PERSONAL DATA PROTECTION POLICY

Version	Date of review by the Conducting Officers	Date of approval by the Board of Directors
V1	10 June 2020	24 June 2020

TABLE OF CONTENTS

1. GLOSSARY

Term	Description
AIF(s)	The alternative investment fund(s) that the AIFM (as defined hereunder) manages
The AIFM	Amethis Investment Fund Manager S.A.
Amethis Group	A group of companies comprising the AIFM and its operating affiliates based in France, Ivory Coast, Kenya and Morocco
CNPD	*Commission nationale pour la protection des données* of Luxembourg
Conducting Officers	The persons who effectively conduct the business of the AIFM
CSSF	*Commission de Surveillance du Secteur Financier*, i.e. the financial services regulator of the Grand-Duchy of Luxembourg
CSSF Circular 18/698	See below, under '2. MAIN APPLICABLE LAWS, RULES AND REGULATIONS'
ESG	Environmental, social and governance
Investors	The counterparties investing directly in the AIFs
Policy	This Voting Rights Policy, as may be amended from time to time
Investments	The companies in which the AIFs have invested or to which they have lent, and all companies to which they intend to do the same (including any downstream borrower)

2. MAIN APPLICABLE LAWS, RULES AND REGULATIONS

European Union	Law, rule and regulation
European Union - Regulation	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" or "GDPR")
Grand-Duchy of Luxembourg	**Law, rule and regulation**
Grand-Duchy of Luxembourg - Law	Law of 2 August 2002 on the protection of persons with regard to the processing of Personal Data as amended

Term	Description
AIF	Alternative Investment Fund
AIFM	Alternative Investment Fund Manager
AIFM Representatives	The Staff members, Board members and Shareholders of the AIFM who have a need to know the Personal Data
Amethis Investment Fund Manager S.A.	The "AIFM"
BoD	Board of Directors of the AIFM
CNPD	Commission Nationale pour la Protection des Données, Luxembourg
Compliance Officer	Natural person in charge of the Compliance function established by the AIFM i.e. the Conducting Officer in charge of Risk Management
Conducting Officers	Persons who effectively conduct the business of the AIFM, i.e. the Conducting Officer in charge of Risk Management and the Conducting Officer in charge of Portfolio Management and any other person who may be nominated as such
CSSF	Commission de Surveillance du Secteur Financier, Luxembourg
Data 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 Personal Data Processing; 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. Joint Data Controller: where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers
Data Processor	A natural or legal person, public authority, agency or other body which processes Personal Data on behalf of the Data Controller.
Luxembourg Data Protection Regulations	Applicable law and regulation as mentioned in Section 2 below
Personal Data	Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is 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 Processing	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
Shareholders	The shareholders of the AIFM
Staff member	Any individual, being part of the management or employee of the AIFM
The Policy	This "Personal Data Protection Policy", as amended from time to time

3. APPLICABLE REGULATIONS

Law	Law of 2 August 2002 on the protection of persons with regard to the processing of Personal Data as amended
Regulation	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" or "GDPR")

4. PURPOSE OF THE POLICY

The Policy applies to any Personal Data Processing by the AIFM. The AIFM shall have operational procedures and controls in place satisfying the requirements described in this Policy. Personal Data is indeed a critical asset and the AIFM, as Data Controller for a number of Personal Data, is accountable for processing such information with the requisite care, integrity and discretion so as to provide appropriate protection to Personal Data and comply with Luxembourg Data Protection Regulations. AIFM Representatives who process Personal Data are therefore each subject to Luxembourg Data Protection Regulations.

Personal Data include all information provided or collected which concern any personal aspect of Staff members and/or Board members and/or shareholders and/or the AIFM and/or personal information around the AIFs managed (members of the Board of Directors of the AIFs, investors in the AIFs, etc.).

The Policy is approved by the BoD and it applies to the AIFM.

5. RESPONSIBLE PERSONS

The Compliance Officer and the DPO are in charge of the AIFM compliance with Luxembourg Data Protection Regulations.

6. PRINCIPLES AND REQUIREMENTS ON PERSONAL DATA PROCESSING

To the extent that it processes such Personal Data, the AIFM, as Data Controller, must be able to demonstrate that it complies with Luxembourg Data Protection Regulations, taking into account the nature, scope, context and purposes of Personal Data Processing as well as the risks of varying likelihood and severity (proportionality principle).

5.1. GENERAL MANAGEMENT AND GOVERNANCE

The AIFM has implemented appropriate technical and organizational measures to ensure and to be able to demonstrate that processing is performed in accordance with Luxembourg Data Protection Regulations:

- The AIFM has, and maintains, a Personal Data Protection Policy available and up to date. More generally, the AIFM ensures systematic documentation of Personal Data protection measures taken;
- The Compliance Officer and the DPO makes sure AIFM Representatives are aware of Personal Data protection requirements (e.g. through raise awareness session);
- The AIFM Representatives comply with the principle of Privacy by design[1] and Privacy by default[2] concepts, *i.e.* both have an approach which takes privacy into account throughout any engineering process, and an approach which by default collect and retain the minimum necessary Personal Data for a said purpose;

[1] Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the Data Controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects (GDPR, Art 25).

[2] The Data Controller shall implement mechanisms for ensuring that, by default, only those Personal Data are processed which are necessary for each specific purpose of the processing and are especially not collected or retained beyond the minimum necessary for those purposes, both in terms of the amount of the data and the time of their storage. In particular, those mechanisms shall ensure that by default Personal Data are not made accessible to an indefinite number of individuals (GDPR, Art 25).

- The AIFM maintains a Personal Data Processings register[3] (and requires its Data Processors to do likewise);
- The AIFM ensures and monitors its Data Processors compliance with Luxembourg Data Protection Regulations requirements.

In addition, in terms of internal organisation, the AIFM ensures careful breakdown and separation, as well as implementation, of roles and responsibilities and in particular, that:

- Everyone processing Personal Data understands that he or she is contractually responsible for following good Personal Data protection practice;
- Everyone processing Personal Data is appropriately trained to do so;
- Everyone accessing Personal Data does not process them except on instructions from the AIFM unless he or she is required to do so by law. In particular, it is forbidden to use Personal Data for private or commercial purposes, to disclose it to unauthorized persons, or make it available in any other way;
- Anybody wanting to make enquiries about handling Personal Data knows what to do;
- It deals promptly and courteously with any enquiries about handling Personal Data;
- All Staff members are aware that a breach of the rules and procedures identified in this Policy may lead to disciplinary action being taken against them.

Staff members are required to consult the Compliance Officer or the DPO before taking any further action in the following cases:

- New initiatives to transfer or disclose Personal Data;
- Uncertainty as to whether information constitutes Personal Data;
- Suspected or actual breach in Personal Data processing requirements;
- Requests for information from/obligation to notify authorities and private persons;
- Uncertainty as to whether a particular transfer or disclosure of Personal Data is permitted and/or if such transfer needs to be approved beforehand and by whom.

5.2. COMPLIANCE WITH MAIN PERSONAL DATA PROTECTION PRINCIPLES

Lawfulness

[3] Such register is not mandatory" to an organisation employing fewer than 250 persons unless the processing it carries out is likely to result in a risk to the rights and freedom of the data subjects, the processing is not occasional, or the processing includes certain categories of data" (GDPR, Art 30). The maintenance of such register appears however critical to guarantee adequate implementation of the GDPR provisions.

In accordance with the data minimisation principle, Personal Data may only be processed for certain legitimate purposes. Thus, prior to any Personal Data Processing[4] within the AIFM, it is determined, together with the Compliance Officer or the DPO (i) whether such Personal Data Processing uses any Personal Data, and (ii) if yes, the related lawfulness basis f, 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.

If none of these lawfulness bases is able to apply, the Personal Data Processing is not permitted.

As concerns first lawfulness basis, i.e. the data subject consent, the latter's validity is to be checked by the Compliance Officer or the DPO so as to ensure its compliance[5] with Luxembourg Data Protection Regulations.

Maintenance of Personal Data

The AIFM ensures that Personal Data are retained for no longer than necessary given the purpose(s) of their processing by the AIFM, as authorised under the applicable law or regulation. As soon as the relevant retention period has expired, Personal Data are disposed of appropriately (deletion, anonymization or other process).

---

[4] For Personal Data, and subject to the proportionality principle, in case a Personal Data Processing is considered to result in a high risk to the rights and freedoms of data subjects, the AIFM, prior to the processing, carries out an assessment of the impact of the envisaged processing operations on the protection of Personal Data. The CNPD needs to give its prior approval for such Personal Data Processing.

[5] The Data Controller shall bear the burden of proof for the data subject's consent to the processing of their Personal Data for specified purposes (GDPR, Art 7).
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 (GDPR, Art 4 (11)).

Safeguarding data subject rights

In accordance with Luxembourg Data Protection Regulations, the AIFM provides relevant information to data subjects, in a concise, transparent, intelligible and easily accessible form, using clear and plain language as concerns their various rights. Specifically, when Personal Data are collected from the data subject or obtained through another mean, the AIFM provides the data subject with the information required in the Luxembourg Data Protection Regulations[6].

Where the AIFM intends to further process Personal Data for a purpose other than the one for which Personal Data were collected, the AIFM provides the data subject prior to that further processing with information on that other purpose and with any relevant further information.

Finally, the AIFM organizes internally to be at all times in capacity to answer to data subjects exercising their rights, e. g. access, rectification, and objection.

Personal Data transfers

Transfer of Personal Data to a third-party country is generally not permitted. All initiatives within the AIFM that involve or could result in the access to or transfer of Personal Data in a third-party country outside the European area must be reviewed by the Compliance Officer or the DPO.

the Compliance Officer or the DPO will generally accept that the transfer of Personal Data is allowed, when applicable, on the basis of an adequacy decision from the European Commission[7], or due to other guarantees as detailed in the Luxembourg Data Protection Regulations[8].

5.3. IT SYSTEM DESIGN AND SECURITY OF PERSONAL DATA

Personal Data processed by the AIFM or its Data Processors are protected at all times against the risk of loss, theft, unauthorized access, transfer or use, using appropriate (to the risk) organizational and technical safeguards. This includes the pseudonymization and encryption of Personal Data, the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services, as well as the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident, and a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

---

[6] For details refer to GDPR, Art 13 and 14.
[7] For details refer to GDPR, Art 45.
[8] For details refer to GDPR, Art 46, 47, 48, 49.

AIFM Representatives who process Personal Data on behalf of the AIFM are responsible for implementing and documenting these measures. The AIFM keeps track of the latter to demonstrate compliance with required security arrangements.

5.4. OUTSOURCING

The AIFM requires its Data Processors to comply with all above mentioned requirements. In particular:

- The AIFM systematically conducts an initial due diligence before contracting with a party, checking the latter's expert knowledge, reliability, and available resources to implement technical and organizational measures as well as security of processing, as required by Luxembourg Data Protection Regulations.
- With regard to the service level agreement with each Data Processor, minimum term standards[9] are to be included, in accordance with Luxembourg Data Protection Regulation provisions;
- As part of its service providers' monitoring, the AIFM ensures that relevant Luxembourg Data Protection Regulation provisions (e.g. lawfulness of Personal Data processing, legitimacy of Personal Data transfers, transparency/ information towards data subjects, management of Personal Data retention periods, security of processing) are complied with in practice overtime by Data Processors.

5.5. PERSONAL DATA BREACH

AIFM Representatives must immediately contact the Compliance Officer or the DPO in case they know, suspect or anticipate that Personal Data have been or may be lost, stolen, or accessed, used, destroyed, modified or disclosed in an unauthorized manner. The Compliance Officer or the DPO then decides on the measures to be launched.

In case a Personal Data breach is confirmed, the AIFM is required to send:

- A notification to the CNPD within 72 hours after learning the breach except if it is considered unlikely that there is a risk for the data subject rights;
- A notification to the data subject without delay[10].

7. REVIEW OF THE POLICY

[9] For details refer to Article 28 of GDPR.
[10] In case it is considered as high risk for individual freedoms and liberties, unless any condition of Article 34 (3) Data Protection Regulation are fulfilled.

The Policy will be reviewed at least once a year by the DPO in committee under the supervision of the BoD. In fact, the Conducting Officers conduct a central and independent review of the implementation of the Policy in order to assess if it:

- Is operating as intended; and
- Is compliant with national, international regulations principles and standards applicable to the sector within which the AIFM operates.

Where no update is required, the Policy will be applied consistently over time. Where update is required, formal approval by the BoD is necessary.

I have acknowledged the Personal Data Protection Policy and I commit to follow it

Made at … the …. / …. / ….

Signature