle use, bookings, trip records, cost allocation and expense tracking within its circles. It decides whom it invites, which roles it assigns and which data it asks members to enter.

3.2 **Co-oto as processor.** Co-oto processes Customer Personal Data only on behalf of the Customer and in accordance with this DPA.

3.3 **Co-oto as independent controller.** Co-oto acts as an independent controller, under its Privacy Policy and outside this DPA, for:

1. user accounts as such (creation, sign-in credentials and sign-in by email code, Apple or Google), as one account may belong to several circles and plans. The name, email address and role shown within the Customer's circles, and the access control applied to those circles, remain Customer Personal Data;
2. subscriptions, billing, payments and accounting records;
3. security of the Service, including bot and abuse prevention (App Check) and app configuration (Remote Config);
4. product measurement through usage events stored in Co-oto's own database, detached from the user's name on account deletion and purged after 13 months, and anonymised aggregates derived from them, including anonymised activity shown on the Co-oto website;
5. communications with the Customer about its account and the Service;
6. compliance with legal obligations and the establishment, exercise or defence of legal claims.

Co-oto does not use Customer Personal Data for any other purpose of its own, does not sell it and does not use it for advertising.

3.4 **Customer responsibilities.** The Customer is responsible for:

1. the lawfulness of the processing, including an appropriate legal basis;
2. informing the data subjects in its circles as required by Articles 13 and 14 GDPR and Article 19 FADP, including about optional fields such as the contact phone number, payment details for reimbursements and driver records (licence and insurance details);
3. the accuracy of the data it enters and the roles and access rights it assigns;
4. instructing members not to enter special categories of personal data (Article 9 GDPR) or sensitive personal data (Article 5(c) FADP) in free-text fields, messages or photos;
5. where it is an employer, its obligations under employment and data protection law, including informing employees, involving employee representatives where required, and complying with Article 328b of the Swiss Code of Obligations, Article 26 of Ordinance 3 to the Swiss Employment Act, Article 88 GDPR and national law.

The Customer shall not use the Service to monitor the behaviour of employees or other drivers beyond what is necessary to organise vehicle use and allocate costs.

4. Instructions

4.1 Co-oto processes Customer Personal Data only on the documented instructions of the Customer, including with regard to transfers to third countries, unless required to do so by Swiss law or EU or Member State law to which Co-oto is subject. In that case, Co-oto informs the Customer beforehand, unless that law prohibits it on important grounds of public interest.

4.2 The Customer's documented instructions are: (a) this DPA and the Terms; (b) the Customer's configuration and use of the Service, including the settings chosen by its circle owners and managers; (c) any further written instruction sent to info@co-oto.app that is consistent with the Terms and the functionality of the Service.

4.3 Co-oto informs the Customer immediately if, in its opinion, an instruction infringes Data Protection Laws, and may suspend that instruction until the Customer confirms or changes it.

5. Obligations of Co-oto

5.1 Co-oto processes Customer Personal Data only to the extent necessary to provide the Service, and only in a way the Customer itself would be permitted to process it (Article 9(1)(a) FADP).

5.2 Co-oto assists the Customer, taking into account the nature of the processing and the information available to it, in complying with Articles 32 to 36 GDPR and Articles 7, 8, 22, 23 and 24 FADP, as set out in Sections 11 and 12.

5.3 Co-oto keeps a record of the processing it carries out on behalf of its customers where required by Article 30(2) GDPR or Article 12 FADP.

5.4 Co-oto makes available to the Customer the information necessary to demonstrate compliance with this DPA, as set out in Section 13.

6. Confidentiality

6.1 Co-oto ensures that every person it authorises to process Customer Personal Data has committed to confidentiality or is under an appropriate statutory obligation of confidentiality.

6.2 Access to Customer Personal Data is limited to the persons described in Annex II, on a need-to-know basis.

7. Security of processing

7.1 Co-oto implements and maintains the technical and organisational measures set out in Annex II to ensure a level of security appropriate to the risk, in accordance with Article 32 GDPR, Article 8 FADP and Articles 1 to 5 DPO.

7.2 Co-oto may update these measures as technology and risks evolve, provided the overall level of protection is not reduced. Material changes are reflected in the published version of Annex II.

7.3 The Customer is responsible for the security measures under its own control, in particular protecting access to owner and manager accounts, assigning roles appropriately, removing members who no longer need access, and handling exported files securely once downloaded.

8. Sub-processors

8.1 **General authorisation.** The Customer grants Co-oto a general authorisation to engage Sub-processors within the meaning of Article 28(2) GDPR and Article 9(3) FADP. The Sub-processors authorised at the effective date are listed in Annex III, Part A.

8.2 **List and notice.** Co-oto keeps an up-to-date list of its Sub-processors, with their location, activity and transfer mechanism, in section 6 of its Privacy Policy at https://www.co-oto.app/privacy-policy/. Co-oto informs the Customer of any intended addition or replacement of a Sub-processor at least thirty (30) days in advance, by email to the circle owner and by updating that list.

8.3 **Objection.** The Customer may object in writing within the notice period, on reasonable grounds relating to data protection. The parties discuss the objection in good faith. If Co-oto cannot reasonably accommodate it, the Customer may terminate its Teams subscription before the change applies. Where the Customer paid Co-oto directly through the website, Co-oto refunds the prepaid fees for the remaining period, pro rata. Where the subscription was bought through the Apple App Store or Google Play, the Customer cancels it through the store and refunds follow the store's policies. If the Customer does not object within the notice period, the change is deemed accepted.

8.4 **Urgent replacement.** Where a Sub-processor must be replaced urgently for reasons of security, availability or legal compliance outside Co-oto's control, Co-oto may make the change with shorter notice and informs the Customer as soon as possible. The right to object under Section 8.3 then runs from that notice.

8.5 **Flow-down and liability.** Co-oto imposes on each Sub-processor, by contract, data protection obligations providing in substance the same level of protection as this DPA, including sufficient guarantees on technical and organisational measures. Co-oto remains liable to the Customer for the performance of its Sub-processors' obligations (Article 28(4) GDPR), subject to Section 14. Some Sub-processors are large cloud providers offering standard terms only; Co-oto provides the relevant terms on request.

9. International transfers

9.1 **Locations.** Customer Personal Data is stored in the European Economic Area, with some email traffic handled in Switzerland, as described in Annex III. Certain technical services (authentication and push notifications) and the AI tools used by the Co-oto team involve processing in the United States.

9.2 **EU/EEA to Switzerland.** Transfers from the EU/EEA to Co-oto rely on the European Commission's adequacy decision for Switzerland (Decision 2000/518/EC), whose continued validity the Commission confirmed on 15 January 2024.

9.3 **From Switzerland.** Transfers by Co-oto to countries listed in Annex 1 DPO, including EU/EEA Member States, rely on that adequacy finding (Article 16(1) FADP).

9.4 **United States.** Co-oto transfers Customer Personal Data to a Sub-processor in the United States only: (a) where the recipient is certified under the EU-U.S. Data Privacy Framework (Commission Implementing Decision (EU) 2023/1795), the Swiss-U.S. Data Privacy Framework (Annex 1 DPO, in force since 15 September 2024) and, where applicable, the UK Extension; or (b) failing that, on the basis of the SCCs, with the Swiss adaptations and, where applicable, the UK Addendum, together with any supplementary measures required after a transfer impact assessment.

9.5 **Fallback.** If an adequacy decision relied on is invalidated, suspended or withdrawn, Co-oto relies without undue delay on the SCCs or another appropriate safeguard offered by the Sub-processor, or takes other measures to bring the transfer into compliance, and informs the Customer. No amendment to this DPA is required.

9.6 **Swiss adaptations.** Where the SCCs apply to transfers subject to the FADP: (a) the FDPIC is the competent supervisory authority for those transfers; (b) references to the GDPR are read as references to the FADP to that extent; (c) the term "Member State" does not prevent data subjects in Switzerland from exercising their rights at their place of habitual residence.

9.7 **United Kingdom.** For Customer Personal Data subject to the UK GDPR transferred to a country without UK adequacy regulations, the UK International Data Transfer Addendum to the SCCs applies.

10. AI assistant and voice integrations

10.1 **Customer control.** Integrations with AI assistants (such as the Co-oto connectors for Claude or ChatGPT) are available in the Customer's circles, and the Customer can disable them at any time in the circle settings. Keeping them enabled is an instruction from the Customer.

10.2 **Member's own assistant.** A member who chooses to use an assistant connects their own assistant, with their own account at the AI provider, and confirms the connection with a code sent by email. Co-oto sends data to an AI provider only at the request of a connected member, never on its own initiative. The AI provider acts under its own terms with the member and is not a Sub-processor of Co-oto.

10.3 **Limited data.** A connected assistant receives only the member's name and role, the circle's vehicles and their rules, and the member's own bookings. Other members appear only as "the owner" or "another member", and free text written by members is filtered before it is sent.

Connection tokens are stored hashed; access tokens expire after 1 hour and refresh tokens after 60 days.

10.4 **Voice assistants.** Voice features of the member's device operating system, such as Siri on iOS, are used at the member's initiative under the member's relationship with the device provider. The Customer can disable them in the circle settings.

11. Assistance

11.1 **Data subject requests.** Co-oto assists the Customer, by appropriate technical and organisational measures and insofar as possible, in responding to requests from data subjects under Chapter III GDPR and Articles 25 to 32 FADP. Owners and managers can view, correct and export data in their circles from the Service. If Co-oto receives such a request directly, it forwards it to the Customer without undue delay and does not respond itself, except to refer the data subject to the Customer, unless instructed otherwise or required by law.

11.2 **Impact assessments.** Co-oto provides reasonable assistance for data protection impact assessments and prior consultations with a Supervisory Authority (Articles 35 and 36 GDPR; Articles 22 and 23 FADP), primarily by making available the information in this DPA and its Annexes.

11.3 **Costs.** Assistance is free of charge where it can be provided through the Service or the published documentation. For assistance requiring significant effort, Co-oto may charge reasonable costs, notified in advance.

12. Personal Data Breach

12.1 Co-oto notifies the Customer of any Personal Data Breach affecting Customer Personal Data without undue delay and, where feasible, no later than forty-eight (48) hours after becoming aware of it (Article 33(2) GDPR; Article 24(3) FADP). Notification is sent by email to the circle owner.

12.2 The notification contains, to the extent available: the nature of the breach, including where possible the categories and approximate number of data subjects and records concerned; the contact point at Co-oto; the likely consequences; and the measures taken or proposed to address the breach and mitigate its effects. Information not available at once may be provided in phases without further undue delay.

12.3 Co-oto takes reasonable measures to contain the breach and mitigate its effects, and cooperates with the Customer so it can meet its own notification obligations. Notifying a breach is not an acknowledgement of fault or liability.

12.4 Co-oto documents every Personal Data Breach, including the facts, effects and remedial action taken.

13. Audits

13.1 On request, Co-oto makes available the information necessary to demonstrate compliance with Article 28 GDPR, Article 9 FADP and this DPA, including: a completed security questionnaire (once per year); a description of its current technical and organisational measures; and the certifications and audit reports of its main Sub-processors, in particular Google's ISO/IEC 27001

certificate and SOC reports for Firebase and Google Cloud. Co-oto does not itself hold a security certification.

13.2 Where that information is reasonably insufficient, or where an audit is required by a Supervisory Authority or follows a Personal Data Breach, the Customer may conduct an audit itself or through an independent auditor bound by confidentiality who is not a competitor of Co-oto, subject to: (a) thirty (30) days' written notice, except when required by a Supervisory Authority or following a breach; (b) one audit per twelve-month period at most; (c) a scope and duration agreed in advance and limited to Co-oto's own processing; (d) remote conduct where possible, during business hours, without access to other customers' data; (e) the Customer bearing its own costs and reimbursing Co-oto's reasonable costs, unless the audit reveals a material breach of this DPA by Co-oto.

14. Liability

14.1 Each party's aggregate liability arising out of or in connection with this DPA is limited to the fees paid by the Customer for the Teams plan in the twelve (12) months preceding the event giving rise to the claim. For matters covered by this DPA, this Section prevails over the limitation and exclusion of liability in the Terms.

14.2 Nothing in this DPA limits or excludes: (a) liability for unlawful intent or gross negligence (Article 100 of the Swiss Code of Obligations) or any other liability that cannot be limited by law; (b) the rights of data subjects under Article 82 GDPR or the FADP, or the allocation of liability between controller and processor under Article 82(4) and (5) GDPR.

15. Retention, return and deletion

15.1 **During the subscription.** Trips, bookings, expenses, photos and circle messages are kept for as long as the circle exists. Co-oto applies no shorter retention period to them. The Customer may ask at any time for specific data to be erased.

15.2 **When a member deletes their account.** The member's profile photo is deleted automatically. Trips, bookings and expenses remain in the circle with the member's name replaced (pseudonymisation). Messages remain visible to the circle with the name shown when they were sent, and are erased on request.

15.3 **Return.** During the subscription and after it ends, owners and managers can export statistics and the cost ledger from the Service. On written request, Co-oto provides an export of the Customer's circle data in a commonly used electronic format within thirty (30) days.

15.4 **Deletion.** On written request of the Customer, in particular at the end of the provision of services, Co-oto deletes the Customer's circles and the related Customer Personal Data, including photos, from its active systems within thirty (30) days, unless storage is required by Swiss law or EU or Member State law. Deleted data remains in point-in-time recovery for up to seven (7) days and in weekly backups for up to ninety-eight (98) days, after which it is overwritten. Until then, backups remain protected by this DPA and are not used for any other purpose. Authentication data held by Firebase Authentication is removed from Google's systems within the period stated by Google (currently up to 180 days).

15.5 Data that Co-oto processes as an independent controller under Section 3.3, such as accounting records kept for ten years (Article 958f of the Swiss Code of Obligations), is governed

by its Privacy Policy.

16. Term, precedence and amendments

16.1 This DPA applies for as long as Co-oto processes Customer Personal Data on behalf of the Customer. Provisions that by their nature survive termination remain in force.

16.2 In the event of conflict, the following order applies: (a) the SCCs, where applicable; (b) this DPA; (c) the Terms.

16.3 Co-oto may amend this DPA to reflect changes in Data Protection Laws, decisions of courts or Supervisory Authorities, or changes to the Service, provided the level of protection of Customer Personal Data is not materially reduced. Co-oto notifies material amendments at least thirty (30) days in advance by email to the circle owner. Earlier versions are available on request.

17. Governing law and jurisdiction

17.1 This DPA is governed by Swiss law, excluding its conflict-of-laws rules.

17.2 The courts of Nyon, canton of Vaud, Switzerland, have exclusive jurisdiction, subject to appeal to the Swiss Federal Supreme Court.

17.3 Sections 17.1 and 17.2 apply without prejudice to: (a) mandatory provisions of the GDPR and of EU/EEA Member State law, including the rights of data subjects under Articles 77 to 79 GDPR; (b) the governing law and jurisdiction clauses of the SCCs, where applicable; (c) mandatory consumer protection rules.

18. EU representative and contact

18.1 Co-oto has designated VGS Datenschutzpartner GmbH, Am Kaiserkai 69, 20457 Hamburg, Germany, as its representative in the European Union under Article 27 GDPR. Its email address is given in section 1 of the Co-oto Privacy Policy.

18.2 Questions, instructions, requests and notifications under this DPA: Co-oto Sàrl, Deniz Ates, Chemin des Tines 5b, 1260 Nyon, Switzerland, info@co-oto.app.

Annex I: Details of processing

Parties. Controller: the Customer, contactable through the email address of its circle owner. Processor: Co-oto Sàrl, Nyon, Switzerland, info@co-oto.app; EU representative: VGS Datenschutzpartner GmbH, Hamburg.

Subject matter. Provision of the Teams plan: software for coordinating the shared use of vehicles within a circle and sharing the related costs.

Duration. For as long as Co-oto processes Customer Personal Data on behalf of the Customer, plus the deletion periods in Section 15.

Nature of processing. Collection, recording, organisation, storage, retrieval, consultation, calculation (costs, balances, statistics), display, transmission (synchronisation, messages, push notifications, transactional emails), export, restriction and erasure.

Purposes, on behalf of the Customer. Managing circle membership and roles; booking vehicles and keeping a shared calendar; recording trips; calculating costs and balances between members (payments take place outside the Service); recording expenses and supporting photos; optionally recording where a vehicle was last parked; messages between circle members; notifications about circle activity; statistics, web dashboard and exports.

Data subjects. Owners and managers of the Customer's circles; drivers and borrowers; other members invited by the Customer, such as employees, colleagues, association members or residents.

Categories of personal data.

Category	Content	Required
Identity	First name, email address; last name only when provided by Apple or Google sign-in	First name and email: yes
Profile	Profile photo; contact phone number (Teams circles only, with consent)	No
Reimbursement details	TWINT number or equivalent, email, username or payment link	No
Driver record	Country, licence categories and validity, insurance details (no document copies uploaded)	No
Circle	Membership, role, invitation status, dates of joining and leaving	Yes
Bookings	Vehicle, dates, times, comments	Yes
Trips	Driver, date and time, start and end odometer readings or distance	Yes
Costs and expenses	Amounts, cost rules, balances between members, expense details	Yes
Photos	Odometer, receipts, supporting documents, vehicle damage; vehicle photo	No
Vehicle	Make, model, category; licence plate optional	Make and model: yes
Location	Last parking location, as a single point	No

Category	Content	Required
Messages	Messages in the circle, sender, time	No
Technical	Internal identifier, push notification token, language, time zone	Yes

Co-oto does not collect users' postal addresses. GPS traces recorded by a member stay on the member's phone for 90 days and are never sent to Co-oto.

Special categories. None intended (Section 3.4).

Annex II: Technical and organisational measures

These measures reflect the Service as operated on 17 November 2026. Co-oto relies on the certified infrastructure of Google Cloud and Firebase and does not itself hold a security certification.

1. Hosting and encryption

- Data is hosted in Google Cloud project infrastructure in Europe: Cloud Firestore in the eur3 multi-region (Belgium and the Netherlands), Cloud Storage in a European multi-region, Cloud Functions in europe-west1 (Belgium).
- Google states that all Firebase services have completed ISO/IEC 27001 and SOC 1, 2 and 3 evaluations, and that Firestore, Cloud Functions, Cloud Storage and Firebase Authentication also hold ISO/IEC 27017 and 27018 certifications.
- Encryption in transit (TLS) between apps, web dashboard and backend; encryption at rest by default by Google.

2. Administrative access

- Administrative access to production is limited to two persons: the managing director and one developer of the Co-oto team, both bound by confidentiality.
- Multi-factor authentication is enabled for both on every administration service: Google Cloud, Firebase, GitHub, Stripe, Mailjet, RevenueCat and Hostpoint.
- Google Cloud Admin Activity audit logs record administrative actions and cannot be disabled. Data Access audit logs are not enabled.

3. Access control within the Service

- Sign-in through Firebase Authentication (email code, Sign in with Apple, Google Sign-In). Co-oto stores no user passwords.
- Firestore and Cloud Storage security rules separate data by circle: a user reads and writes only the circles they belong to, according to their role.
- Firebase App Check (with reCAPTCHA on the web) restricts backend access to genuine app instances.

4. Data minimisation

- No postal addresses; licence plate and parking location optional; no upload of licence or insurance documents.
- GPS traces stay on the member's phone and are never sent to Co-oto.
- No third-party analytics, crash reporting or advertising tools in the apps (no Firebase Analytics, Crashlytics or Performance Monitoring). Product measurement is internal and its events are purged after 13 months.
- AI assistants receive only the limited data described in Section 10.3.

5. Availability and backups

- Managed Firestore backups every week, kept 98 days, stored with the database in Google Cloud.
- Point-in-time recovery enabled over 7 days.

6. Development and local copies

- Source code is kept in a private GitHub repository with multi-factor authentication. It contains no customer data and no backups. Automated tests run against production with an internal test account only; their screenshots of that account are kept 90 days.
- Administrative exports (for example before a change of circle owner) are written to a local folder outside the repository, on a disk encrypted with FileVault.

7. Incident management

- Breaches are handled through detection, containment, assessment, notification under Section 12, remediation and an internal incident register.
- Security reports: info@co-oto.app.

8. Deletion

- Deleting a profile or a vehicle deletes its photo automatically. Deleting a circle on request deletes its data and photos (Section 15).
- Deleted data leaves backups within the periods in Section 15.4.

9. Organisation

- Confidentiality commitments of every person with access; selection of Sub-processors on the basis of their documented guarantees; review of these measures at least once a year and after any significant incident.

Annex III: Sub-processors and other providers

The current list is kept in section 6 of the Co-oto Privacy Policy (Section 8.2). Status on the effective date:

Part A: Sub-processors of Customer Personal Data (Section 8)

Entity	Service	Purpose	Data location	Transfer mechanism
Google Cloud EMEA Ltd / Google LLC	Cloud Firestore, managed backups	Storage of circle data	eur3: Belgium and the Netherlands	EEA
Google (as above)	Cloud Storage for Firebase	Storage of photos	European multi-region	EEA
Google (as above)	Cloud Functions, Cloud Scheduler, Secret Manager	Backend logic, calculations, scheduled tasks, AI connector endpoint	europe-west1 (Belgium)	EEA
Google (as above)	Firebase Hosting	Serving the web app and the AI connector address	Global network	EU-U.S. and Swiss-U.S. DPF; SCCs as fallback
Google (as above)	Firebase Authentication	Access control to the Customer's circles (also used by Co-oto as controller for user accounts)	United States	EU-U.S. and Swiss-U.S. DPF; SCCs as fallback
Google (as above)	Firebase Cloud Messaging	Push notifications	Global, including the United States	EU-U.S. and Swiss-U.S. DPF; SCCs as fallback
Apple Inc. / Apple Distribution International Ltd	Apple Push Notification service	Delivery of push notifications to iOS devices	Global, including the United States	SCCs
Mailjet SAS (Sinch group), France	Email API, transactional sub-account	Invitations, sign-in codes, notifications	EU (Google Cloud, Frankfurt and Saint-Ghislain)	EEA
Hostpoint AG, Switzerland	Email (SMTP) and mailboxes	Backup email route, first route for emails with a QR code, support mailbox	Switzerland	None required
Anthropic Ireland, Limited / Anthropic, PBC	Claude, under Anthropic's commercial terms	AI tools used by the Co-oto team for development, maintenance and support; occasional processing of only the data a given task requires; no use of that data to train models	United States	SCCs (Anthropic Data Processing Addendum)

Maps. The apps display maps through Google Maps Platform. When a member opens a map, Google receives the location displayed (such as a vehicle's last parking location) and technical data from the device. Google acts as an independent controller for this data under the Google Maps Controller-Controller Data Protection Terms and is not a Sub-processor.

Part B: Providers used by Co-oto as independent controller (listed for transparency)

Entity	Service	Purpose	Data location
Apple	App Store, Sign in with Apple	Purchase of iOS subscriptions; sign-in option	Global, including the United States
Google	Google Play billing, Google Sign-In	Purchase of Android subscriptions; sign-in option	Global, including the United States
RevenueCat, Inc.	Subscription management	Validation of in-app subscriptions	United States (SCCs)
Stripe Payments Europe Ltd / Stripe, LLC	Web payments	Payment of subscriptions bought on the website	Ireland and United States (DPF, SCCs)
Google	App Check with reCAPTCHA; Remote Config, A/B Testing, Installations	Security and app configuration	Global, including the United States
Mailjet SAS	Newsletter account	Newsletter to subscribers	EU
Matomo (self-hosted)	Website analytics	Audience measurement of co-oto.app	Switzerland
Hostpoint AG	Web hosting	Hosting of the co-oto.app website	Switzerland
Web3Forms	Contact form	Website contact form	India, servers in the United States
Healthchecks.io	Monitoring	Monitoring of scheduled tasks	Latvia

Part C: Not part of the Teams plan

Teltonika (Co-oto Link devices) and the Google Compute Engine server for those devices, flinkey and Tapkey (Co-oto Access), and Smartcar are not offered to Teams customers and process no Customer Personal Data under this DPA. They will be added under Section 8.2 before any such service is offered.

Signatures

This DPA applies without signature when the Customer subscribes to the Teams plan (Preamble (B)). This page is for customers who wish to keep a signed copy for their records.

Co-oto has signed below. The Customer may complete and sign its part and keep this copy; it does not need to be returned to Co-oto.

Co-oto Sàrl (Processor)

Name	Deniz Ates
Title	Managing Director
Place and date	Nyon, 19 November 2026
Signature	

Customer (Controller)

Organisation	
Address	
Name	
Title	
Place and date	
Signature	