Finare Asset Management S.A.
77 boulevard
Grande-Duchesse Charlotte
L-1331 Luxembourg

FINARE ASSET MANAGEMENT S.A.

Personal Data Protection Policy

Ref	Finare Asset Management S.A. ("the Company")
Name	**Data Protection Policy**
Version	1
Effective Date	01/07/2021
Amended Date	-
Approved by	Board of Directors
Next Review Date	Mid 2022
Status	In force

Finare Asset Management S.A.
77 boulevard
Grande-Duchesse Charlotte
L-1331 Luxembourg

Table of Contents

Definitions

The following definitions apply throughout this procedure:

- Finare Asset Management S.A. ("the **Company**")
- **Applicable Luxembourg Law** means the Luxembourg laws, regulations and CSSF Circulars listed in Regulatory Framework of the present procedure, referred to collectively as "applicable Luxembourg Law"
- The **Board** means the Board of Managers of the Company
- The **Board Members** means the Members of the Board of Managers/Directors of the Company
- The **Senior Management** means the Senior Management Committee of the Company
- The **Internal Control Functions**: Risk, Compliance and Internal Audit functions:
  - The Permanent Risk Management Function (PRMF)
  - The Compliance Function
  - The Internal Audit Function
- **AML/CFT** means anti-money laundering and combating financing of terrorism
- **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** means Commission for the Supervision of the Financial Sector
- **CNPD** means National Commission for Data Protection
- **Processing** means 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, organization, 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

Finare Asset Management S.A.
77 boulevard
Grande-Duchesse Charlotte
L-1331 Luxembourg

1. Introduction to the Company.

The Company is authorised under agreement 27/15 to manage following activities:

- Investment Advisor
- Broker on financial Instruments
- Commissioner
- Portfolio Manager
- Distributor of UCI shares
- Registrar Agent
- Family office

2. Purpose of the policy

This Personal Data Protection Policy ("Policy") defines how the Company processes personal data, in accordance with the General Data Protection Regulation ("GDPR").

This Policy focuses solely on the protection of personal data of physical persons, such as:

- Investors and potential investors
- Employees and secondees (herein after referred to collectively as "employees")
- Key decision makers at the Company and the funds it manages
- Representatives of service providers

This Policy applies to the Company and the funds it manages.

3. Regulatory framework

The applicable Laws and Regulations in the context of personal data protection include:

- 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, as amended (General Data Protection Regulation – "GDPR")

- Law of 1 August 2018 establishing the National Commission for Data Protection and implementing 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), amending the Labour Code and the amended Law of 25 March 2015 laying down the salary system and the conditions and procedures for the advancement of State officials
- Law of 1 August 2018 on the protection of individuals with regard to the processing of personal data in criminal matters and on national security
- The Penal Code, and in particular Articles 309 and 458 thereof
- Law of 5 April 1993 on the financial sector, and in particular Article 41 on obligation of professional secrecy
- Luxembourg Constitution, and in particular Article 28 thereof, on the secret status of letters
- Law of 11 August 1982 on the protection of privacy, art. 7 about correspondence and privacy.
- Employment code, including Article L.261-1 thereof, which lays down when surveillance may be performed
- Law of 29 March 2013 on the organisation of criminal records ("*casier judiciaire*") and on the exchange of information from criminal records between member states of the European Union
- Law of 23 July 2016, which modifies the Law of 29 March on the organisation of criminal records

4. Principles on data processing

Under the Company's Code of Conduct, the Company, all Members of the Board and employees, it manages commit to:

- Respect the general duty of confidentiality as a basic rule
- Respect personal data protection requirements
- Protect the information and data on its systems as well as any information and data transmitted to it
- Ensure that any processing of the information is carried out in a secure manner

- Keep records in accordance with the applicable Luxembourg Law

Professionals who leave the Company are required to respect the confidential or privileged nature of information they have had access to, even after they leave,without any time limit.

The Procedure manual, which includes the Code of Conduct, is signed for acceptance by every employee and director which means that a breach to the Code of Conduct is considered a fault in respect to professional obligations.

The Company commits to ensure that personal data:

- Remains confidential, e.g. accessible only to those whose mission requires access to the data
- Is processed in a way that ensures protection against unauthorized or unlawful processing, accidental loss, destruction or damage

5. Types of persons whose personal data may be collected ("datasubjects")

In the course of business, the Company will collect, record, store, adapt, transfer and otherwise process information by which physical persons may be directly or indirectly identified ("data subjects"). These persons may include, inter alia:

- Employees and secondees (herein after referred to collectively as "employees"), including members of Senior Management
- Candidate for positions at the Company
- Key decision makers at the Company and the funds it manages including the Members of the Board of the Company
- Clients (including fund investors) and potential Clients, their representatives, and beneficial owners and ultimate beneficial owners
- Representatives of service providers, and where relevant, beneficial owners and ultimate beneficial owners

Finare Asset Management S.A.
77 boulevard
Grande-Duchesse Charlotte
L-1331 Luxembourg

6. Types of personal data which may be collected

Personal data usually collected may include:

- Identification data (e.g. name, email, postal address, telephone number, country of residence, passport, identity card, driving licence, utility bills, tax identification number, extracts from public registers, electronic identification data (e.g. IP address, cookies, trafficdata))
- Personal status (e.g. gender, date of birth, marital status, children)
- Employment and occupation (e.g. employer, function, title, place of work, specialisation)
- Banking and financial data (e.g. financial identification, bank account details, source of funds and source of wealth, amount invested, financial situation, risk profile, risk appetite, investment objectives and preferences, investment experience)
- Health and medical-related data (e.g. medical condition, sickness certificates, handicaps…)
- Criminal records
- Publicly available information (newspaper articles, inclusion of official lists, etc)
- Tax-related data
- Contractual data, including any Power of Attorney
- Communications (e.g. exchange of letters and emails)
- Images and sound (e.g. copies of identification documents)
- Advertisement and sales data (e.g. potential interesting products for you)

7. Source of personal data

The Company normally receives data through its business relationship with the data subject. The Company receives the data either directly from the subject or through Funds and/or sub-funds that it manages, as well as their placement and distribution agents, investment managers and/or advisors, depositary banks, and central administration, registrar and transfer agents.

The Company may receive data from external sources, such as AML/CFT tools; such external sources must always comply with personal data protection requirements of their home jurisdiction. The Company may also require that such data is provided in compliance with applicable

Luxembourg Law.

In the case of nominees subscribing to a Fund managed by the Company on behalf of a physical person, the data may be collected by the nominee. In those cases, the nominee will be acting as independent data controller in accordance with the provisions of GDPR and/or the requirements of their home country. Investors subscribing to any of the Funds and/or sub-funds through a nominee should consult the data privacy notice of the nominee, when available.

8. Role of AIM: data controller or processor

The Company is the Data Controller in relation to all personal data it processes as well as in respect to any external service provider that processes personal data on the Company's behalf (e.g. Transfer Agent, payroll service provider).

The Company is not the Data Controller in respect to depositaries.

9. Personal data processing purpose

The Companymay only process personal data where:

- The data subject has given consent to the processing of his or her personal data for one or more specific purposes (written or oral declaration)
- 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
- Processing is necessary for compliance with a legal obligation to which the controller is subject
- Processing is necessary in order to protect the vital interests of the data subject or of another natural person
- 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
- Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party (e.g., marketing, anti-fraud, processing of the customers or employees data, processing security, etc.), 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

In general, the Company processing of personal data will be strictly limited to the context of the performance of its business unless the data subject has given his specific consent to its use for other purposes and where processing of personal data is based on consent. In such case, the subject has the right to withdraw his consent at any time.

The Company will always assure that personal data processing is limited to that which is necessary to achieve the purposes for which they are collected.

In respect to clients (such as fund investors), the Company and/or any of its delegates or service providers may process personal data, inter alia, for any one or more ofthe following purposes:

- To comply with any applicable legal, tax or regulatory obligations on the Company and its clients, including AML/CFT obligations
- For any other legitimate business interests

Clients, such as fund investors, are required to provide their personal data for statutory and contractual purposes. Failure to provide the required personal data or an objection to processing may result in the Company being unable to initiate or continueits relationship with the client.

The Company will always ensure that personal data are adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

10. Provision of information on data processing

The Company will always provide information to data subjects on how their personal data will be used and for which purpose.

This description may be made available to data subjects, *inter alia*:

- In the contract
- In a notice
- In the fund offering document

- In the subscription form
- In a disclosure on the website, where applicable

In certain situations, such as Board of Directors' meetings or other similar events, representatives of the Copany or a delegate may record certain conversations, for the following purposes:

- In order to document certain decisions, transactions or marketing communications
- To ease the process of drafting the minutes of such meetings

In such cases, the attendees are informed prior to the meeting and requested to provide consent for such recording.

Key disclosures to data subjects	
Type of data subject	**Place and type of disclosure**
Visitors to website	On the website: • General Personal Data Processing Statement • Cookie Policy • Personal Data Processing Statement for fund investors
Fund Investors	• In fund prospectuses: section on Personal Data Processing for fund investors • In the subscription form: General Personal Data ProcessingStatement • In the AML/CFT form: AML/CFT-specific Personal Data Processing Statement • On the website: Personal Data Processing Statement for fund investors
Direct clients	• In the Agreement: Personal Data Processing Statement for direct clients • In the AML/CFT form: AML/CFT-specific Personal Data Processing Statement • In case of recording of a call or conversation: oral request for authorisation to record the meeting; the consent may be recorded
Employees	• In the employment contract: a Personal Data Processing Clause • In the Data Processing Statement for employees • In this Personal Data Processing Policy
Delegates and other service providers	Either or both: • In the contract: Personal Data Processing Clause • In a separate statement: Personal Data Processing Statements The clause or statement may be calibrated as a function of the relevance of personal data to that service provider
Meeting participants	• In case of recording: oral request for authorisation to record the meeting; the consent may be recorded

11. Rights of data subjects

The Company fully respects the data subject's rights granted to them by the GDPR, including:

- The right of access:
  - The right to request confirmation 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
  - Where personal data are transferred to a third country or to an international organisation, the right to be informed of the appropriate safeguards relating to the transfer
- The right to rectification: if appropriate, a rectification of any personal data that is inaccurate
- The right to be forgotten: the right to request erasure of 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
- The right to restrict processing: the right to request restriction on 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 certain other cases accordingly
- The right to withdraw consent: the right to withdraw his/her consent at any time, if consent was the lawful ground for processing
- The right to object: the right to 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 legalclaims)
- Data portability: the right to 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)
- The right to complain either to the CNPD in Luxembourg or any other relevant data protection authority

12. Disclosure or transfer of personal data

The Company does not transfer personal data to third parties unless at least one of the following conditions is met:

- The transfer of personal data is 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
- The transfer of personal data is 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.
- The transfer of personal data is required by a 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

The Company and/or any of its delegates or service providers may disclose or transfer personal data to other delegates, duly appointed agents providers (and any of their respective related, associated or affiliated companies or sub-delegates) and to third parties including advisors, regulatory bodies, taxation authorities, auditors, technology providers for the purposes specified above situated either in the European Union/European Economic Area(EEA) or outside the European Union.

The Company and/or any of its delegates and service providers will not transfer personal data to a country outside of the EEA unless that country ensures an adequate level of data protection or appropriate safeguards are in place or the transfer is in reliance on one of the derogations provided by the GDPR. The European Commission has prepared a list of countries that are deemed to provide an adequate level of data protection which will be updated from time to time.

The Company, its Funds and/or any party lawfully related to them may, subject to all applicable laws, disclose to any Luxembourg or foreign governmental, regulatory or taxation authority or court, such information relating to data subjects as the Company or the Funds it manages reasonably determine. For the avoidance of doubt, this includes all information which in the reasonable

determination of the discloser, may be required to be disclosed to such authority, such Competent Authorities responsible for AML/CFT and disclosures pursuant to the Common Reporting Standard (CRS) as adopted by the OECD Council on 15 July 2014, as subsequently amended and implemented, and the US Foreign Account Tax Compliance Act (FATCA), as subsequently amended and implemented.

13. Appointment of service providers

Where processing is to be carried out by a service provider on behalf of the Company, the Company will only engage service providers whichcomply with the GDPR or equivalent requirements.

The Company will ensure that:

- Its contracts set out the service provider's specific mandatory obligations, including the processing of personal data only in accordance with the documented instructions from the Company and/or
- It obtains a Personal Data Processing Policy or Statement from the service provider settingout how the service provider processes personal data

The Company performs due diligence and oversight on all its service providers, including those that keep personal data on behalf of the Company. An important aspect of the due diligence on service providers is to ensure that they comply and are able to comply with the GDPR in respect to personal data and monitoring thatthey continue to comply.

14. Personal data protection measures

The Company implements appropriate administrative, technical, physicaland security measures to:

- Meet the legal requirements on data processing and any specific requirements in agreements in place
- Safeguard personal data against loss, theft and unauthorised access, use or modification
- Keep personal data accurate, complete and up-to-date
- Ensure that any service providers processing the data in its behalf apply adequate security and safeguard measures

- Ensure that the service providers have in place adequate organisational and technical measures which will allow the AIM to comply with the GDPR requirements

15. Personal data retention

General rule

The Company and/or any of its delegates or service providers will not keep personal data for longer than is necessary for the purpose(s) for which they were collected or to fulfil regulatory requirements.

In determining appropriate retention periods the Company and/or any of its delegates or service providers should take into account any applicable regulation, including anti-money laundering, counter-terrorism, and tax legislation.

The Company will:

- Take all reasonable steps to destroy or erase the data from its systems when they are no longer required for the purpose(s) for which they were collected or to fulfil regulatory requirements
- Ensure that its delegates and other service providers which process personal data take reasonable steps to destroy or erase the data from its systems when they are no longer required for the purpose(s) for which they were collected or to fulfil regulatory requirements

The Company may always keep data for a longer period if explicitly authorized by the Data Subject.

Applications for positions

If a candidate applies to a position with the Company and is not hired for the position, the Company may then keep his application and personal data for maximum 3 months after he was advised that his application is not accepted.

Criminal records

If the Company requests an extract of a criminal record, the retention of the criminal record depends on the scenario:

- In case of recruitment process or during the period of employment, the Company will not keep that extract for more than 1 month after it has been received
- In case of appointment of an employee to a new position, the Company will not keep that extract for more than 2 months after it has been received

Data retention register

The Company keeps a register with the dates on which such personal data have been requested and the dates they were destroyed.

16. Data Protection Officer

The Company does not have, and is not required to have, a Data Protection Officer (DPO) as defended under the GDPR for the following reasons:

- The Company' staff is under 150
- The Company does no process personal data on a large scale (directly or indirectly through external processors)

The Person responsible for Personal Data Protection is the Compliance Officer.

The Compliance Officer is responsible for all questions relating to Personal Data Processing and Protection.

17. Training on data protection

The Company will ensure that appropriate training is provided to staff onthe rules regarding the processing of personal data and its protection.

Finare Asset Management S.A.
77 boulevard
Grande-Duchesse Charlotte
L-1331 Luxembourg

18. Personal data processing register

The Company keeps a register of all personal data processing performedby itself or on its behalf.

The register includes, inter alia, information on:

- The processing purposes
- The initial business unit processing data (internal or delegate)
- The data source / data subjects
- The type of document
- The categories of personal data processed
- The categories of individuals involved in data processing (internal and delegate)
- The involvement of the Company in the data processing
- The department(s) of the Company accessing this data
- Other recipients of the data
- Whether the data is related to the main activity of the company
- Whether the data is sensitive data
- The legal basis for processing the data
- Whether there is international transfer of the data and, if so, whether adequate protection measures are in place for international transfers and description of these measures
- The data retention period
- The personal data protection risk level

19. Employee private data

The Company expects its employees to use its systems and communications channels for the purposes of conducting the Company's business, unless otherwise agreed with the employee by contract.

The Company understands that there may nevertheless be occasions when employees may need to use its systems and communications channels for private personal reasons. This may include, for example, private telephone conversations and emails.

The Company expects its employees to:

- Keep private use of the Company's systems, communications channels and premises to a strict minimum
- Clearly segregate any private communications or documentation from professional communications (e.g. by marking them as "Private")

The Company does not:

- Access the private communications of employees through or on its systems or in its premises without the consent of the employee
- Monitor employees through surveillance systems without informing them in advance and receiving prior written consent of the employee

20. Reporting of breaches

Personal data breaches will be reported to the relevant national supervisory authority, such as the CNPD in Luxembourg and to the data subject where required.