MEOGROUP

PERSONAL DATA PROTECTION POLICY

INFORMATION SYSTEMS & TECHNOLOGIES DEPARTMENT
03/04/2025

CONTENTS

VERSION MANAGEMENT

VERSION	AUTHOR	ROLE	DATE
1.0	Anaïs LANGEVIN *Corporate Chief Information Officer* *Corporate Data Protection Officer*	Editor	03/04/2025
	Frédéric DUPONT *EIPM Marketing and Communications Officer* *Data Protection Officer EIPM*	Proofreader	14/04/2025
	Alice GASNIER *Corporate Chief Compliance Officer*	Proofreader	22/04/2025
	Lisa PUDDU *Quality engineer*	Proofreader	22/04/2025
	Bilal AIT-GACEM *Corporate IT & Security Project Leader*	Proofreader	11/04/2025
	Célia YVAIN *Corporate Chief HR Officer*	Proofreader	14/04/2025

GLOSSARY

- **Control authority:**
  National body responsible for ensuring that personal data protection regulations are applied.

- **Legal basis:**
  Legal justification for processing personal data in compliance with local regulations.

- **Personal data (PD):**
  Any information relating to an identified or identifiable natural person (e.g. surname, first name, e-mail address, telephone number, IP address).

- **Sensitive personal data (SPD):**
  A special category of personal data including, for example, information relating to health, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, or biometric and genetic data.

- **European Economic Area (EEA):**
  Area comprising the Member States of the European Union plus Iceland, Liechtenstein and Norway.

- **Person concerned:**
  Individual whose personal data is collected and processed.

- **Data controller (RT):**
  Entity (natural or legal person) that determines the purposes and means of processing personal data.

- **Subcontractor (ST):**
  Entity that processes personal data on behalf of and on the instructions of a data controller.

- **Processing of personal data:**
  Any operation carried out on personal data, whether automated or not.

- **Personal data breach:**
  Violation of data security leading to its destruction, loss, alteration, unauthorised disclosure or unauthorised access.

INTRODUCTION

Founded in 2005 by Richard Caron, MEOGROUP is a business performance consulting group operating in France and internationally. With more than 850 employees, the group generates sales of over €100 million.

MEOGROUP consists of 10 firms specialising in consulting and services, interim management and recruitment, as well as a training institute. Our areas of expertise include Purchasing & Supply Chain, Finance & Management Control, and Project Management & Transformation (Industrial, IT, Architecture & Design).

MEOGROUP consultants support companies in all sectors, from major accounts to start-ups, in their transformation and performance improvement projects.

COMMITMENT TO THE PROTECTION OF PERSONAL DATA

MEOGROUP attaches the utmost importance to the security and confidentiality of the personal data it collects and processes.

In compliance with legal requirements, the Group implements strict measures to guarantee the protection of this information and to ensure that it is processed in a way that respects the rights of individuals.

MEOGROUP undertakes to collect only the data that is necessary, to store it securely and to process it transparently and responsibly. The trust of its customers, partners and employees is essential, and the group deploys all necessary means to protect their data against any misuse, unauthorised access, alteration or unauthorised disclosure.

PURPOSE OF THIS DOCUMENT

The main objective of this Personal Data Protection Policy (PDPP) is to ensure the security, confidentiality and compliance of personal data collected, processed and stored by the Group.

This policy aims to respect the rights of individuals by ensuring transparent and responsible management of their personal information. It complies with legal requirements and implements rigorous security measures to protect data against unauthorised access, alteration or loss.

By introducing secure practices and raising awareness among all stakeholders, MEOGROUP is committed to protecting the privacy of individuals while minimising the legal and operational risks for the company.

REVISION OF THIS DOCUMENT

This document is periodically reviewed to ensure that it complies with current legal, regulatory and organisational requirements. This review is carried out at least once every three years or following any significant change that may have an impact on the management of personal data.

Any updates are carried out under the supervision of the Corporate Data Protection Officer (DPO) in consultation with the stakeholders concerned. Any changes made are communicated to the people concerned.

SCOPE OF APPLICATION

PEOPLE CONCERNED

Unless otherwise stated, this policy applies to all MEOGROUP contacts.

BRANDS CONCERNED

Unless otherwise stated, this policy applies to all the brands that make up MEOGROUP:

- Adven,
- Axel,
- Cadele,
- Cost House,
- Cristal Decisions,
- EIPM,
- Luca,
- Masai,
- Meotec,
- SolvHA,
- Sowing,
- Valoptia.

COUNTRIES CONCERNED

Unless otherwise stated, this policy applies to all countries in which MEOGROUP operates:

- Belgium,
- Brazil,
- Canada,
- Spain,
- France,
- Italy,
- Luxembourg,
- Morocco,
- Switzerland.

LEGISLATIVE CONTEXT

Regarding the protection of personal data, MEOGROUP complies with the legal and regulatory requirements in force, particularly those set out in the General Data Protection Regulation (GDPR) and other applicable national and international legislation.

- **Belgium:**
  - General Data Protection Regulation (GDPR),
  - Law on the protection of personal data which complements and transposes the RGPD in Belgium and is regulated by the Commission for the Protection of Privacy (Data Protection Authority, DPA).

- **Canada:**
  - The federal Personal Information Protection and Electronic Documents Act (PIPEDA), which governs the collection, use and disclosure of personal information in the private sector,
  - Act respecting the protection of personal information in the private sector (Bill 25).

- **Spain**:
  - General Data Protection Regulation (GDPR),
  - Organic Law 3/2018 on the Protection of Personal Data and the Guarantee of Digital Rights, which complements the RGPD, considering national specificities and digital rights. It is overseen by the Spanish Data Protection Agency (AEPD).

- **France:**
  - General Data Protection Regulation (GDPR),
  - Loi Informatique et Libertés, which supplements the RGPD and sets out specific aspects of data protection. It is supervised by the Commission Nationale de l'Informatique et des Libertés (CNIL).

- **Italy:**
  - General Data Protection Regulation (GDPR),
  - Privacy Code, which is governed by the Privacy Code (Legislative Decree no. 196/2003), updated to comply with the RGPD. It is regulated by the Guarantor for the Protection of Personal Data.

- **Luxembourg:**
  - General Data Protection Regulation (GDPR),

- Law of 1 August 2018 on the protection of personal data, which complements the RGPD by clarifying certain aspects specific to Luxembourg and is overseen by the National Commission for Data Protection (CNPD).

> **Morocco:**

- Law 09-08 on the protection of individuals about the processing of personal data, which governs the processing of personal data. It is overseen by the National Commission for the Supervision of Personal Data Protection (CNDP).

> **Switzerland:**

- Federal Data Protection Act (DPA),
- Data Protection Regulation (DPR), which accompanies the DPA and sets out the procedures for implementing data protection rules.

ORGANISATION FOR THE PROTECTION OF PERSONAL DATA

Organising the protection of personal data involves defining the teams responsible for security, responsibilities and governance.

THE DATA PROTECTION OFFICER (DPO)

The DPO defines and steers MEOGROUP's personal data protection policy.

It is required to:

- Ensure compliance with applicable regulations,
- Supervising documentation
- Ensuring people's rights are respected,
- Arbitrating risks with management
- Advise project teams and support the implementation of recommendations,
- Participating in audits, notifying the competent authorities of breaches, cooperating with the supervisory authorities,
- Raising employee awareness.

THE CORPORATE CHIEF INFORMATION OFFICER (CIO)

The IT Department defines the Group's IT strategy and guarantees data security, availability and integrity.

It is required to:

- Managing IT projects,
- Managing the risks associated with information systems,
- Deploy measures to protect personal data (encryption, traceability, back-ups, etc.).
- Managing security incidents involving personal data, by providing an appropriate and documented technical response,
- Integrate data protection requirements into all IS projects.

THE CORPORATE CHIEF HUMAN OFFICER (CHO)

The HR Department defines HR policies in line with Group strategy.

It is required to:

- Ensuring that the processing of data relating to employees, applicants and collaborators complies with the obligations in force.
- Participating in impact analyses and implementing appropriate confidentiality measures,
- Work with the DPO and the IT Department to secure HR projects (recruitment, payroll, training, etc.).

THE CORPORATE CHIEF COMPLIANCE OFFICER (CCO)

The DC coordinates MEOGROUP's overall regulatory and ethical compliance system.

It is required to:

- Drawing up internal policies,
- Organising controls and audits,
- Oversee training in relation to legal obligations (anti-corruption, personal data, ethics, etc.).

THE INFORMATION SECURITY MANAGER (ISSM)

The CISO oversees the security of MEOGROUP's information system.

It is required to:

- Defining safety rules,
- Raising employee awareness,
- Supervising disaster recovery plans,
- Monitoring security incidents.

OUR CROSS-GOVERNANCE

Process / Activity	DPO	CIO	CHO	CCO	ISSM
Definition of the policy	P	C	C	PC	C
Compliance / audits	P	C	C	PC	C
Privacy by Design / Privacy by Default	P	PC	C	C	PC
Impact analysis	P	C	C	C	C
Security incident management	C	PC	C	C	P
Notification to supervisory authorities / information to data subjects	P	C	S	C	S
Processing people's rights	P	S	PC	C	S
Managing the data processing register	P	F	F	S	F
Raising employee awareness	P	S	PC	PC	PC
Regulatory intelligence and international compliance	P	S	S	CP	S

P = pilot; C = contributor; S = support; CP = co-pilot; F = information provider

PERSONAL DATA MANAGEMENT

COMPLIANCE MONITORING TOOL

MEOGROUP uses the Data Legal Drive solution from EQS Group to manage compliance on a day-to-day basis, by keeping a register of processing operations and managing requests from data subjects.

PROCESSING OF PERSONAL DATA

MEOGROUP processes personal data as part of its consultancy activities, in compliance with the applicable regulations. This processing mainly concerns employee management, relations with candidates, customers and partners, and improving the services offered.

The data collected is processed in a lawful, fair and transparent manner, and is limited to specific and legitimate purposes. It is kept for a period strictly necessary to achieve these purposes, in accordance with legal obligations and the recommendations of data protection authorities. At the end of this period, it is deleted, anonymised or archived in a secure manner. It is subject to appropriate security measures to guarantee its confidentiality, integrity and availability

A detailed description of the processing carried out, including the legal basis, the categories of data and the retention periods, is recorded in the register of processing operations, which is kept up to date under the supervision of the DPO.

APPLICATION OF PRIVACY BY DESIGN AND PRIVACY BY DEFAULT

MEOGROUP applies the principles of Privacy by Design and Privacy by Default to every project involving personal data. This means that:

- Anticipating risks at the design stage,
- Only collect data that is strictly necessary,
- Set high privacy settings by default,
- Restrict access to authorised persons only,
- Raising awareness of these requirements among project and business teams.

These principles are incorporated into tools, processes and employee training.

IMPACT ANALYSIS (AIPD / DPIA)

A Data Protection Impact Assessment is carried out when a MEOGROUP processing operation presents a high risk to the rights and freedoms of individuals. It identifies the risks and proposes appropriate corrective measures.
Where necessary, MEOGROUP shall consult the competent supervisory authority before implementing the processing concerned.

Employees involved in setting up new processing operations are encouraged to anticipate the risks and to contact the DPO as soon as the project is being considered.

DATA SHARING

> Sharing personal data

MEOGROUP may share certain personal data with third parties during its activities, but only to the extent necessary to achieve the defined purposes and in compliance with the regulations in force:

- One or more MEOGROUP subsidiaries for operational, administrative or commercial reasons,
- Service providers and subcontractors working on behalf of MEOGROUP,
- Partners and customers, where this is necessary for the performance of the tasks entrusted to us or for the management of contractual relations,
- Administrative and judicial authorities, when required by law or as part of legal proceedings.

All data sharing is subject to a strict contractual framework to ensure its protection, through the inclusion of confidentiality clauses and, where applicable, the implementation of specific agreements.

> Data transfers outside Europe

As part of its activities, MEOGROUP may transfer personal data outside the European Economic Area (EEA). These transfers only take place when this is necessary for the purposes defined and in compliance with the regulations in force.

When data is transferred outside the EEA, to group subsidiaries, MEOGROUP implements appropriate safeguards to ensure its protection.

Where data recipients are in a country that does not benefit from an adequacy decision from the European Commission, appropriate safeguards are put in place, such as the European Commission's standard contractual clauses or other recognised mechanisms for ensuring an adequate level of protection.

RIGHTS OF THE PERSONS CONCERNED

In accordance with the applicable laws, everyone has several rights (see non-exhaustive list below) relating to his or her data. These rights aim to guarantee transparency, security and control over the use of their personal information.

1. **Right of access:**
   An individual has the right to know whether his or her personal data is processed by MEOGROUP and, if so, to obtain detailed information on the purposes of the processing, the categories of data collected, the recipients of the data, as well as the storage period.

2. **Right of rectification:**
   An individual may request the correction of any personal data held about him or her by MEOGROUP if he or she believes it to be inaccurate or incomplete.

3. **Right to erasure (or right to be forgotten):**
   An individual may request the deletion of their personal data held by MEOGROUP if it is no longer necessary for the purposes for which it was collected, or if they withdraw their consent where consent is the legal basis for the processing.

4. **Right to object:**
   An individual may object, without justification, to the processing - carried out by MEOGROUP - of his/her data based on legitimate interest. In certain cases, they may also object to their data being processed for commercial prospecting purposes.

5. **Right to withdraw consent:**
   A person may withdraw his or her consent from MEOGROUP at any time, without this affecting the lawfulness of the processing carried out prior to the withdrawal.

PROCEDURE FOR EXERCISING THE RIGHTS OF DATA SUBJECTS

To exercise their rights relating to the protection of personal data, data subjects must submit a written request, specifying the right they wish to exercise:

- Or by e-mail: dpo@meogroup-consulting.com,
- Or by using the form on the platform on which the data is collected,
- Or by post:
  MEOGROUP - For the attention of the DPO
  27/33 Quai Alphonse LE GALLO
  92100 Boulogne-Billancourt
  France.

The request must include the information necessary to clearly identify the data subject, such as contact details and, if necessary, a copy of an identity document.

The DPO has one month from receipt of the request to respond. Depending on the complexity and number of requests, this period may be extended by a further two months.

If the request is deemed unfounded or excessive, a fee may be charged, or the request may be rejected.

If the data subject considers that his or her rights are not being respected, he or she may refer the matter to the competent data protection authority.

DATA SECURITY

LIST OF TECHNICAL AND ORGANISATIONAL MEASURES

Technical and organisational measures are described by country and in separate documents.

The following documents are also available:

- Security Policy of our Information System (ISSP),
- User Charter of our Information System,
- Data backup and restoration policy,
- Password definition and management policy,
- Policy on the loan of computer and telephone resources,
- Procedure for managing incidents involving personal data,
- Mapping of solutions, flows and infrastructure,
- Administration charter,
- Solution access logging policy,
- Internal and external audits planning.

DATA BREACH MANAGEMENT

In the event of a personal data breach, a specific procedure is implemented to limit the impact and ensure compliance with legal obligations.

Any suspicion or identification of a violation must be reported immediately to the DPO.
An analysis is carried out to assess the nature, extent and potential consequences of the incident.

If the breach presents a risk to the rights and freedoms of the data subjects, the competent supervisory authority will be notified within a maximum of 72 hours of its discovery, in accordance with the regulations in force. Where the risk is high, the persons concerned will also be informed as soon as possible.

Corrective and preventive measures are put in place to remedy the situation and avoid any recurrence.

An incident log is kept ensuring that the data protection system is monitored and continuously improved.

AWARENESS AND TRAINING

MEOGROUP attaches particular importance to raising awareness and training its employees in the protection of personal data and cyber security.

To reinforce the culture of data protection within the company, we have set up a cyber awareness programme, enabling every employee to better understand the risks and adopt good practice.

This programme, detailed in a separate document, includes:

- Regular training,
- Awareness-raising workshops for new arrivals,
- Videos to explain key concepts in simple terms,
- Webinars to explore the main topics in greater depth, explain the impact and assess understanding,
- Case studies to raise employees' awareness of the issues,
- Tests, exercises and simulations to test your reflexes,
- In-house resources and guides on best practice in data confidentiality and security.

MAIN CONTACTS

- If you have any queries about the protection of personal data, please contact our dedicated team at **dpo@meogroup-consulting.com**.
- If you have any questions or concerns about cyber security, please contact our dedicated team at **cybersecurity@meogroup-consulting.com**.
- If you have a complaint, please contact our dedicated team at **reclamation@meogroup-consulting.com.**
- For any IT support or queries, please contact our dedicated team at **si@meogroup-consulting.com**.