VAM GLOBAL MANAGEMENT COMPANY SA
Public limited liability company (*société anonyme*)
Registered office: Josy Welter House. 8-10, rue Genistre, L-1623 Luxembourg
R.C.S. Luxembourg: B 207.262
("**VAM GMC**")

Data Protection Policy (the "Policy")

This Policy has been adopted by, and therefore covers:
VAM Global S.a.r.l.
VAM Funds (Lux) SICAV
VAM Managed Funds (Lux) SICAV

Policy	Data Protection Policy	**Approved by**	The Board of Directors of VAM GMC	
Policy application date	Effective immediately upon adoption	**Original Approval date**	02.04.2019	Version 4.0
		Last Revision Date	17/10/2023	Version 7
Next revision date	2024 Q4	**Distribution**	Internal / ManCo website	

Index:

1. Introduction

VAM Global Management Company SA (hereafter "VAM GMC") is a public limited liability company (société anonyme) incorporated and governed by the laws of the Grand Duchy of Luxembourg, having its registered office at Josy Welter House. 8-10, rue Genistre, L-1623 Luxembourg, registered with the Registre de Commerce et des Sociétés de Luxembourg under number B207.262.

VAM GMC is currently licensed by the CSSF as a Management Company under the regime set out in Chapter 15 of the Law of December 17th, 2010 on undertakings for collective investment. Accordingly, VAM GMC is what is commonly known as a 'UCITS management company'.

1.1 Legal background

This Policy provides for the principles and measures adopted by VAM GMC based on the following European Union and Luxembourg laws and regulations, including without limitation:

- Regulation EU 2016/679 – General Data Protection Regulation "GDPR";
- Directive 2002/58/EC on Privacy and electronic communications;
- Law of August 1st, 2018 implementing certain aspects of GDPR and regarding the organisation of the *Commission National pour la protection des données* "CNPD";
- Law of August 1st, 2018 regarding processing of personal data in criminal matters and national security;
- Law of May 30th, 2005 as modified from time to time laying down specific provisions for the protection of persons with regard to the processing of personal data in the electronic communications sector.

All terms in capital letters unless otherwise defined in this Policy shall have the meaning given by GDPR.

1.2 Purpose

This Policy lays down the principles to which employees must adhere to guarantee confidentiality and professionalism in activities involved in Personal Data Processing in compliance with the applicable legal provisions.

The Policy sets forth:

- The principles and obligations of the Data Controller regarding Processing of the Personal Data;
- The rights of the Data Subject whose Personal Data is processed;
- The various types of Personal Data Processing;
- The principles of Transfers of Personal Data;
- The principles of Processing of Personal Data of Employees and candidates;
- The organisational solutions adopted by VAM GMC;
- The procedure of Personal Data Breach management.

VAM GMC may collect and use its clients' (being the individual or institutional or corporate investors, hereinafter collectively called the "Clients") and its potential Clients' Personal Data (e.g. name, age and date of birth, address, residence, e-mail etc.). When the Clients or potential Clients are legal entities, VAM GMC may collect the Personal Data of these companies' representatives, ultimate beneficial owners, authorised signatories etc. for the purposes relating to performance of contracts including pre-contractual arrangements, or to comply with specific regulatory requirements. VAM GMC also collects and uses the Personal Data of its current and former employees for employment related activities exclusively. The rules set forth in this Policy will equally apply to processing of any Personal Data collected by VAM GMC on behalf of the funds under its management acting for this purpose as joint controllers.

All these natural persons listed below:

- Clients, potential Clients;
- Client companies' representatives, ultimate beneficial owners, authorised signatories;
- Employees and former Employees;
- Members of Management;
- Representatives, ultimate beneficial owners, authorised signatories, employees of any service providers used by VAM GMC;

are the Data Subjects according to GDPR, and VAM GMC, which determines the purpose and means of the processing, will act as the Data Controller in the meaning of GDPR.

1.3 The scope of application

This Policy and the principles herein apply to Management (e.g. the members of the Board of Directors, the Conducting Persons, the management and control bodies), and to all employees, including any temporary employees, officers, interns, contractors of VAM GMC (collectively the "Employees").

Failure to comply with these guidelines may result in disciplinary action including termination of employment in very serious cases.

In addition, these guidelines aim to provide a reference area for activities related to Data Processing but exclude all issues relating to logical security which are dealt with elsewhere.

The Data Protection Responsible Officer should be contacted for all issues relating to Data Protection according to the subject being dealt with (see § 2.1).

2. GENERAL OVERVIEW

2.1 The organisational approach adopted by VAM GMC

VAM GMC has adopted the following organisational approach which envisages the division of responsibilities between the Data Protection Responsible Officer and the Conducting Person in charge of IT Department.
Namely:

- Data Security is the responsibility of the IT Department which is under supervision of the Conducting Officer in charge of IT, who defines appropriate guidelines, validates processes and procedures in scope of the first level controls. The second level controls are performed by the Compliance Department;
- Data Processing is the responsibility of the Data Protection Responsible Officer who defines appropriate guidelines, validates processes and procedures in scope of the first level controls and consequently designs and executes the second level controls and provides advice/opinions;
- VAM GMC has decided not to appoint a Data Protection Officer "DPO", as it has assessed that, given the limited amount of data being processed and the size of VAM GMC, the implementation of this requirement is not necessary. However, VAM GMC decided to appoint the Compliance Officer to act as Data Protection Responsible Officer (the "DPRO") who will be overseeing the implementation and application of data protection policy rules.

2.2 General principles of Data Processing

VAM GMC, in the course of its activities, carries out various types of Personal Data Processing that complies with the following general principles:

- Data must be processed fairly, lawfully and in a transparent way;
- Data must be collected for specified, explicit and legitimate purposes and not subsequently processed in a way incompatible with those purposes;

- Data Processing must be adequate, relevant and must not be excessive in relation to the purposes for which data was collected and/or subsequently processed;
- Data must be accurate and, where necessary, updated. Reasonable steps must be taken to ensure that data which is inaccurate or incomplete is erased or rectified;
- Data must be kept in a form which permits identification of Data Subjects and for no longer than is necessary for the purposes for which it was collected or processed and for as long as required by law.

Moreover:

- Data must be processed in a confidential manner and stored in a way and place which ensure appropriate security and restricted access to it;
- Surveillance at the workplace shall be possible only to the extent strictly limited by law.

It is the responsibility of the Data Protection Responsible Officer to ensure that these principles are complied with.

Access to Personal Data must be based on appropriate authorisation and a clear need for its use connected with one of the lawful grounds for processing as set out in the GDPR. Every third party receiving the access to Personal Data held by VAM GMC is responsible for protecting it and for being compliant with the applicable data protection laws and regulations. VAM GMC is responsible for ensuring that such third party is subject to regular monitoring through proper due diligence.

At VAM GMC, any suspected breach of the rules set forth in this Policy must be reported to the DPRO.

3. GENERAL OBLIGATIONS

VAM GMC complies with the following requirements when Processing Personal Data:

- **Information notice to the Data Subject:** The Data Controller must ensure that the Data Subject receives the following information when the Personal Data is obtained directly from the Data Subject. The below information shall be provided at the time when personal data is obtained:
    - The details of the Data Controller and, where appointed, the Data Processor;
    - The purposes and legal basis for the Processing;
    - Where the Processing is based on the legitimate interest pursued by the Data Controller or by a third part, this legitimate interest shall be communicated;
    - The recipients or categories of recipients to whom data is communicated;
    - The possibility of transfer of the Personal Data to third country or international organisation, the existence or absence of an adequacy decision by the CNPD, or information about appropriate or suitable means applied by the Data Controller (including information where copy of them is available or how to obtain the copy);
    - The voluntary or mandatory nature of providing the requested data as well as the possible consequences of failure to provide data;
    - The existence of the rights listed in article 4 below and how they may be exercised;
    - The period for which the Personal Data will be stored, or, if that is not possible, the criteria used to determine that period.

VAM GMC is not obliged to provide the Data Subject with the information which the Data Subject already has. Pursuant to accountability rules, VAM GMC shall be able to demonstrate which information the Data Subject has already obtained.

When the data has been obtained from a source other than the Data Subject, within a reasonable period after obtaining that data, but no later than one month, the Data Controller must ensure that the Data

Subject in addition to the above information receives also information about the categories of data concerned and the source from which the data originated and whether that was a publicly accessible source.

VAM GMC is not obliged to provide the Data Subject with the information when:

a) The Data Subject already has the information;
b) The provision of such information is impossible or would involve a disproportionate effort;
c) The Data Controller is subject to national or European law requirements which provide appropriate protection for Data Subject's legitimate interests;
d) The data must remain confidential due to professional secrecy obligations binding the Data Controller.

Other particular obligations of the Data Controller:

- Data Subject's consent: it is one of the legal bases for the lawful processing of Personal Data. VAM GMC needs to obtain consent when no other lawful basis applies. Under GDPR the consent is defined as "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 the personal data relating to him or her". VAM GMC as Data Controller is responsible for obtaining the consent under the advice received from the DPRO.
- The Data Controller provides a clear privacy notice wherever Personal Data is collected to ensure that the consent is informed and that the Data Subject is informed of their rights. When the consent was not in writing, the fact that it was collected should be otherwise documented.
- Whenever the consent is obtained from the Data Subject, the Data Subject shall also be informed about the right to withdraw the consent at any time and how to exercise this right.
- For written consent the Data Subject shall sign the Consent Form which is the Appendix 1 to this Policy.
- The Data Controller will ensure that explicit consent is obtained for the following situations, unless there is another legal basis for processing the data;
    - Processing of special categories of Personal Data, i.e. ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation (art.9 GDPR);
    - Automated individual decision-making, including profiling (art. 22 GDPR);
    - Transfer of the Personal Data to third country or international organisation in the absence of appropriate safeguards.

All consents obtained from the Data Subjects have to be registered in Consent Register which is the Appendix 6 to this Policy.

- Processing for direct marketing purposes: Data Subject shall be informed at the latest at the time of the first communication that he/she has the right to object to processing for direct marketing purposes. The Controller will ensure that this information is presented clearly and separately from other information.
- Implementation of organisational, technical and security measures: The Data Controller must implement appropriate technical, organisational and security measures to protect Personal Data against accidental or unlawful destruction or accidental loss, unauthorized disclosure or access. This shall include the users' access management procedure, reporting on information security weaknesses and information security events. The Data Controller will put in place a Personal Data Breach Register which template is attached as Appendix 2 to this Policy.
- Appointment of Data Processor: The Data Controller may appoint one or more entities as Data Processors. Data Processors must have experience and skill, be reliable and able to offer sufficient

guarantees regarding the technical security measures and organisational measures governing the Processing to be carried out. In this context, the Controller will perform an adequate due diligence before appointment of a new Processor. The Data Controller will also take into account if the potential delegate has in place appropriate technical and organisational measures for the fulfilment of the Controller's obligations to respond to requests of the Data Subject's rights laid down in article 4 of this Policy. The Data Processor may only carry out the Processing in accordance with written instructions given by the Data Controller.

- The Data Controller will put in place and keep up to date a Data Processing Inventory (Appendix 3 to this Policy).

4. RIGHTS OF THE DATA SUBJECT

Each Data Subject has the right to request the Data Controller:

1. To confirm whether or not his/her data is being processed, and when it is, the right to access to his/her data, and to receive a copy of the Personal Data held by the Data Controller or appointed Data Processor;
2. If appropriate, a rectification of any Personal Data that is inaccurate;
3. To erase Personal Data when the Processing is no longer necessary for the purposes for which it was obtained, or it is no longer lawful, or the data has been unlawfully processed, or when erasure is required by other legal obligations, subject to applicable retention periods;
4. To restrict the Processing of personal data where the accuracy of the personal data is contested, the Processing is unlawful, if the Data Subjects have objected to the Processing and in other cases accordingly to article 18 (1) of GDPR;

Each Data Subject has also the right to:

5. Object to the Processing of Personal Data (including profiling) on the grounds of a legitimate interest that we as Controller pursue, unless there are legitimate grounds for us to do so (e.g. the establishment, exercise or defence of legal claims);
6. Receive the Personal Data in structured, commonly used and machine-readable format, or to have this data transmitted directly to another controller where technically feasible (data portability right);
7. Withdraw his/her consent at any time, if consent was the lawful ground for processing;
8. In the case of transfer of Personal Data outside of the EU, obtain information about the existence or absence of the adequacy decision published by the European Commission, and when applicable, a copy of, or access to, the appropriate or suitable safeguards which have been implemented by the Data Controller;

Whenever the Data Controller receives the Data Subject's request to exercise any of the above rights, VAM GMC shall be provided with a document confirming the applicant's identity. After the identity has been confirmed, such a document should not be retained unless it is required for other purposes (such as Anti-Money Laundering, for instance).

In order to exercise the Data Subject's right to access his/her data, the Data Subject shall specify which set of data held by VAM GMC he/she seeks by filling in the Access Request Form (Appendix 4 to this Policy) The Data Subject may request all data held on them. The completed Access Request Form (hereinafter the "ARF") is immediately forwarded to the DPRO who records the date of receiving the ARF and ensures that the requested data is collected. One month after the receipt of the request, the Data Controller shall provide the Data Subject with information on actions taken regarding the request; this delay may be extended up to two months for complex and multiple requests. The Data Controller shall inform the applicant about that extension and the reason for it. If after the review of the ARF, the DPRO decides that

no action will be taken, he should inform the applicant within one month of receipt of the request of reasons for not taking action and on the possibility of lodging a complaint with CNPD. The copy of information shall be provided in the same form as the ARF was submitted, unless it is technically not feasible. The first copy of the data shall be provided for free, however, for any further copies VAM GMC may charge a reasonable administrative fee.

When the data Processing has been restricted, VAM GMC may only store the data in question, and any processing of the restricted data requires the Data Subject's consent, unless Processing is necessary for exercise or defence of legal claims, protection of another person's rights or for reasons of important public interest described in article 18 (2) of GDPR. VAM GMC shall inform the Data Subject before the restriction is lifted and data will be processed again.

Unless prohibited by any applicable law, VAM GMC acting as the Data Controller will inform all recipients about any rectification, erasure or restriction of data which have been disclosed to them.

VAM GMC shall facilitate the exercise of the above rights and shall execute them without undue delay.

All requests and complaints regarding Processing shall be sent to email:
vamglobalmanco@vamgrouplux.com

Complaints regarding Data Processing are subject to rules set forth in the VAM GMC Complaints Handling Policy.

5. DATA PROCESSING

5.1 Communication of Personal Data to third parties

VAM GMC does not communicate the Personal Data to third parties unless:

- Necessary for the performance of a contract and in an appropriate manner under the applicable data protection regulation;
- There is a provision of law that requires such communication, e.g. for purposes relating to anti-money laundering regulations, prevention of fraud, bribery or market abuse, for the regulatory and tax reporting purposes, etc.;
- The relevant consent has been obtained from the Data Subject;
- Necessary for the purpose of the legitimate interest pursued by the Data Controller, e.g. exchange of anonymous data for statistical or market analysis purposes, transfer of Employees' data for the purposes related to labour contract management, etc.;
- Required by any judgement of court or tribunal and any decision of an administrative authority, however, if coming from a jurisdiction outside the EU, such transfer of data may only take place on the basis of mutual legal assistance treaty in force between the requesting country and the EU or Luxembourg.

VAM GMC takes every necessary precaution to ensure the legality and protection of such communication.

Whenever the third party which is either the recipient or the Processor is located in a jurisdiction outside the EEA, VAM GMC shall inform the Data Subjects concerned if the country benefits from an adequacy decision, or what kind of safeguards the Data Controller will apply in order to ensure enforceability of Data Subject's rights.

5.2 Protection measures

VAM GMC uses appropriate administrative, technical, physical and security measures to:

- Meet the legal requirements and any specific requirements set forth in labour agreements in place with the Employees;
- Safeguard Personal Data against loss, theft and unauthorized access, use or modification;
- Keep Personal Data accurate, complete and up-to-date;
- Ensure that the Processors processing the data apply adequate security and safeguard measures;
- Ensure that the Processors have in place adequate organisational and technical measures which will allow the Controller to comply with the GDPR requirements.

5.3 Retention of Personal Data

Personal Data is generally retained only for as long as is needed to meet the purposes for which it has been collected or as provided for by contract or legal requirements in the country in which the data is collected and processed or according to document retention requirements.

VAM GMC may retain the documents which contain Private Data either in hard copies or/and in electronic copies. Hard copies are stored at the Controller's premises at Josy Welter House. 8-10, rue Genistre, L-1623 Luxembourg, Grand-Duchy of Luxembourg, the electronic copies are stored with Rcube Professional Services S.A VAM GMC's Cloud system provider.

After the required retention period, the documents which contain the Private Data will be destroyed by use of shredding machine according to the internal documents' destruction procedure. In the case of electronic files, VAM GMC will be supported by Rcube Professional Services S.A., which manages the Cloud systems for VAM GMC.

5.4. Surveillance at workplace

VAM GMC adopts surveillance means exclusively for the safety and security of VAM GMC itself, and not for the purpose of remote monitoring of the Employees, appropriate means such as signage, circulars, etc. shall inform the Data Subjects of the surveillance in place, in compliance with the applicable legal provisions.

5.5. Processing of online data

When processing personal information collected during visits to VAM GMC website, VAM GMC consistently observes the rules laid down in applicable data protection laws. An online Privacy Notice is available on VAM GMC website to explain the type of information collected when the public visit the website and outlines precisely how VAM GMC uses this information.

6. EMPLOYEES' DATA AND DATA OBTAINED FOR THE PURPOSE OF RECRUITMENT

The Employees are considered as Data Subjects and consequently benefit from the rights listed in section 4. of this Policy. In order to exercise their right, Employees should directly contact the DPRO. The Employees shall be exempted from the obligation to present a document to confirm their identity. The Data Controller is required to ask the Employees for consent if VAM GMC plans to process sensitive data, e.g. disability, ethnic origin, etc.

Candidate's data such as name, address, email address and employment history, is considered as Personal Data, and candidates shall be considered as Data Subjects. The Data Controller is entitled on the basis of legitimate interest to process candidate's data as long as it is job related information and only if the Data Controller intends to contact sourced candidates within 30 days. When sourcing candidates online, the Data Controller can only keep a candidate's data without informing them for 30 days, after which time the Data Controller must delete their data immediately.

The Data Controller is required to ask candidates for consent when processing sensitive data, e.g. disability, ethnic origin, etc.

The person in charge of recruitment who contacts the candidates shall provide the candidate with a relevant Privacy Notice describing his/her rights or provide the required information by other means and document it. This information should clearly state that the data will be used for recruitment purposes only and disclose for how long it will be held.

The candidates' Personal Data shall be deleted within one month after obtaining the information if the candidate has never been contacted, or after receiving the candidate's request to erase the data. Documents which contain the Personal Data of candidates obtained before 26th May, 2018, and which are no longer used for a purpose of a recruitment process, must be destroyed.

7. NOTIFICATION OF A PERSONAL DATA BREACH

In the case of a Personal Data breach, VAM GMC shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the Personal Data breach to the competent supervisory authority (the CNPD), unless the Personal Data breach is unlikely to result in a risk to the rights and freedoms of natural persons. VAM GMC shall notify the CNPD by using a relevant form published on the supervisory body's website. If the notification is not made within the above time, it shall be accompanied with justification of the delay.

VAM GMC establishes and maintains an up-to-date record of all Personal Data breaches accordingly in a Personal Data Breach Register (Appendix 2).

When the Personal Data breach is likely to result in a high risk to the rights and freedoms of natural persons, VAM GMC shall communicate the breach to the Data Subject without undue delay by using the Personal Data Breach Notification Form (Appendix 5). Notification to Data Subjects will not be required if:

a) VAM GMC used appropriate technical and organisational protection measures, like encryption, which render the Personal Data unintelligible to any person;
b) VAM GMC has taken subsequent measures which ensure that the high risk to the rights and freedoms of the Data Subject is no longer likely to materialise;
c) Notification would involve disproportionate effort. In such a case, VAM GMC shall instead make a public communication or similar measure to effectively inform the concerned Data Subjects.

8. UPDATE OF THIS POLICY

The DPRO is responsible for review and regular update of this Policy, e.g. after implementation of any new regulations or decisions regarding the Personal Data Protection.

9. TRAINING ON DATA PROTECTION RULES

The DPRO will ensure that appropriate training on the rules regarding the Processing of Personal Data and its Protection is implemented at VAM GMC.