Group Privacy Policy

Revision	Author	Job Title	Last Update	Due Date
01	Julien Grange	Group CEO	30/06/2026	31/12/2026

AIM & SCOPE

This Privacy Policy clearly and concisely explains how PURFLUX GROUP collects, uses, and protects personal data in the course of its professional activities.

Our company, committed to developing innovative mobility solutions at international level, works with key players in the automotive sector. In this context, we process only a limited amount of personal data, mainly related to the management of our employees, service providers, and internal tools required for our industrial, logistics, and security activities.

Our company is a global player in mobility technologies operating in the fields of logistics and industrial management. It processes only a limited volume of personal data, mainly relating to its employees, service providers, and internal users of its tools (HR, IT, site access, security).

In accordance with Regulation (EU) 2016/679, known as the GDPR, and the principles of the CNIL, we undertake to collect only the information strictly necessary for the performance of employment contracts, compliance with our legal obligations, and the secure operation of our sites and systems.

This policy aims to provide full transparency on:

- the types of data collected,
- the purposes of processing,
- the recipients of the data,
- the retention periods,
- the rights of the data subjects,
- and how to contact our GDPR representative / DPO.

Our objective is to ensure responsible, proportionate, and secure use of personal data within the company.

KEY PRINCIPLES

1. Type of Personal Data Collected

As part of our industrial, logistics, and mobility activities, we collect only the personal data strictly necessary for the operation of the company and for the management of our employees, service providers, and internal users of our tools and infrastructure.

The categories of data that may be collected are as follows:

Identification data (e.g., name, identity card and passport numbers, nationality, place and date of birth, photograph).

Contact data (e.g., address, telephone number, postal or email address).

Personal life data (e.g., family situation, number of children).

Professional life data (e.g., level of education, job, employer name).

Administrative and contractual data (e.g., information related to the employment contract, HR management data such as attendance and leave, information required for payroll processing).

IT and access data (e.g., professional identifiers and IT accounts, SAP access, technical connection logs such as VPN and MFA logs, entry/exit badge data, information relating to the use of company IT equipment).

Security and safety data (e.g., recordings from video surveillance on certain sites, used only for the protection of people and property).

2. Data Not Collected

The company never collects sensitive data such as:

- Political or trade-union opinions
- Biometric data[1]
- Genetic data
- Sexual orientation
- Religious or philosophical information

Unless required by law, for example for medical obligations managed by an authorized body.

This section provides fictitious content representing process requirements, operational expectations, or compliance guidelines. The information presented here is purely indicative and does not reflect the actual rules of the organization. Teams must ensure that procedures remain consistent with internal standards, applicable regulatory obligations, and documented operational controls.

Additional fictitious information is added to simulate realistic content, enabling the development of templates, flowcharts, or governance documents without using real

[1] The Group prioritizes non-biometric means of identification. Where the use of biometric data is authorized by local regulations, it is implemented in compliance with applicable legal requirements.

operational data. This section provides fictitious content representing process requirements, operational expectations, or compliance guidelines.

3. Legal Basis

This data is necessary:

- For the performance of the employment contract or professional assignments,
- For compliance with legal and regulatory obligations,
- Or for the pursuit of the company's legitimate interests (security, site access, incident prevention).

This corresponds to the legal basis provided for in Article 6(b) of the GDPR (performance of a contract) and to HR and security obligations.

4. Purpose of Data Collection and Processing

The site and the company collect your data for the following purposes:

- To ensure administrative management of personnel (e.g., contracts, payroll, absences, mandatory declarations)
- To manage access to premises, IT tools, and infrastructure (badges, IT accounts, SAP, industrial terminals)
- To ensure the security of people, property, and systems (logging, video surveillance, incident detection, site access)
- To manage internal requests (IT support, HR services, security)
- To ensure compliance with the legal, social, tax, and regulatory obligations applicable to the company
- To enable the operational functioning of industrial sites, logistics warehouses, and transport activities

Therefore, all information we collect is used exclusively to:

- Ensure the proper functioning of industrial and logistics activities
- Guarantee the security of employees, equipment, and infrastructure
- Manage your HR file and employment relationship
- Contact you in connection with your professional assignments
- Respond to legal obligations and any requests from competent authorities

No data is used for marketing, advertising, or commercial purposes, as the company does not carry out activities aimed at private individuals.

5. Data Retention Period

PURFLUX GROUP retains personal data only for the period necessary to achieve the purposes for which it is collected, and in accordance with applicable legal or regulatory obligations.

Retention periods vary depending on the nature of the data processed:

- Administrative and contractual personnel data: retained for the duration of the employment relationship, then archived according to applicable legal deadlines (e.g., social, tax, and accounting obligations). The detailed retention periods applicable to these documents are specified in the internal document "Retention Period for Social Documents - February 2026".
- Data related to the management of access to sites and IT tools (badges, IT accounts, connection logs): retained for limited periods necessary for security and system operation (generally from a few weeks to 12 months depending on security requirements).
- Video surveillance recordings: retained for a maximum period defined by local regulations, generally short, unless required in connection with a security incident.
- Data related to suppliers, service providers, and partners: retained for the time necessary for contractual follow-up and administrative obligations.

Retention periods are communicated to the data subjects when data is collected and are strictly observed to ensure responsible and proportionate data management.

6. Record of Processing Activities

PURFLUX GROUP, as data controller, maintains an up-to-date record listing all personal data processing activities carried out as part of its industrial, logistics, and administrative activities.

This record identifies, for each processing activity, its purpose, the categories of data concerned, the recipients, the retention periods, and the associated security measures.

The company undertakes to make this record available to the competent supervisory authority upon request, in order to verify the compliance of processing activities with the regulations in force on personal data protection.

7. User Rights

In accordance with the General Data Protection Regulation (GDPR), any person whose personal data is processed by PURFLUX GROUP has the following rights:

- Right of access: to obtain confirmation that personal data is being processed and to receive a copy of it.
- Right to rectification: to have any inaccurate or incomplete data concerning you corrected.
- Right to erasure: to request the deletion of certain personal data in the cases provided for by law.
- Right to restriction of processing: to request the temporary suspension of the processing of your data where permitted by law (e.g., dispute, verification).
- Right to object: to object to the processing of your data on legitimate grounds.
- Right to withdraw consent: where processing is based on your consent, it may be withdrawn at any time, without retroactive effect.
- Right to data portability: to obtain the data you have provided in a structured, machine-readable format, where applicable.
- Post-mortem right: to define instructions regarding the fate of your data after your death (retention, deletion, communication).

8. How to Exercise Your Rights

You may exercise all of these rights, subject to proof of your identity, by contacting:

GDPR / DPO email address:
dpo@purfluxgroup.com

Postal address:
PURFLUX GROUP
Data Protection Department
Immeuble Renaissance
1 avenue Claude Monet
78280 Guyancourt - France

The company will respond to any request within the timeframes provided for by the regulations.

In accordance with applicable regulations, you have the right to lodge a complaint with the competent supervisory authority.

9. Security and Confidentiality

PURFLUX GROUP implements appropriate technical and organizational measures to protect personal data against loss, alteration, unauthorized access, or disclosure. These measures cover both industrial environments and the information systems used in our logistics and operational activities.

Data is protected using security mechanisms such as:

- Strict access controls based on business needs and the principle of least privilege;
- Secure user authentication, including multifactor authentication where necessary;
- Access logging and monitoring, with logs protected against any unauthorized modification;
- Securing the networks and servers hosting the data;
- Regular system updates and security patches;
- Secure backups and periodic restoration checks;
- Encryption of communications and sensitive data where necessary;

Access to personal data is limited to duly authorized employees and service providers within the scope of their assignments (HR, IT, security, maintenance).

These persons are required to respect the confidentiality of the information and to use it only for strictly professional purposes.

Where external service providers are used, PURFLUX GROUP contractually imposes GDPR-compliant security safeguards and ensures that the measures necessary to protect the data are applied.

10. Data Recipients

As part of its industrial, logistics, and administrative activities, PURFLUX GROUP may be required to disclose certain personal data to internal or external recipients who are strictly authorized and only where necessary for the performance of assignments or compliance with legal obligations.

The main categories of recipients are as follows:

- Authorized internal departments: Human Resources, IT departments, site security, operational managers, within the limits of their duties.
- Technical and IT service providers acting on behalf of the company: hosting, maintenance, cybersecurity tools, cloud services, business application providers (e.g., SAP, M365).
- Logistics and industrial service providers involved in transport, shipping, or internal flow management operations, where this involves limited access to professional data.
- Social security bodies and administrations: social protection organizations, tax administrations, or legally authorized authorities (e.g., judicial or regulatory requests).
- Contractual partners where strictly necessary for the management of a contract, assignment, or legal obligation.

The company neither sells nor markets any personal data.

Any transfer of data to a third party is carried out within a secure framework and in accordance with the GDPR. External service providers acting on behalf of the company are subject to strict contractual confidentiality and security obligations.

Outside these cases, personal data is never disclosed unless required by law or requested by a competent authority.

11. Cross-Border Transfers

If certain personal data has to be transferred to Group entities located outside the European Union, PURFLUX GROUP ensures that such transfers are strictly necessary for internal operations and are carried out in accordance with applicable

regulations. The appropriate safeguards provided for by the GDPR will be implemented before any actual transfer.

Guyancourt, 30th June, 2026

Julien GRANGE

CEO PURFLUX GROUP