


Personal Data Protection Policy

Fleet Catalog +200 products





- Lenovo Thinkpad P16s
- MacBook Air 13" M3
- Persy Booths PersyTWO
- Iphone 15 pro Max

MacBook Air 13" M3
B53L89KH

Alex Moreau arrival date : 24/08/2024

MDM : Device secured 

Device management - MDM

- Firewall 
- Automatic updates 
- Screen lock 
- App deployment 

Fleet SAS – March 2026

Table of Contents

Preamble

Article 1 – Identity of the Data Controller

Article 2 – Data Collected and Purposes

Article 3 – Recipients and Sub-Processors

Article 4 – Retention Periods

Article 5 – Data Security

Article 6 – Data Subject Rights

Article 7 – Post-Mortem Data Rights

Article 8 – Cookies and Similar Technologies

Article 9 – Google Workspace

Article 10 – Data Processing – Data Processing Agreement (DPA)

Article 11 – Data Retention and Deletion Policy

Article 12 – Data Protection Impact Assessment (DPIA)

Article 13 – Contact and Complaints

Article 14 – Policy Updates

Version	Date	Main Changes
1.0	January 2020	Initial version
2.0	January 2023	Sub-processor update, addition of DPA
3.0	March 2026	Full overhaul: HRIS integrations, MSP/Secure, Fleet Copilot, mobile plans, Sirdata cookies, sub-processor update



Preamble

Fleet attaches the greatest importance to the management and protection of personal data. In the course of its activities, Fleet provides IT equipment and managed services to professionals (the “Clients”). Fleet also maintains relationships with a variety of service providers (the “Partners”) with whom Fleet has entered into a partnership agreement.

Accordingly, Fleet collects, via its website <https://fleet.co> (the “Website”) and in the course of performing its services, personal data relating to individuals using the Website features, employees of Clients using IT equipment provided or managed by Fleet, individuals acting on behalf of Clients and individuals acting on behalf of Partners (the “Users”).

This document is intended to inform all Users of how Fleet collects, uses, processes and transmits personal data, in accordance with Regulation (EU) No. 2016/679 of 27 April 2016 on the protection of personal data (“GDPR”) and French Law No. 78-17 of 6 January 1978 relating to data processing, files and freedoms (“Data Protection Act”).

Fleet does not process special categories of data within the meaning of Article 9 GDPR (health data, political opinions, biometric data, etc.) in connection with its Services. Fleet does not target minors and its Services are exclusively intended for professionals. Fleet does not carry out fully automated decisions producing significant legal effects within the meaning of Article 22 GDPR.

Unless otherwise specified herein, terms defined in Fleet’s general terms and conditions of service retain, when used in this document, the meaning given to them by those general terms and conditions.

Article 1 – Identity of the Data Controller

Subject to the provisions of Article 10, the data controller for personal data collected in connection with Fleet Services is:

Fleet SAS

- Registered office: 45 rue de Maubeuge, 75009 Paris, France
- Paris Trade Register: 848 427 449
- VAT number: FR31848427449
- Website: www.fleet.co
- Contact: privacy@fleet.co

Data Protection Representative:

- Internal Data Protection Representative, Personal Data Department



-
- Email: privacy@fleet.co

Article 2 – Data Collected and Purposes

The personal data collected by Fleet includes in particular:

- First names, last names, email addresses and telephone numbers of Fleet's contacts or their agents, representatives, advisors or employees
- Login credentials of users of services offered by Fleet
- Financial data (financial statements, invoicing, etc.)
- Browsing data on the www.fleet.co website and pages published by Fleet

Data is collected in particular on the occasion of:

- Browsing on the www.fleet.co website
- Opening and using a client account on the online platform published by Fleet
- A user's connection to said platform
- Ordering and subscribing to a product or service offer
- Payment for products or services provided by Fleet
- Exchanges of communications with Fleet or via communication tools provided by Fleet

The collection of this data results from the performance of contracts to which Fleet is a party as well as Fleet's legitimate interests. It aims to enable Fleet to provide its services, including the provision of the platform, its improvement and maintenance in a secure environment.

Data collection enables in particular the following operations:

- Access to and use of the platform by the user
- Management and optimisation of the platform
- Ordering and payment of products and services provided by Fleet
- Organisation of payment service usage conditions
- Verification, identification and authentication of data transmitted by a Fleet contact
- Provision of means of communication with Fleet
- Provision of assistance to Fleet's contacts
- Personalisation of services offered to Fleet's contacts
- Fraud prevention and detection
- Management of security incidents
- Management of any disputes with a Fleet contact

Fleet also collects personal data in the course of its commercial activities via:

- Contact forms on the Website www.fleet.co



-
- Lead generation forms on professional social networks
 - Direct commercial interactions (calls, emails, etc.)

Fleet may use these contact details to send targeted commercial communications, in particular via segmentation and scoring tools (HubSpot). These analyses are used to tailor communications to the profiles of prospects.

This method of data collection is based on Fleet's legitimate interests or the consent of Fleet's contact.

Article 3 – Recipients and Sub-Processors

Fleet transfers personal data to third parties only to the extent strictly necessary for the provision of its Services, and only to recipients providing sufficient guarantees under the GDPR.

3.1 Recipients

Personal data may be transferred to the following recipients, acting as independent data controllers:

- The Client's duly authorised employees
- Partners contributing to the implementation of the services provided by Fleet (Assignees, telecoms operators, insurers, advertising retargeting partners, etc.)
- Judicial or administrative authorities in the event of a legal requisition

In the event of a change in Fleet's corporate structure (sale, merger, transfer of business), Fleet will ensure that the receiving entity complies with applicable data protection regulations.

3.2 Sub-Processors

Fleet uses sub-processors for the performance of its Services. When Fleet uses sub-processors, it ensures compliance with applicable standards using one or more of the following mechanisms:

- Standard Contractual Clauses (SCCs) adopted by the European Commission (Decision 2021/914 of 4 June 2021)
- Adequacy decision of the European Commission, in particular the EU-US Data Privacy Framework (DPF), adopted on 10 July 2023
- Binding Corporate Rules (BCRs) for certain global groups, where applicable
- Data Processing Agreement (DPA) covering each sub-processor

The complete and up-to-date list of sub-processors is available on request at privacy@fleet.co. Fleet undertakes to inform Clients of any change of sub-processor having an impact on their data, in accordance with Article 28.2 GDPR.



Article 4 – Retention Periods

Fleet retains personal data for limited periods proportionate to the purposes for which they were collected and to applicable legal obligations.

Data Category	Retention Period	Justification
Cockpit account data (credentials, connection logs)	Contract duration + 12 months	Contract performance / Legitimate interests
Contractual data (Leasing, Leaseback, Upfront)	5 years after contract end	Civil limitation period (Art. 2224 Civil Code)
Invoices and accounting documents	10 years	Legal obligation (Art. L123-22 Commercial Code)
Bank details	13 months after last direct debit	SEPA standards
Delivery data, compliance reports, return slips	5 years after return	Contractual limitation period
Equipment condition reports (repair, damage)	5 years after contract end	Legitimate interests
Employee data (Employee View / HRIS)	Contract duration + 3 months, or deletion on Client request	Contract performance (Fleet as processor)
MSP data (MDM logs, support tickets)	12 rolling months	Legitimate interests (security / service quality)
EDR SentinelOne data (alerts, security events)	12 rolling months	Legitimate interests (system security)
Enrollment data (ABM / Intune)	Service duration + 3 months	Contract performance
Fleet API logs (technical)	1 year	Legitimate interests (security / debugging)



Insurance claim data	5 years after case closure	Civil limitation period
Commercial prospecting data	3 years after last contact	Legitimate interests + CNIL guidelines
Analytics and performance cookies	13 months maximum	Consent / CNIL guidelines
Browsing data (server logs)	1 year	Legitimate interests (security)
Electronic signature data	10 years	Probative value (eIDAS)
Fleet Copilot requests (LLM API)	Not retained after processing	LLM API no-training policy

Upon expiry of these periods, data is deleted or irreversibly anonymised. Certain data may be retained for longer in the event of ongoing legal proceedings or regulatory investigations.

Article 5 – Data Security

Fleet implements appropriate technical and organisational measures to protect personal data against any loss, destruction, alteration, unauthorised access or disclosure, in accordance with Article 32 GDPR.

5.1 Technical Measures

- Encryption of data in transit (TLS 1.2+) and at rest (AES-256)
- Mandatory multi-factor authentication (MFA) for all access to Fleet systems
- Secure cloud architecture on AWS (VPC, network isolation, WAF application firewall)
- Automated encrypted backups with regular restoration tests
- Periodic penetration testing – last test performed by MyCyber in December 2024
- Application monitoring with anonymisation of debugging data (Sentry)

5.2 Organisational Measures

- Role-based access control (RBAC) based on the principle of least privilege
- Mandatory training for all Fleet staff on personal data protection
- Confidentiality clause signed by any employee accessing personal data
- Data Processing Agreement (DPA) covering each sub-processor (Art. 28 GDPR)



- ISO 27001 certification process under way, covering Fleet's information security management
- Fleet selects its sub-processors based on their ability to guarantee processing security through appropriate measures

5.3 Data Breach Procedure

In the event of a personal data breach likely to result in a risk for the rights and freedoms of individuals, Fleet undertakes to:

- Notify the CNIL within 72 hours of discovery (Art. 33 GDPR)
- Notify the affected Client(s) as data controller(s) within 48 hours of breach confirmation, so that they may fulfil their own notification obligations
- Inform the data subjects without undue delay in the event of a high risk (Art. 34 GDPR)
- Document any breach in the internal security incident register

Incident detection is provided by Fleet's monitoring systems and, for Clients of the Secure offering, by the Cyna CERT SOC operating 24/7 surveillance.

Article 6 – Data Subject Rights

In accordance with Articles 15 to 22 GDPR, any individual whose data is processed by Fleet has the following rights.

Right	Description
Right of access (Art. 15)	Obtain confirmation that your data is being processed along with a copy of it and information on the processing conditions.
Right to rectification (Art. 16)	Have inaccurate or incomplete data concerning you corrected.
Right to erasure (Art. 17)	Request deletion of your data when it is no longer necessary or consent is withdrawn, subject to legal retention obligations.
Right to restriction (Art. 18)	Request temporary suspension of processing in the cases provided for by the GDPR.

Right to portability (Art. 20)	Receive your data in a structured, machine-readable format (CSV or JSON), or have it transmitted directly to another data controller. The Fleet Cockpit enables export of fleet data in CSV format.
Right to object (Art. 21)	Object at any time to processing based on Fleet's legitimate interests, in particular for commercial prospecting or marketing segmentation. In the event of objection to segmentation, the User will continue to receive untargeted commercial communications.
Rights relating to automated decisions (Art. 22)	Fleet does not carry out fully automated decisions producing significant legal effects. Segmentation tools (HubSpot, Segment) are used solely to tailor communications.
Right to withdraw consent (Art. 7.3)	Withdraw your consent at any time for processing based on consent, without this affecting the lawfulness of prior processing.

Special case of Client or Partner employees: If you are an employee of a Fleet Client or Partner and wish to exercise your rights regarding data processed by Fleet as a data processor, please contact your employer (the Client or Partner) directly, who is the data controller. Fleet will process any request transmitted by the Client or Partner within thirty (30) days.

How to exercise your rights: By email at privacy@fleet.co or by post to Fleet SAS – Personal Data Department – 45 rue de Maubeuge, 75009 Paris. The request must be accompanied by proof of identity. Fleet undertakes to respond within one (1) month, extendable by two (2) additional months for complex requests, with prior notification.

Article 7 – Post-Mortem Data Rights

In accordance with Article 85 of the French Data Protection Act, every User has the right to define directives regarding the retention, deletion and communication of their personal data after their death.

These directives may be general (covering all processing) or specific (covering only Fleet's specific processing). The User may transmit them to Fleet at privacy@fleet.co or by post to Fleet SAS – Personal Data Department – 45 rue de Maubeuge, 75009 Paris.

In the absence of directives made during the User's lifetime, heirs may contact Fleet to exercise rights of access, rectification and erasure under the conditions provided for by law.

Article 8 – Cookies and Similar Technologies

The website www.fleet.co and the Fleet Cockpit use cookies and similar technologies (scripts, pixels, web beacons, local storage). In accordance with CNIL guidelines, non-essential cookies are only deposited after obtaining your consent.

8.1 Strictly Necessary Cookies

Deposited without prior consent – essential for service operation:

- Session and authentication cookies (maintaining Cockpit login)
- Security cookies (CSRF protection, fraud prevention)
- Interface preference cookies (language, display settings)

8.2 Analytics and Performance Cookies

Deposited only after consent – maximum duration of 13 months:

- Google Analytics 4: website audience measurement, pages visited, traffic source
- Sentry: event collection, measurement, analysis

8.3 Functional and Advertising Cookies

Deposited only after consent:

- HubSpot: tracking of contact forms and marketing campaigns
- Advertising pixels (LinkedIn Insight Tag, Google Ads, etc.)
- Conversion tracking and advertising retargeting

8.4 Advertising Retargeting

Fleet may use retargeting services to identify internet users who have visited the Website and send them personalised communications on other platforms. This processing takes place only with your prior consent. You may object at any time via the cookie manager or at privacy@fleet.co.

8.5 Social Networks

Fleet may use social networks to offer targeted advertising and generate leads via native forms (LinkedIn Lead Gen Forms). Fleet invites all Users to consult the data protection policies of the relevant platforms.

8.6 Consent Management

On your first visit to the website, a consent banner is displayed via Sirdata (www.sirdata.com), a solution certified as compliant with CNIL guidelines. You may modify your preferences at any time:

- By clicking on the “Manage my cookies” link at the bottom of each page of the website
- Via your browser settings (Safari, Chrome, Firefox, Opera)
- Via your mobile device settings (iOS, Android)

In accordance with CNIL recommendations, your consent to non-essential cookies is renewed every 13 months. No non-essential cookie is deposited before this period has expired without obtaining new consent.

Article 9 – Google Workspace

Fleet uses Google Workspace in the course of its internal operations. Fleet undertakes to comply with the limited use restrictions imposed by Google and confirms that:

- Data processed via Google Workspace is used solely to provide and improve Fleet’s services
- Fleet does not sell user data to third parties
- Fleet does not use such data for advertising purposes
- Fleet does not use such data to train artificial intelligence or machine learning models

Article 10 – Data Processing – Data Processing Agreement (DPA)

Where Fleet processes personal data on behalf of a Client – in particular in connection with MSP services, ABM/Intune enrollment, Employee View management or HRIS synchronisation – or a Partner, Fleet acts as a data processor within the meaning of Article 28 GDPR.

It is the responsibility of the Data Controller to provide Fleet with:



-
- Its instructions regarding processing carried out by Fleet
 - The categories of data processed and the data subjects concerned
 - Fleet's obligations in terms of security, confidentiality and data breach notification
 - Assistance to the data controller in connection with the exercise of data subjects' rights
 - The conditions for deletion or return of data upon completion of the service
 - General authorisation for Fleet to use its sub-processors (Art. 28.2 GDPR). Fleet will inform the data controller of any addition or replacement of a sub-processor, enabling it to exercise its right to object

A template Data Processing Agreement (DPA) prepared by Fleet is available on request at privacy@fleet.co.

Article 11 – Data Retention and Deletion Policy

11.1 Data Life Cycle

- Active data: retained in active database for the duration of the ongoing service
- Archived data: transferred to restricted-access secure storage with access logging, to meet legal retention obligations
- End-of-life data: deleted or irreversibly anonymised at the end of the applicable retention period

11.2 Deletion on Request

Following a deletion request from a data subject, Client or Partner (under the DPA), Fleet proceeds to delete or anonymise the data within thirty (30) days, subject to legal retention obligations. Fleet ensures that its sub-processors carry out the same deletions, in accordance with the DPAs concluded.

Article 12 – Data Protection Impact Assessment (DPIA)

Fleet conducts Data Protection Impact Assessments (DPIAs) for processing operations likely to present a high risk to the rights and freedoms of data subjects, in accordance with Article 35 GDPR.

Processing operations subject to a DPIA include in particular:



-
- MSP services with extended device monitoring (Secure offering – SentinelOne EDR / Cyna CERT SOC)
 - Large-scale processing of data relating to Equipment fleet management
 - HRIS synchronisation involving data of numerous Client employees
 - Any new processing involving systematic monitoring or sensitive data

DPIAs are reviewed regularly and are available on request at privacy@fleet.co.

Article 13 – Contact and Complaints

13.1 Contacting Fleet

Fleet SAS – Data Protection Representative

Internal Data Protection Representative, Personal Data Department

By email: privacy@fleet.co

By post: Fleet SAS – Personal Data Department – 45 rue de Maubeuge, 75009 Paris

13.2 Contacting the Supervisory Authority

If Fleet's response is unsatisfactory or no response is received within the time limit, you have the right to lodge a complaint with the competent supervisory authority:

Commission Nationale de l'Informatique et des Libertés (CNIL) – French Data Protection Authority

- Address: 3 place de Fontenoy – TSA 80715 – 75334 Paris Cedex 07
- Telephone: +33 1 53 73 22 22
- Website: www.cnil.fr

13.3 Cross-Border Complaints

For Clients established in other EU Member States, the CNIL is Fleet's lead supervisory authority. You may also contact the data protection authority in your country of residence.

Article 14 – Policy Updates

Fleet reserves the right to modify this Personal Data Protection Policy at any time, in particular in the event of changes to processing carried out or sub-processors used, new legal or regulatory obligations, or the launch of new Fleet services or features.



In the event of a material change, Fleet will notify Clients via Cockpit notification or by email within a reasonable period before the new provisions come into force.

The current version of this Policy is permanently accessible at: www.fleet.co/privacy-gdpr
Changes to this Policy apply only from their effective date and are not retroactive. This Policy is consistent with Fleet's General Terms and Conditions (GTC), available at www.fleet.co/cgv. In the event of conflict, the GTC prevail for contractual aspects and this Policy prevails for personal data protection aspects.

Fleet Personal Data Protection Policy – Version 3.0 – March 2026

Fleet SAS • 45 rue de Maubeuge, 75009 Paris • privacy@fleet.co