6 Monks (6M)
Société à responsabilité limitée
1A Heienhaff, L-1736 Senningerberg, Grand Duchy of Luxembourg
R.C.S. Luxembourg: B 259714

DATA PROTECTION POLICY

CONTENTS

Classification	Confidential
Audience	All employees and Management
Ownership	Head of Legal and Compliance

Version	Date	Name	Description
0.01	September 2023	Julie Bourgeois	Initial Document
0.02	December 2024	Julie Bourgeois	Adhoc review
0.03	December 2025	Julie Bourgeois	Adhoc review

Document Circulation

This document will be made available on the Company's One Drive for the defined audience as soon as the document will be approved and finalized. Copies are not controlled.

Review Cycle

This document shall be reviewed on a yearly basis at least or when required by major changes in the organization (internal governance framework) and operational processes of the Company.

Version	Approval Date by Executive Committee	Approval Date by Board of Managers
0.01	None.	December 2023
0.02	November 27, 2024	December 16, 2024
0.03	November 27, 2025	December 15, 2025

Table of Contents

1. BACKGROUND

6 Monks (6M) (the "**Company**", "**6M**" or "**we**") is a Luxembourg private limited liability company (*société à responsabilité limitée*), having its registered seat at 1A, Heienhaff, L-1736 Senningerberg, Grand Duchy of Luxembourg, and registered with the Luxembourg Trade and Companies Register under number B 259714.

6M is an authorized alternative investment fund manager ("**AIFM**") by the Luxembourg *Commission de Surveillance du Secteur Financier* under number A00003285 offering fund management services for alternative investment funds ("**AIF**").

In order to conduct its business purposes, 6M must gather and use information, such as information considered as personal data about individuals. These individuals, also known as Data Subjects, may include investors, Customers, employees or any person the organization may have a relationship with.

The guidelines contained in this document are aligned and based on the Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of Personal Data and on the free movement of such data, and repealing Directive 95/46/EC ("**General Data Protection Regulation**" or "**GDPR**") completed by the Luxembourg law of 1 August 2018 on the organisation of the National Commission for Data Protection (the "**Luxembourg Personal Data Protection Law**" and together with GDPR and any regulations and or CSSF circulars, the "**Data Protection Legal Framework**").

The Company has set up this Data Protection Policy (the "**Policy**") with the aim to set out in a written document the process related to personal data protection as well as to make sure personal data protection are treated in accordance with GDPR and notably its Article 5.

The Policy must be approved by the executive committee (the "**Executive Committee**") and the board of managers (the "**Board of Managers**"), be available to the Company's employees and published on the Company's website.

2. SCOPE OF THE POLICY

In relation to the Policy in the event of a valid request by a competent authority, all requested data, information or documents shall be provided. In case of doubts the Legal and Compliance function must be consulted.

The Company has a high degree of vigilance to the protection of privacy and personal data. In its quality of AIFM, the Company applies professional secrecy as defined in Article 41 of Luxembourg law of 5 April 1993 on the financial sector as amended and pays special attention to all the business processes where Personal Data may be collected and processed.

The Company implements all technical and organizational measures in order to ensure Personal Data protection and security for all its employees and Customers, delegates, intermediaries and providers.

The Policy addresses the processing of Personal Data by 6M, as a data Controller and/ data Processor, of all Data Subjects (including customers, suppliers, and business partners). It further addresses how Personal Data must be processed by a third party, such as a service provider, on behalf of 6M. This Policy is binding on 6M and its employees, including the Board of Managers. It specifically applies to all Personal Data whether collected by electronic or paper base means.

Through the Policy, 6M ensures:

- Compliance with Data Protection Legal Framework;
- Protection from the risk of a Data Breach such as wrongful loss, alteration, disclosure or access;
- Transparency in the manner it deals with information;
- Protection of the rights of Data Subjects;
- Personal Data are updated, complete and accurate;
- Disclosure of Personal Data to third parties in accordance with this Policy.

Personal Data include all information provided or collected which concern any personal aspect of 6M's employees and/or Board members and/or shareholders and/or personal information around the entities managed by 6M (related members of the board of directors, investors, etc.).

This Policy is made available to all employees. It applies to Company employees, members of the Board of Managers, delegated third parties and limited partners of AIFs managed by the Company.

This Policy must be read in conjunction with the IT Policy.

3. DEFINITIONS

ALFI	Association of the Luxembourg Fund Industry.
Customers	Means any AIF managed by 6M or any investor of any AIF managed by 6M.
CNPD	Means the Luxembourg *Commission Nationale de Protection des Données*.
Consent (of the data subject)	Means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.
Controller	Means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.
CSSF	The Luxembourg *Commission de Surveillance du Secteur Financier*.
Data subject	Means an identified or identifiable natural person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
DPO	Means Data Protection Officer as required by Article 37 of the GDPR.
Identified or identifiable natural person	Means one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Personal Data	Means any information relating to a Data Subject.
Personal Data Breach	Means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.
Personal Data Processing	Means, in accordance with Article 1 of GDPR, any operation or set of operations which is performed on Personal Data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
Processor	Means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the Controller.
Pseudonymization	Means replacing any information which could be used to identify an individual with a pseudonym, or, in other words, a value which does not allow the individual to be directly identified.
Senior Management	Means the persons who effectively conduct the business of the Company as AIFM within the meaning of Article 102(1)(c) of the 2010 Law and Article 7(1)(c) of the 2013 Law.

4. PROCESSING OF PERSONAL DATA

4.1. Principles of processing personal data

To the extent that it processes Personal Data, 6M, as Data Controller, must be able to demonstrate that it complies with the Data Protection Legal Framework, taking into account the nature, scope, context and purposes of Personal Data Processing as well as the risks of varying likelihood and severity in accordance with the proportionality principle.

In accordance with GDPR, 6M shall ensure that all Personal Data are:

- processed lawfully, fairly and in a transparent manner in relation to the Data Subject ("lawfulness, fairness and transparency");
- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes ("purpose limitation");
- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ("data minimization");
- accurate and where necessary, kept up to date ("accuracy");
- kept in a form which permits identification of data subjects for no longer than necessary for the purpose the personal data are processed ("storage limitation"); and
- processed in a manner that ensures appropriate security of the personal data, including the protection against unauthorized or unlawful processing ("integrity and confidentiality").

4.2. Data collected and processed

Personal Data from Customers, third parties, investments, services providers or employees are collected upon consent of the other party and in order to fulfil the regulatory or contractual duties of 6M as AIFM, such as:

- compliance with legal obligations;
- the detection or prevention of any unlawful activities, in the course of financial screening;
- facilitating the management and administration of AIFs and entities for which 6M has been appointed as AIFM/service provider;
- for communicating in connection with the provision of administration services;
- operating IT systems, software and business applications;
- supporting IT, Business Applications Support, Accounting, Legal, Tax, Reporting, Compliance, Internal Audit and Risk Management, as well as the Administrative, Transfer, Document Storage, Record Keeping and other related teams and functions;
- to enforce or defend the Company's rights, or those rights of third parties to whom we each may delegate responsibilities or rights in order to comply with a legal or regulatory obligations imposed on 6M;
- collecting, processing, transferring, and storing "customer due diligence", source of funds information and verification data in accordance with the Luxembourg anti-money laundering and terrorist financing laws and regulations; and
- liaising with or reporting to any regulatory authority (including tax authorities) with whom 6M is required to cooperate with and to report to.

Categories of data collected:

- ID: these include the name, the first name and the job title;
- Contact information: this includes the e-mail address(es), phone numbers (landline and mobile);
- Tax residence: knowing tax residence enables the Company to determine the possible obligations, particularly tax obligations, to the State of which the beneficiary is a national but also in terms of social levies;
- Data relating to the economic and financial situation;
- National identification numbers (e.g. social security number, tax identification number);
- Information contained on ID documents (e.g. passport, identity card);
- Personal characteristics (e.g. date of birth, gender, marital status, dependents and emergency contacts, nationality and entitlement to work in Luxembourg);
- Banking and financial data (e.g. bank account number, national insurance number, entitlement to benefits such as pensions or insurance coverage);
- Employment and occupation (e.g. job title and responsibility, qualifications, skills, periods of leave taken by you, including holiday and other absence records, and the reasons for the leave);
- Documents gathered during the recruitment process (experience and employment history, including start and end dates, with previous employers and with the company);
- Performance information (including management metrics, appraisals, feedback);
- Expenses and travel information (e.g. details of travel that you undertake in connection with your employment, details of expenses you incur, including on any corporate credit card);
- Details of any disciplinary or grievance procedures in which the Data Subject has been involved, including any warnings issued to the Data Subject and related correspondence);
- Images and sound (e.g. photos and videos);
- Special categories of data (e.g. criminal records);
- Details of your schedule (days of work and working hours) and attendance at work;
- Other information provided by you (e.g. survey responses).

Criminal records data may only be processed within the limits of the Luxembourg law of March 29, 2013 on the criminal records register as amended.

In processing Personal Data, 6M must inform Data Subjects of the data that is being collected, how it is being used, how long it will be kept and whether it will be shared with any third parties. This information must be communicated concisely and in plain language.

4.3. Processing of activities tracker

In accordance with Article 30 of GDPR, 6M must, as Controller (Article 30 (1)) or as Processor (Article 30 (2)), implement and keep up to date a record of processing activities. Such record of processing activities is maintained on 6M's network under the Compliance function network in a dedicated folder.

6M shall make the record available to the CNPD on request.

5. RECIPIENTS AND USERS OF THE PERSONAL DATA

The Company may have to communicate the personal data to the following categories of recipients (without limitation):

- The authorized members of 6M' employees and any natural or legal person authorized by it to process personal data;
- Affiliated companies of 6M;
- If applicable, courts concerned, arbitrators, and/or mediators;
- The concerned public authorities, supervisory authorities and all public bodies authorized to receive them;
- Transfer agent, auditors of AIFs managed by the Company;
- Goods and services providers (such as providers of marketing services where we are permitted to disclose your personal information to them) intermediaries, banks, brokers and other individuals, counterparties and entities that partner with 6M;
- Departments responsible for controls such as auditors as well as the departments responsible for internal control;
- A potential buyer, transferee, merger partner or seller and their advisers in connection with an actual or potential transfer or merger of part or all of 6M's business or assets, or any associated rights or interests, or to acquire a business or enter into a merger with it;
- Delivery Settlement Systems;
- Credit reference agencies or other organizations that help us to conduct anti-money laundering and anti-terrorist financing checks and to detect fraud and other potential criminal activity; or
- Any person to whom disclosure is allowed or required by local or foreign law, regulation or any other applicable instrument.

These recipients may be located outside Luxembourg, in this respect obligations as referred to in section 8 of the Policy must be applied.

6. DATA PROTECTION OFFICER

In accordance with article 37 of GDPR, 6M does not fall into the situation where it shall appoint a DPO. Indeed, 6M is not treating personal data on a large scale and has, as of the date of the Policy, a limited number of employees (less than 100). However, considering that 6M through its activities shall be in position where personal data must be treated, 6M shall remain committed to GDPR compliance at all times and in proportion to its activities. 6M shall therefore closely monitor the evolution of the criteria according to which the need of a DPO might be assessed.

According to Article 39 of GDPR, the following tasks have been assigned to the Head of Legal and Compliance:

- to inform and advise the Controller/Processor and the employees who will carry out their processing of the obligations pursuant to the GDPR and to other European Union ("**EU**") countries or Member State data protection provisions;
- monitor compliance with the GDPR, with other EU or Member States data protection provisions and with the policies of the Controller/Processor in relation to the protection of personal data, including the assignment of responsibilities, awareness
- raising and training of employee involved in processing operations, and the related audits;
- provide advice where requested in regards of the DPIA (as such term is defined below) and monitor its performance;
- responsible person for investigation and filing of potential data breaches;
- cooperation with the supervisory authorities;
- act as the main contact point for the supervisory authority on issues relating to processing and consult, where appropriate, with regard to any other matter.

7. LEGITIMATE INTEREST

In accordance with the data minimisation principle, Personal Data may only be processed for certain legitimate purposes. Thus, prior to any Personal Data processing within 6M, it is determined, together with the Head of Legal and Compliance (i) whether such Personal Data Processing uses any Personal Data, and (ii) if yes, the related lawfulness basis, i.e. either:

- The Data Subject has given consent to the processing of his or her Personal Data for one or more specific purposes, or
- Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the Data Subject prior to entering into a contract, or
- Processing is necessary for compliance with a legal obligation to which the Data Controller is subject, or
- Processing is necessary in order to protect the vital interests of the Data Subject or of another natural person, or
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, or
- Processing is necessary for the purposes of the legitimate interests pursued by the Controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the Data Subject which require protection of Personal Data, in particular where the data subject is a child.

8. PERSONAL DATA TRANSFER

The Company and its Customers and counterparties are active outside Luxembourg and data may therefore, in accordance with the objectives described above, be transferred to EU countries or to third countries, i.e. countries located outside the EU or the European Economic Area ("**EEA**").

As stated by Article 45 of GDPR, "a transfer of personal data to a third country or an international organisation may take place where the European Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection. Such a transfer shall not require any specific authorisation". This country shall be considered as an adequate country in the frame of the Data Protection Legal Framework.

In case the counterparty is located outside of the EEA and in a third-party country which does not ensure an adequate level of protection with respect to Personal Data Processing, 6M should put in place a basis for Personal Data transfer as further described in Article 46 of the GDPR and may notably but not exclusively use the relevant standard contractual clauses ("**SCCs**") and have it signed by the counterparty or binding corporate rules to render the transfer of Personal Data outside of the EEA lawful. An annual review of the SCCs must be performed by 6M ensuring whether specific amendments have been performed.

If Personal Data must be transferred cross-border to a third party located in a non-adequate country and in the absence of appropriate safeguards such as SCCs or binding corporate rules, a transfer or a set of transfers of Personal Data may only take place if at least one of the following conditions is satisfied:

- The Data Subject has given explicit consent to the transfer after having been informed of the possible risks of such transfer;
- The transfer is necessary for the performance of a contract with the Data Subject and 6M as Controller or to take necessary steps at the request of the Data Subject prior to enter into a contract;
- The transfer is necessary for the conclusion or performance of a contract concluded in the interest of the individual between 6M and another person;
- the transfer is necessary for important reasons of public interest;
- the transfer is necessary for the establishment, exercise or defence of legal claims;
- The transfer is necessary to protect a vital interest of the individual where the individual is physically or legally incapable of giving consent;
- The transfer is made from a register which according to EU or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down by EU or Member State law for consultation are fulfilled in the particular case.

9. OUTSOURCING

For any initiation of relationship with an external counterpart, 6M's employees should check with the Head of Legal and Compliance whether the present guidelines have been complied with. The protection of Personal Data shall be always guaranteed to 6M's Customers.

The laws of third countries regarding Personal Data may not be as complete as the laws applicable in the territory of Luxembourg and the EU. However, if the Company uses service providers in a third country, it requires them to apply the same level of protection as that applicable in the EU.

More generally, the Personal Data can be transferred to a third country only in a manner authorized by the Data Protection Legal Framework and ensuring that the country to which the personal data are transferred is considered by the EU Commission to provide an adequate level of protection, putting in place contractual clauses the EU Commission consider to provide the same level of protection as further described in paragraph 8 above.

The Company shall track, in the Processing Activity Tracker as referred to in paragraph 4.3 the level of protection applied by the services providers to which personal data are transferred and put in place or carefully review provisions or agreements of outsourcing including Customers or employees Personal Data.

The Company also ensures that its delegates have appropriate safeguard and control measures in case they collect and/or process personal data outside the EU or EEA.

The outsourcing does not relieve 6M of its legal and regulatory obligations or its responsibilities to its Customers when it comes to Personal Data Processing.

Data protection agreement must be put in place when 6M as Controller transfer Personal Data to another entity acting as Processor. The outsourcing shall not result in any delegation of 6M's responsibility to the Processor.

10. MARKETING AND RIGHT TO OPT-OUT

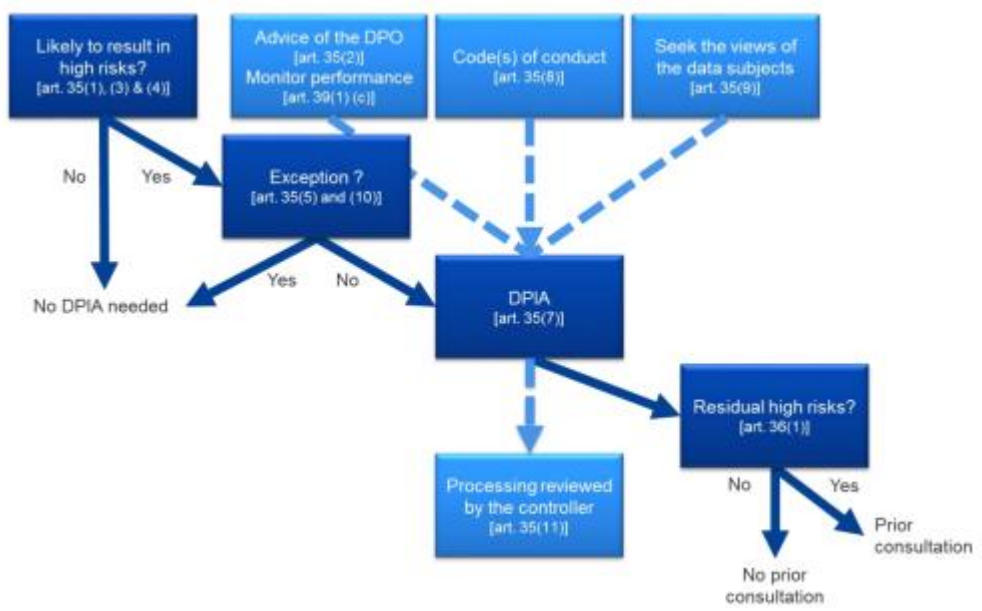
6M will not process Personal Data for marketing purposes if the employees, investors, intermediaries, delegates and providers do not wish to receive marketing materials. Data Subjects can request that 6M stop processing Personal Data for marketing purposes at any time by clicking on marketing opt-out links in any electronic marketing materials sent by 6M or by making a request to julie.bourgeois@6m.lu.

11. DATA PROTECTION IMPACT ASSESSMENT ("DPIA")

Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, 6M shall, prior to the Personal Data Processing, carry out an assessment of the impact of the envisaged processing operations on the protection of Personal Data. A single assessment may address a set of similar processing operations that present similar high risks.

The DPIA aims to assess the necessity and proportionality of the data processing and to give a guidance on managing the risks to the rights and freedom of data subjects resulting from the processing of personal data.

The following chart shows how to process with a DPIA:



Source: Article 29 Data Protection Working Party[1]

The following examples of processing published by ALFI are considered as data processing's which require a DPIA[2]:

Type of data processing	Matching DPIA criteria
Phone recordings	- Systematic monitoring - Sensitive or highly personal data - Vulnerable subjects (employees) - Innovative or technical/organisation solutions - Large scale
AML/KYC International sanctions (Customers & Employees) Frequent transactions monitoring Dormant accounts, etc.	- Sensitive or highly personal data - Large scale - Evaluation or scoring - Matching or combining data sets - Automated decision making - Systematic monitoring - Prevents service or contract

[1] Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for purposes of Regulation 2016/679. Adopted on 4 April 2017. European Data Protection Board.
[2] ALFI GDPR Q&A Issue 3, Luxembourg, 14 June 2021 p.21

Whistleblowing	- Sensitive or highly personal data - Vulnerable subjects (employees) - Innovative or technical / organisational solutions
Fraud database	- Evaluation or scoring - Automated decision making - Prevents service or contract - Sensitive or highly personal data
CRS/FATCA/Tax	- Sensitive or highly personal data - Large scale - Evaluation or scoring - Systematic monitoring - Matching or combining data sets - Prevents service or contract
Tracking/Marketing	- Evaluation or scoring - Systematic monitoring - Innovative or technical/organisational solutions
Profiling in categories	- Profiling (Evaluation/Scoring) - Large scale - Innovative or technical/organisational solutions
Insider trading lists (Customers & Employees)	- Vulnerable subjects (employees) - Systematic monitoring
CRM/Customer database	- Large scale - Sensitive or highly personal data - Evaluation or scoring - Matching or combining data sets
Robo-advice	- Evaluation or scoring - Automated decision making - Innovative or technical/organisation solutions - Large scale - Sensitive or highly personal data

The DPIA has to be performed by the Controller and needs to be continuously reviewed and regularly re-assessed.

12. PERSONAL DATA BREACH

12.1. Types of data breaches

In the case of Personal Data Breaches, it has to be differentiated if 6M is acting as a Controller or as a Processor:

- In its capacity as a Controller (the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data), 6M is required to report any Personal Data Breaches without any delay, but not later than 72 hours after having become aware, to the CNPD, unless the Personal Data Breach is unlikely to result in a risk to the rights and freedoms of natural persons. In case the notification has not been done within 72 hours, a justification for the delay in reporting is required.
- In its capacity as Processor (a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller), 6M has to inform the Controller immediately after becoming aware of such breach.

Any employee of 6M is required to immediately inform the Head of Legal and Compliance of actual or potential Personal Data Breaches by using the email address julie.bourgeois@6m.lu.

In case of becoming aware of a Personal Data Breach, the following information are mandatory to report:

- a description including the nature and, where possible the categories, as well as any impact of the Personal Data Breach;
- a list of the involved parties/departments when employees are involved;
- the approximate number of Data Subjects and Personal Data concerned;
- name and contact details of Head of Legal and Compliance in case further information are required (if applicable).

Based on the information received, the Head of Legal and Compliance will decide if the Personal Data Breach must be reported to the authorities and/or the concerned Data Subjects according to GDPR.

A register containing all personal data breaches including its reasons, its impact, and effects as well as the remedial actions taken is maintained and monitored by the Legal and Compliance Function. The activities tracker must be provided to CNPD upon request.

12.2. Communication of Personal Data Breach to the Data Subject

In case the Personal Data Breach is likely to result in a high risk to the rights and freedom of a Data Subject a communication needs to be sent to the persons impacted.

The communication to the Data Subject is not required to the extent:

- 6M as Controller has implemented appropriate organizational and technical measures to protect Personal Data and those measures have been applied to the Personal Data affected by the breach, e.g. techniques as encryption;
- 6M as Controller has taken subsequent measures to ensure that the high risk is no longer likely to materialize;
- the communication to the Data Subject would involve disproportionate effort, in such cases a public communication or similar measures should be taken.

13. DATA SUBJECT RIGHTS

The Company acting as Controller, shall take appropriate measures to provide any information and any communication in accordance with GDPR relating to Personal Data Processing to the Data Subject in a concise, transparent, intelligible and easily accessible form. Communication shall be made by written form including electronic form except when orally requested by Data Subject.

In accordance with the legal and regulatory obligations Personal Data must be processed in accordance with the rights of the Data Subjects, namely:

- The right of access
- The right to be informed
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to receive the Personal Data
- The right to object
- The rights related to automated decision making, including profiling

Data Subject may exercise rights at any time by sending an email at julie.bourgeois@6m.lu.

In annex to the present Policy, 6M has highlighted the individual rights granted by the GDPR, explained what they mean in practice, and describe the process put in place in relation thereto.

14. DATA RETENTION RULE

Personal Data cannot be kept in the Company's files for un undefined period, and unless specified by law, a retention period must be defined according to the purpose for which the Personal Data was collected. Once the purpose has been achieved, Personal Data must be archived, deleted, pseudonymised or made anonymous. 6M must define, according to the nature of the data, their usefulness and the purpose sought, the duration of Personal Data retention.

Pursuant to the legal and regulatory obligations and subject to any amendments of the retention periods, 6M will, notably but not solely, keep employees, Customers, delegates, intermediaries and providers' Personal Data for the following periods:

- Extract of criminal records: 1 month;
- Employment contracts: 10 years as of the end of the employment contract and 2 years for potential (not hired) candidates;
- Personal data as mentioned by Section 4.2(e.g. name, date of birth, tax registration number, social security number, address, email address): 10 years;
- Data for purposes of payroll records (e.g. wages, tax and social security records, including timesheets and data resulting from the badge authentication to monitor working hours): 3 years;
- Unactive data subject: personal data of people who have been inactive for 3 years in the Company's database can be erased. Ideally, those personal data shall be placed in an exclusion database allowing to justify the processing. These data can also be made pseudonymised in order to keep them for their statistical value.

15. SUPERVISORY AUTHORITY

6M is supervised by the CNPD which is the competent data protection authority in Luxembourg. The CNPD is an independent authority which is entitled to verify the legality of the processing of Personal Data and ensures the respect of personal freedoms and fundamental rights with regard to Personal Data protection and privacy. The CNPD further ensures the respect of the specific rules for the protection of privacy in the sector of electronic communications.

16. PRIVACY NOTICE

6M ensures that Data Subjects are aware that their Personal Data is being processed, and that they understand how it is being used and how to exercise their rights.

6M has a Data Privacy Notice, setting out how Personal Data relating to Data Subjects is used by 6M. 6M's Data Privacy Notice is available on 6M's website.

17. POLICY OWNER AND DATE OF IMPLEMENTATION

The Head of Legal and Compliance has been formally appointed as the owner of this Policy. Any amendment to this Policy may be made by the Legal and Compliance Function and Senior Management and must be duly approved by the Board of Managers of the Company. The Policy must be updated on an annual basis at minimum and ad hoc upon trigger events, such as but not limited to, changes in applicable regulations.

18. APPROVAL

This Policy has come into force by approval of the Executive Committee and adoption by the Board of Managers and has no signatures.

Annex 1: GDPR Rights

GDRP Rights	GDPR Articles	Rights details	How 6M address it
Right to be informed	12, 13, 14	Before Personal Data is collected, Data Subject has the right to know how it will be collected, processed, and stored, and for what purposes.	Make available clear Policies informing the Data Subject before the collection of Personal Data starts.
Right to Access	12, 15	After Personal Data is collected, a Data Subject has the right to know how it has been collected, processed, and stored, what Personal Data exists, and for what purposes.	• track all Personal Data relating to the Data Subject, • vet a right to access request, and • provide that information to the Data Subject.
Right to Correction ("Rectification")	12, 16	Data Subject has the right to have incorrect or incomplete Personal Data corrected.	• vet a right to access request, • correct the Personal Data, and • confirm correction to the Data Subject. As this also applies to Personal Data 6M might pass on to third parties, the Company needs to securely inform the Data Subject of the correction.
Right to Erasure (Right to Be Forgotten)	12, 17	Data Subject has the right to have Personal Data permanently deleted.	• track all data relating to Data Subject in 6M's systems, • Data Subjects are vetted a right to erasure request, • erase all Personal Data in the request, and • confirm erasure to the Data Subject.
Right to Restriction of Processing	12, 18	Data Subject has the right to block or suppress Personal Data being	• track all data relating to Data Subject in 6M's systems,

		processed or used.	• Data Subjects are veted a right to restriction of processing request, • 6M must be able to stop processing without erasing the Personal Data, and • confirm the restriction in processing to the Data Subject.
Right to Data Portability	12, 20	Data Subject has the right to move, copy, or transfer Personal Data from one Controller to another, in a safe and secure way, in a commonly used and machine-readable format. Wherever technically possible, this also includes the right to have the Personal Data transferred directly from one Controller to another without the Data Subject having to handle the Personal Data.	• track all Personal Data relating to requestor in 6M's systems, • vet a right to Personal Data portability request; • transfer Personal Data to another Controller or else the Data Subject securely, and • confirm the transfer to the Data Subject if applicable.
Right to Object to Processing	12, 21	Data Subject has the right to object to being subject to public authorities or companies processing its Personal Data without explicit consent. Data Subject also has the right to stop Personal Data from being included in direct marketing databases.	• track all data relating to Data Subject in 6M's systems; • vet a right to object to processing;
Right to Not Be Subject to Automated Decision Making	12, 22	Data Subject has the right to demand human intervention, rather than having important decisions made solely by algorithm.	Inform the Data Subject that they will be subject to algorithmic decision-making and that they can opt out of it.

ANNEX 2: REGULATORY REFERENCES

The Company takes the necessary steps to align its Data Protection Policy with current best practices and the relevant Luxembourg regulatory framework.

Laws	Law of 10 August 1915 on commercial companies
	30 May 2005 concerning the specific provisions for protection of the individual in respect of the processing of personal data in the electronic communications sector, and amending Articles 88-2 and 88-4 of the Code of Criminal Procedure
	Law of 17 December 2010 relating to undertakings for collective investment
	Law of 12 July 2013 on alternative investment fund managers
	Luxembourg law of 1 August 2018 on the organisation of the National Commission for Data Protection and implementation of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data
CSSF Circular	Circular CSSF 18/698 on the authorisation and organisation of investment fund managers incorporated under Luxembourg law and including specific provisions on the fight against money laundering and terrorist financing applicable to investment fund managers and entities carrying out the activity of registrar agent
Code	Criminal Code of the Grand Duchy of Luxembourg
Directive	Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data
Regulations	Grand-Ducal Regulation of 27 November 2004 (on data protection officers) concerning the data protection officer, in implementation of Article 40 (10) of the Amended Act of 2 August 2002 on the protection of individuals with regard to the processing of personal data
	Grand-Ducal Regulation of 24 July 2010 (on traffic and localisation data) Regulation determining the categories of personal data generated or processed in connection with the provision of electronic communications services or public communication networks
	CSSF Regulation N° 10-04 transposing Commission Directive 2010/43/EU of 1 July 2010 implementing Directive 2009/65/EC of the European Parliament and of the Council as regards organisational requirements, conflicts of interest, conduct of business, risk management and content of the agreement between a depositary and a management company
	Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)