PRIVACY POLICY

FLEETONAIR PLATFORM

Version effective as of 2 November 2026

This document explains how we collect, use and protect personal data in connection with the FleetOnAir platform — a telematics system for vehicle fleet management that we offer under the SaaS model.

FleetOnAir is a B2B solution intended for companies and persons conducting business activity. The System may be used by persons acting on behalf of or for the benefit of the Client, e.g. fleet administrators, employees, associates or drivers.

This Policy has been prepared in accordance with the GDPR (Regulation (EU) 2016/679), the Act of 10 May 2018 on the Protection of Personal Data, the Act of 18 July 2002 on the Provision of Electronic Services and the Act of 12 July 2024 – Electronic Communications Law.

We act as the data controller with respect to the Client's contact persons, account users, website visitors and persons corresponding with us. With respect to the data of drivers, employees and other persons using the Client's vehicles, we generally act as a processor, processing the data on the Client's instructions. Detailed information about our roles can be found further in this Policy.

1. Personal data controller

The controller of personal data within the scope described in this document is Core Logic spółka z ograniczoną odpowiedzialnością with its registered office in Kraków, ul. Feliksa Radwańskiego 15/1, 30-065 Kraków, entered in the register of entrepreneurs of the National Court Register (KRS) under number 0000542498, NIP 6762484560, REGON 360742116 (hereinafter "FleetOnAir", "Core Logic", "we").

In matters concerning the protection of personal data — including in order to exercise the rights described in section 10 — you may contact the Data Protection Officer (DPO) appointed by us at iod@core-logic.com or privacy@fleetonair.com, as well as by traditional mail to the company's registered office address.

Messages sent to iod@core-logic.com or privacy@fleetonair.com are handled by the Data Protection Officer appointed by us.

By running a company profile on LinkedIn and other social media profiles, we act as joint controllers of the data of persons visiting these profiles together with the entities operating the platforms — primarily LinkedIn Ireland Unlimited Company and Meta Platforms Ireland Ltd. (Facebook, Instagram). Each platform applies its own data processing rules described in its privacy policy. In matters concerning data collected through our profiles, you may contact us at the address indicated above.

2. Scope of this Policy

This document covers all elements of the FleetOnAir System and all situations in which you contact us in connection with our offer. In particular, the Policy applies to:

- the fleetonair.com website, including its subdomains and landing pages
- the fleet administrator web panel, available after logging in at the address provided to the Client after the conclusion of the agreement
- the web application for Authorised Users
- the mobile application for Android and iOS
- the Ticketing Panel used for technical support

- commercial correspondence, the sales process and pre-sales and after-sales support

These elements are jointly referred to as the "System" or the "Service".

3. Our roles in data protection

Due to the nature of the Service, we act in two different roles — depending on whose data we process and in what context.

3.1. We are the controller

We act in this role with respect to the data of persons whose data we receive directly from them or from the Client in the context of concluding and performing the agreement. We are the controller, among others, with respect to:

- the Client's contact persons — the person representing the company when concluding the agreement and persons designated for commercial, technical and billing contact
- Authorised Users, with respect to their authentication data, security event logs and account parameters
- persons visiting the fleetonair.com website, filling in contact forms and registering an Account in the System on their own (including during the free trial period)
- persons conducting commercial correspondence with us, sending requests for quotation, holding conversations on LinkedIn or attending networking meetings
- recipients of the newsletter and marketing materials

In each of these cases, we independently determine the purposes and means of data processing — in compliance with the principles of the GDPR.

3.2. We are the processor

We act in this role with respect to the data of third parties which the Client enters into the System or which are automatically collected in the System in connection with the operation of the GPS Devices. This concerns primarily:

- drivers, employees and other persons using the Client's vehicles
- data entered by the Client about Authorised Users (position, function, vehicle assignments)
- persons associated with vehicles indicated by the Client in the System configuration

In this role, we process data only on the documented instructions of the Client, under the terms set out in the data processing agreement concluded with the Client (Art. 28 GDPR). The controller of this data is the Client — it is the Client who determines the purposes and means of its processing.

> If you are a driver or an employee of a company using FleetOnAir and you are reading this Policy because you want to find out what happens to your location data — please remember that your employer is the controller of this data. Questions about the purpose, scope and legal basis of the monitoring should be addressed to your employer in the first place. We process this data technically, on your employer's instructions.

4. Scope of data collected

The scope of data we process depends on how you use the System or contact us. Below you will find the complete list of categories.

4.1. Identification data of the Client and related persons

- the Client's business name and legal form, registered office address, correspondence address
- NIP, KRS, REGON, bank account number
- first name, surname, position, business e-mail address and telephone number of persons representing the Client and persons designated for contact

4.2. Account data and Authorised User data

- login (usually an e-mail address)
- password in the form of a cryptographic hash (we have no access to the password in plain text)
- additional information entered by the Client or the account administrator (first name, surname, position, department, telephone number)
- scope of permissions in the System, role assignments
- date and time of logins, IP address, type of browser or mobile application
- history of actions in the System recorded in the audit log

4.3. Vehicle and driver data (in the Fleet Tracker package and the CAN/OEM Module)

- vehicle identification data: registration number, VIN, make, model, year of manufacture, technical data entered by the Client
- data from GPS Devices based on the OBD-II interface: real-time location, speed, ignition status, history of routes and stops, security events (collision alert, towing attempt, signal jamming)
- diagnostic data from the vehicle's computer (OBD): mileage, fuel level, battery voltage, DTC error codes — to the extent made available by the vehicle
- advanced vehicle data from the CAN bus or factory OEM telematics (activated as part of the CAN/OEM Module): fuel level and consumption, engine temperature, odometer readings, operating parameters of vehicle systems
- driver identification data (e.g. iButton/Dallas identifiers) — if the Client has activated the identification module
- driver data entered by the Client: first name, surname, identifier, telephone number, vehicle assignments, results of driving style analyses

4.4. Data from using the Fleet Starter package

The Fleet Starter package does not include GPS monitoring — within it, the Client may enter into the System and manage:

- vehicle records, fleet documents, events, faults, damage
- inspection schedules, calendars, reminders
- manually entered mileage records

The scope of data entered in the Fleet Starter package depends solely on the Client's decision.

4.5. Billing data

- order number, selected package, list of active Add-on Modules
- payment history, dates, amounts, methods
- data of issued VAT invoices and pro forma invoices (Deposit)

4.6. Technical data collected automatically

- the IP address from which the connection to the System is made
- browser type and version, operating system, language, screen resolution

- mobile device identifier, FleetOnAir application version
- dates and times of actions in the System, server logs, error logs
- approximate geographic location derived from the IP address

4.7. Correspondence data

- content of messages sent via the form, e-mail, Ticketing Panel, chat, LinkedIn
- date of contact, subject, attachments
- notes from sales conversations kept in the CRM system

5. Purposes and legal bases of processing

For each purpose of processing, we indicate the legal basis on which we rely.

Purpose	Description	Legal basis
Conclusion and performance of the agreement with the Client	Negotiations, signing of the SaaS agreement, launching the System, providing access credentials, assigning GPS Devices to the account, handling handover protocols, changes to the package configuration and Add-on Modules.	Art. 6(1)(b) GDPR — necessity for the conclusion and performance of the agreement (for sole traders); Art. 6(1)(f) GDPR — legitimate interest consisting in the performance of the agreement with the entity employing the contact persons.
Provision of the Service — access to the System and processing of vehicle data	Maintaining the Account, authenticating Authorised Users, collecting data from GPS Devices, presenting location and telemetry data, generating reports, handling Add-on Modules.	Art. 6(1)(b) GDPR (performance of the agreement). With respect to the data of the Client's drivers — we act as a processor on the basis of the data processing agreement; the legal basis with respect to the data subjects is indicated by the Client.
Settlement of the agreement and invoicing	Issuing VAT invoices and pro forma invoices for the Deposit, keeping accounting records, archiving accounting documentation, handling payments.	Art. 6(1)(c) GDPR in conjunction with the Accounting Act, the VAT Act and the Tax Ordinance.
Handling of tickets in the Ticketing Panel and technical support	Receiving tickets, diagnosis, technical correspondence, remote assistance, handling annexes and configuration changes.	Art. 6(1)(b) GDPR (performance of the agreement).
Handling of commercial correspondence and requests for quotation	Responding to enquiries sent via the form, e-mail, telephone or LinkedIn; conducting the sales process, preparing offers, contact after industry events.	Art. 6(1)(f) GDPR — legitimate interest consisting in conducting commercial activity.
Own B2B marketing	Newsletter, information about new System features, invitations to webinars and trade fairs, remarketing campaigns on LinkedIn, Meta and Google networks.	Art. 6(1)(f) GDPR (legitimate interest), and with respect to marketing conducted by electronic means — Art. 398 of the Act of 12 July 2024 – Electronic Communications Law (the recipient's consent to receive commercial information, which also applies to B2B relationships).

Purpose	Description	Legal basis
Integration with partners (TOLL, parking, fuel cards)	Transfer of location and identification data to third parties — solely within the scope of the activated Add-on Module.	Art. 6(1)(b) GDPR (performance of the agreement) with respect to the Client; with respect to the data subject, the legal basis is indicated by the separate controller (the module partner).
Internal analytics and System development	Examining System performance, detecting errors, A/B tests, analysing the use of features — usually on pseudonymised or aggregated data.	Art. 6(1)(f) GDPR — legitimate interest consisting in product development.
Securing and pursuing claims	Archiving contractual documentation, correspondence history and logs in case of a dispute, official inspection or court proceedings.	Art. 6(1)(f) GDPR — legitimate interest consisting in securing claims.
System security and abuse prevention	Detecting unauthorised access attempts, logging security events, protection against attacks, audit log of administrative actions.	Art. 6(1)(f) GDPR — legitimate interest consisting in protecting the System and Clients' data.

6. Where we obtain your data from

In most situations, we receive data directly from you — during agreement negotiations, self-registration of an Account in the System (including a free trial account), filling in the contact form, a sales conversation or use of the System. In the case of Authorised Users, the data is provided to us by the Client, who maintains their Accounts in the System.

Location and telemetry data is generated automatically by the GPS Devices installed in the Client's vehicles and transmitted to our servers via a SIM card. Some technical data (IP address, device type, logs) is recorded automatically when the System is used.

We do not buy data from external brokers and we do not link FleetOnAir profiles with profiles held on other services — except for integrations expressly activated by the Client (e.g. the LinkedIn Insight Tag, to the extent and on the basis of the consents given in the cookie panel).

> In the B2B environment, the data of contact persons sometimes reaches us through their employers or colleagues — for example, when the Client's company provides us with the data of its representative for commercial or technical contact. In such a case, we inform the person concerned of the processing of their data at the first direct contact with us, in accordance with Art. 14 GDPR.

> Providing personal data is voluntary — except in situations where it is required by law (e.g. data necessary to issue a VAT invoice). However, failure to provide the required data may prevent the conclusion of the agreement, activation of the account or provision of the selected Add-on Module.

7. Location data — special note

The essence of the Fleet Tracker package is monitoring the location of the Client's vehicles. Location data belongs to a category that is particularly intrusive to privacy — its analysis makes it possible to draw conclusions about the habits, whereabouts, working time and rest time of the person driving the vehicle.

We protect this data with measures appropriate to the risk — encrypted transmission, role-based access control, an audit log of administrative access, infrastructure segmentation and two-factor authentication for

personnel with access to production data.

At the Client's request, the System can be configured so that, during trips marked as private, it does not collect coordinates or route history, but only driving style data. It is also possible to completely disable the collection of location data at the GPS Device level. In that case, coordinates are not transmitted to our servers.

> **The Client's obligations towards drivers and employees:** As the controller of the data of drivers and employees, the Client is obliged to fulfil the information obligation towards them (Art. 13 GDPR), to have an appropriate legal basis for the processing (most often Art. 6(1)(f) GDPR — the employer's legitimate interest, subject to the balancing test) and — in employment relationships — to take into account the restrictions under Art. 22^2 and 22^3 of the Labour Code concerning employee monitoring. The Client is solely responsible for fulfilling these obligations.

8. Recipients of data

We operate within an ecosystem of technology providers and partners who support the provision of the Service. Each of them is bound to us by an appropriate data processing agreement (in the role of processor) or acts as a separate controller — depending on the nature of the relationship.

8.1. Entities to which we entrust processing

- the provider of cloud infrastructure and data centres (centres located in the European Union)
- the provider of the e-mail system and team communication tools
- the provider of the CRM system in which we keep the history of relationships with Clients
- the provider of the invoicing system and the accounting office
- providers of the Ticketing Panel and helpdesk tools
- providers of tools for sending newsletters, mailings and marketing automation
- SIM card operators providing data transmission from GPS Devices
- the manufacturer of the GPS Devices (Teltonika Telematics) — with respect to device servicing
- IT subcontractors and companies providing implementation, training and consulting services on our behalf
- law firms, tax advisers, auditors — where necessary

We make the current list of key processors available to Clients in an annex to the data processing agreement and on request.

8.2. Add-on Module partners (separate controllers)

Some integrations involve the transfer of selected data to partners who process it as independent controllers. This applies to:

- operators of municipal parking zones — after activation of the parking integration module
- issuers of fuel and fleet cards — after activation of the fuel settlement module
- providers of analytics and advertising tools present on the fleetonair.com website — within the scope of the consents given in the cookie panel

The privacy policies of these partners, together with the scope of the data transferred, are made available upon activation of the relevant module or in the consent panel.

8.3. Public authorities

Data may be disclosed to authorities authorised under the law — the police, the public prosecutor's office, courts, tax inspection authorities, the President of the Personal Data Protection Office and the Chief Inspector of Road Transport. We verify each request in terms of its legal basis and scope, refusing to disclose data beyond what the law requires.

9. Transfer of data outside the European Economic Area

We store and process FleetOnAir System data on our own server infrastructure located in Poland. In a typical scenario of using the System, data does not leave the EEA.

The exception are certain supporting tools present mainly on the fleetonair.com website and in marketing systems (Google analytics tools, LinkedIn Insight Tag, Meta Pixel, newsletter tools). Transfers to providers based outside the EEA (mainly in the United States) take place on the basis of a European Commission adequacy decision (EU–U.S. Data Privacy Framework — provided that the given provider holds a current certification) or on the basis of standard contractual clauses with supplementary technical measures (pseudonymisation, encryption).

A detailed list of tools involving transfers outside the EEA is made available in the cookie consent management panel.

10. Your rights

The GDPR grants data subjects a set of rights. You may exercise each of them by sending a request to privacy@fleetonair.com.

1. Right of access (Art. 15 GDPR) — you may ask whether we process your data and what information we hold about you; on request, we will provide you with a copy.
2. Right to rectification (Art. 16 GDPR) — if the data is incomplete or incorrect, you may request its correction.
3. Right to erasure (Art. 17 GDPR) — in the cases specified in the GDPR, you may request the erasure of data. We must retain certain data due to legal obligations (e.g. invoices — for 5 years from the end of the calendar year in which the tax payment deadline expired).
4. Right to restriction of processing (Art. 18 GDPR) — you may request a temporary suspension of active processing, e.g. while the accuracy of the data is being verified.
5. Right to data portability (Art. 20 GDPR) — you may receive data processed on the basis of consent or an agreement in a machine-readable format.
6. Right to object (Art. 21 GDPR) — you may at any time object to processing based on legitimate interest, including direct marketing.
7. Right to withdraw consent — if we process data on the basis of consent, you may withdraw it at any time; withdrawal does not affect the lawfulness of processing carried out before the withdrawal.
8. Right to lodge a complaint with the President of the Personal Data Protection Office (ul. Stawki 2, 00-193 Warsaw, uodo.gov.pl).

We respond to requests without undue delay, and no later than within one month; in complex cases, this period may be extended by a further two months, of which we will notify you in advance.

> If you are a driver or an employee of the Client and wish to exercise the above rights with respect to your location or telemetry data — please address your request to the Client (your employer), who is the controller of this data. We will forward any such request sent directly to us to the Client for handling.

11. Automated decision-making and profiling

We do not make decisions concerning data subjects based solely on automated processing that would produce legal effects concerning them or similarly significantly affect them.

The System provides the Client with algorithm-based analytical features — including the Eco Driving and Safe Driving modules and predictive modules. The results of these analyses are informative in nature — it is the Client, as the controller, who decides how to use the data generated by the System (e.g. for assessing driving style or planning training). Any consequences for the driver or employee are decisions of the Client, not ours.

12. Retention periods

We store individual categories of data for different periods — for as long as this is justified by the purpose of collection or required by law.

Data category	Retention period
Contractual data and correspondence from negotiations	For the duration of the agreement; after its termination, for the limitation period for claims arising from the agreement — generally 3 years for claims related to conducting business activity (Art. 118 of the Civil Code).
Account data (login, password hash, preferences)	For the term of the agreement. After termination of the agreement, Account data is deactivated and deleted within the period specified in the Terms of Service (as a rule, 30 days from termination of the agreement), subject to backup copies deleted in the cycle appropriate for the backup system and to data whose further retention is required by law.
Location and telemetry data of the Client's vehicles, route history, reports	In the System, route history in the Fleet Tracker package is stored for 6 months, in accordance with the Agreement. After termination of the agreement, the data is deleted within 30 days, unless the Client has requested earlier deletion or an export of the data.
Accounting documentation and VAT invoices	5 years from the end of the calendar year in which the tax payment deadline expired (Art. 74 of the Accounting Act in conjunction with Art. 86 § 1 of the Tax Ordinance).
Security event logs, audit log, administrative access logs	Up to 24 months. If an incident is detected, logs relating to the incident are stored until the matter is closed.
Tickets in the Ticketing Panel, technical support history	For the term of the agreement and, after its termination, until the limitation of claims.
Data from the contact form and requests for quotation without conclusion of an agreement	Up to 24 months from the last contact or until the person objects to further communication.
Data processed on the basis of consent (newsletter, marketing)	Until consent is withdrawn and, after withdrawal, to the extent necessary to demonstrate that it previously existed.

Data category	Retention period
Data collected by cookies and analytics tools	In accordance with the lifetime of individual cookies indicated in the consent management panel — from the browser session up to 24 months.

13. Data security

We treat data security as a priority. The technical and organisational measures implemented include, among others:

- encryption of transmission using TLS 1.2+ between user devices and FleetOnAir servers
- encryption of sensitive data at rest on the servers
- storage of passwords as hashes generated by algorithms resistant to brute-force attacks (bcrypt/argon2)
- two-factor authentication available to Authorised Users
- regular backups stored in two independent locations
- role-based access control (RBAC), the principle of least privilege
- audit log of administrative access to Clients' data
- regular security reviews, penetration tests, vulnerability scanning
- an incident response procedure — in the event of a personal data breach, we notify the Client without undue delay, and no later than 48 hours after becoming aware of the breach, in accordance with Art. 33(2) GDPR
- regular staff training in data protection and cybersecurity
- verification of processors (due diligence) before commencing cooperation and periodically during its course

14. Cookies and similar technologies

14.1. What cookies are

Cookies are small text files saved by the browser in the device's memory. They make it possible to recognise the user on subsequent visits, remember preferences and measure the effectiveness of activities. In addition to cookies, we also use similar technologies — local browser storage (localStorage), tracking pixels and mobile device identifiers.

14.2. Types of cookies

- necessary cookies — required for the website to work and for logging in to the panel and applications; we always use them without asking for consent, because the System cannot function without them
- functional cookies — remember preferences, e.g. language and display settings
- analytics cookies — help us understand how users use the website and the System; we use them after obtaining consent
- marketing cookies — used to measure the effectiveness of campaigns on LinkedIn, Meta and Google; they require separate consent

14.3. Managing cookies

On your first visit, a consent selection panel appears where you can accept all cookies, reject optional ones or select specific categories. You can change your settings at any time — a link to the panel is located in the website footer.

Regardless of the panel, cookies can be controlled at the browser level (Chrome, Firefox, Safari, Edge). Please remember that disabling necessary cookies may prevent you from logging in to the administration panel and the web application.

15. External tools

On the website, in the panel and in the applications, we use tools of external providers supporting analytics, marketing communication and customer service. A general description is provided below; we publish an up-to-date list with links to the providers' privacy policies in the cookie consent management panel.

- Google Analytics — visit statistics and analysis of behaviour on the website
- LinkedIn Insight Tag — campaign measurement and ad targeting in the LinkedIn ecosystem
- Meta Pixel — measuring campaign effectiveness in the Meta ecosystem (Facebook, Instagram)
- tools for sending newsletters and transactional mailings
- Ticketing Panel (service ticketing system, e.g. Redmine) — technical support
- CRM system — management of Client relationships and sales history
- tools for usability research and A/B testing in the web panel

Analytics and marketing tools are launched only after the relevant consents have been obtained. Tools necessary for the operation of the System (e.g. the Ticketing Panel, CRM) are used on the basis of legitimate interest or in connection with the performance of the agreement.

16. B2B marketing

FleetOnAir is aimed at companies, so marketing communication is conducted in a B2B environment. We send commercial messages to persons who:

- have previously consented to such communications (e.g. subscribed to the newsletter or requested materials)
- provided us with their data in the course of a request for quotation and have not objected to further communication
- have established a business relationship with us under a previous or ongoing agreement

Each marketing message includes a simple way to unsubscribe. Unsubscribing is processed immediately — except for data whose retention is necessary to demonstrate the lawfulness of previous communication.

We use ad personalisation tools on LinkedIn, Meta and Google — solely on the basis of the consents given in the cookie panel. We do not link the activity of website visitors with their accounts on these platforms without a separate legal basis.

17. Changes to the Policy

The content of this Policy may change — in particular in connection with the development of the System, the introduction of new integrations, changes in the law or the use of new external tools. We inform about material changes at least 14 days in advance — by e-mail to Clients and newsletter subscribers and by a notice on the website and in the administration panel.

The current version of the Policy is always available at a permanent address on the fleetonair.com website, and archived versions are made available on request sent to privacy@fleetonair.com.

18. Contact

Please send questions, comments and requests related to the protection of personal data to:

- e-mail: privacy@fleetonair.com
- correspondence address: Core Logic sp. z o.o., ul. Feliksa Radwańskiego 15/1, 30-065 Kraków

We usually respond within a few business days.