Documents

Data processing agreement

Version 1.1 · Updated: 2026-11-21

This document sets out the terms on which Trackomo processes personal data on a customer's instructions, in accordance with Article 28 of Regulation 2016/679 (GDPR). You accept it electronically when registering your company in the application, and you can also download it as a PDF.

1. Parties

The controller is the customer using the Trackomo application, below the "Controller". The processor is IT Dominik Pakuński, ul. Zielona 4, 96-500 Sochaczew, Poland, VAT number PL8371840336, contact@trackomo.com, below the "Processor".

This agreement is concluded when the Terms are accepted while creating an organisation in the application - the Terms name it as Annex 2. The current version of this document is always available at trackomo.com, and the Processor gives notice of every change by e-mail.

2. Subject matter, nature and purpose

The Processor processes personal data solely in order to provide the vehicle and transport condition monitoring service, to the extent needed for it to work: receiving data from devices, storing it, presenting it in the panel, generating reports and sending notifications. In the routes module the service also covers planning and settling deliveries, sending notices to recipients named by the Controller and giving them a link to track that one delivery.

Processing is continuous and lasts for the term of the service contract.

3. Categories of data and data subjects

Categories of data subjects:

- users of the application on the Controller's side (people who create and operate the account)
- drivers and other people operating the Controller's vehicles
- people named as recipients of reports and notifications
- recipients of the Controller's deliveries and contact people at delivery points

Categories of data:

- identification and contact data: name, email address, job title or role
- vehicle location data: coordinates, time, speed, heading, route
- vehicle operating data: ignition, driving and stopping hours, distance
- technical vehicle data: fuel level, voltage, fault codes, temperature sensor readings
- driver identifiers: an iButton key number or an assignment to a vehicle
- technical access data: IP addresses, browser information, audit log entries
- delivery point and recipient data: name, address, coordinates, contact person, email address and phone number entered by the Controller

The Processor does not process special categories of data under Article 9 GDPR or data on criminal convictions as part of the service. The Controller undertakes not to enter such data into the application, in particular in free-text fields.

4. The Processor's obligations

- processes data only on the Controller's documented instructions, which include the use of the application's features, and informs the Controller if an instruction infringes the law
- ensures that persons authorised to process the data have undertaken to keep it confidential
- applies the security measures set out in section 6

- assists the Controller with its obligations under Articles 32 to 36 GDPR, including data protection impact assessments
- assists with data subject requests, to the extent available in the application and through data export
- on termination of the service, deletes or returns the data as set out in section 9
- makes available the information needed to demonstrate compliance and allows audits as set out in section 8

5. The Controller's obligations

- determines the legal basis for processing in relation to its own employees and drivers and meets the information duties
- when monitoring company vehicles, complies with national employment law, including recording the purpose, scope and manner of monitoring and informing employees before it starts
- decides whether to switch on notices to delivery recipients and secures a lawful basis for contacting them, including the information duty towards them
- grants and revokes access for users in its organisation and keeps those permissions appropriate
- does not enter into the application data going beyond the scope in section 3

6. Security measures

- TLS encryption of traffic for the panel, the API and mail
- user passwords stored only as an Argon2id hash
- role-based access control on a least-privilege basis
- two-factor sign-in available to users and required for administrative access
- an audit log recording configuration changes with the IP address and the user identifier
- separation of each organisation's data at application and database level
- availability monitoring and technical alerts for the operations team
- daily database backups with access limited to the administrator, verified weekly by a test restore and kept for 14 days

7. Sub-processors

The Controller gives general authorisation for the Processor to use the sub-processors listed below:

Sub-processor	Scope	Location
OVH SAS	hosting of application, database and mail servers	Germany (Frankfurt am Main)
Cloudflare, Inc.	DNS for the trackomo.com domain	USA / global network
Google Ireland Limited / Google LLC	mail from the contact address, signing in with a Google account	Ireland / USA

The Processor notifies the Controller by email of any intended addition or replacement of a sub-processor at least 30 days in advance. The Controller may object on reasonable grounds within that period. If an objection cannot be resolved, the Controller may terminate the service contract with effect at the end of the billing period, at no additional cost.

The Processor imposes on its sub-processors data protection obligations equivalent to those in this agreement and remains liable to the Controller for their acts.

8. Audits

The Controller may audit the processing no more than once per calendar year, on at least 30 days' notice, on working days and in a manner that does not disrupt the Processor's operations. An audit must not compromise the confidentiality of other customers' data.

Instead of an on-site audit the Processor may provide a current independent audit report or answers to a security questionnaire, provided they cover the scope indicated by the Controller. Additional audits beyond that limit are at the Controller's cost.

9. Personal data breaches

The Processor notifies the Controller of a personal data breach without undue delay and in any event within 48 hours of becoming aware of it. The notification describes the nature of the breach, the categories and approximate number of data subjects and records concerned, the likely consequences and the measures taken or proposed.

Where full information is not available at once, the Processor provides it in phases rather than waiting for the analysis to finish. Notifying the supervisory authority and the data subjects remains the Controller's obligation.

10. Termination and the fate of the data

On termination of the service the Controller has 30 days to download its data in a reusable form – reports as PDF and CSV, and data export through the API. After that period the Processor deletes the data from the production system.

Backups containing deleted data expire on their own cycle, no later than 30 days after deletion. At the Controller's request the Processor confirms the deletion in writing or by email.

11. Liability and final provisions

The parties are liable on the basis set out in Article 82 GDPR. In all other respects the service contract and Polish law apply. Where this agreement conflicts with the terms of service on data protection matters, this agreement prevails.

Every version of this document carries a number and a date. The Processor announces a change of version by email at least 30 days before it takes effect; continued use of the service after that date constitutes acceptance of the new version, and refusal entitles the Controller to terminate the service contract.