FARAD INVESTMENT MANAGEMENT
INDEPENDENT PORTFOLIO MANAGEMENT & SUSTAINABLE INVESTMENTS

DATA PROTECTION POLICY

Enter into effect last version:	13/09/2023
Approval by FARAD I.M. Executive Committee:	06/09/2023
Approval by FARAD I.M. Board of directors:	13/09/2023
Line Managers or departments involved	ALL Employees
Legal requirements	In preparing this Policy, FARAD I.M. has endeavored to align its procedures with the relevant legal requirements and current best practice. In particular, this Policy is designed to satisfy the requirements of: - Law of 2 August 2002, as amended; -Regulation (EU) 2016/679 related to the protection of natural persons with regard to the processing of personal data ("GDPR").
Aim and application	The purpose of the Policy is to enable FARAD I.M. to comply with the law in respect of the data it holds about individuals, follow good practice, protect employees and protect FARAD I.M. from the consequences of a breach of its responsibilities.
Updating / Review	In the following cases: - Change of applicable legislation; - Any new legal requirement; Any other change that would have an impact on the Policy.
Communication to the CSSF	Upon request of the CSSF

TABLE OF CONTENTS

Glossary

Consent: 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;

Data subject: an identified or identifiable natural person;

Personal data breach: means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

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 breach: means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

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;

Processor: means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

Profiling: means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;

Pseudonymisation: means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;

Third party: means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

I. Introduction to the applicable legislation

FARAD I.M. has the obligation to follow the requirements of the Law of 2 August 2002 on the Protection of Persons with regard to the Processing of Personal Data, as amended by the GDPR.

The purpose of GDPR and the Law of 2 August 2002, is to protect the fundamental rights and freedoms of natural persons, particularly their private lives, as regards the processing of personal data.

II. Scope of application and purpose of the policy

The Policy applies to the processing of personal data, within FARAD I.M. (acting as controller), wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system of FARAD I.M.

This Policy applies to the processing of personal data in the context of the activities of FARAD I.M. in the Union, regardless of whether the processing takes place in the Union or not.

The purpose of the Policy is to enable FARAD I.M. to comply with the law in respect of the data it holds about individuals, follow good practice, protect employees and protect FARAD I.M. from the consequences of a breach of its responsibilities.

III. Failure to comply with this Policy (and, therefore, the applicable legislation) could result in compensation claims against the Company (and disciplinary proceedings against employees of the Company). General policy

FARAD I.M. and its employees use and process personal data carefully and confidentially. Information must not be given out inappropriately or be able to be accessed by unauthorized individuals or organisations.

3.1. Principle relating to processing of personal data

3.1.1 General principle

FARAD I.M. have measures in place to comply with the following principles related to the processing of personal data:

1. Personal data must be processed fairly, lawfully, in a transparent manner in relation to the data subject and only for one or more specified and lawful purposes. In particular, the processing is considered lawful only and to the extent that at least one of the below items applies. Therefore FARAD I.M. ensures:
    - To receive the consent from the data subject to the processing of his or her personal data for one or more specific purposes; or
    - That the 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
    - That the processing is for compliance with a legal obligation to which FARAD I.M. is subject; or
    - That the processing is necessary in order to protect the vital interests of the data subject or of another natural person; or

- That the processing is necessary for the purposes of the legitimate interests pursued by FARAD I.M. or by a third party.

2. Personal data process is accurate, adequate, relevant, up to date and not excessive in relation to the purpose for which data are collected and/or further processed. In particular, FARAD I.M.ensures:

    a. That personal data are collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes is not considered to be incompatible with the initial purposes ('purpose limitation');
    b. That personal data are adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');
    c. That personal data are accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');
3. Personal data must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected and processed. FARAD I.M. identifies the adequate period of time to store the personal data in light with other specific legislation applicable to FARAD I.M. of one its entity such as anti-money laundering and fight against financial terrorism laws and regulations.

Processing frameworks have to inherently protect the data when they are designed. Technical and organizational measures must be put in place to ensure that processing of personal data is limited by default to the specific purpose for which data is processed.

3.1.2 Process of specific personal data

FARAD I.M. does not process personal data revealing racial or 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, unless necessary and in accordance with article 9 of GDPR.

FARAD I.M. processes personal data relating to criminal convictions and offences or related security measures based on article 6(1) of GDPR only under the control of official authority or when the processing is authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects.

3.2 Obligation of FARAD I.M.

3.2.1 Rights of data subject and FARAD I.M.'s correlated obligations

Each time FARAD I.M. or its employees is collecting personal data of a data subject, either electronically or physically in order to electronically process the information it provides the data subject with the following information contact details of FARAD I.M. or its employees, the contact details of the data protection officer , the purpose of the processing, the legal basis for the processing , the legitimate interest (when applicable), the storage period, existence of the right the right attached to the personal data including right to lodge a complaint, whether the provision of personal data is a statutory or contractual requirement or a requirement necessary to enter into a contract and possible consequences.

When the legal basis to process personal data is the consent of the data subject, FARAD I.M. or its employees receive the prior written consent of the individual. Prior to give its consent, the data subject is informed that, at any time, it has the right to withdraw its consent. The consent of the individual is requested in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain languages. Furthermore, the data subject is informed of its rights in relation to its personal data as described in the present section.

When assessing whether consent is freely given, particular attention is given, on whether the performance of a contract, including the provision of a service, is conditional to the consent to the processing of personal data that is not necessary for the performance of that contract.

In addition and in relation to the principle mentioned in section 3.1, FARAD I.M. puts in place adequate measures in order to comply with the following obligation:

- Transparent information and communication:
    - Provide information and communication related to the data subject on the processing of personal data which is transparent, concise, easy to understand, clear, in a plain language, free of charge and easily accessible;
    - Inform the data subject that at any time it has the right to withdraw its consent;
    - Inform the data subject on the purpose follow in the collection of its personal data (limited purpose);
    - Inform the data subject about its rights when its personal data are collected in accordance with GDPR and in particular Chapter III "Rights of the data subject" of the latter.
    - Inform in due time the data subject and the CNPD each time FARAD I.M. is subject to a data breach,
    - Inform the Data subject clearly and separately from other information, at the latest at the time of the first communication with the Data subject, of the right to object 1) on the processing of its Personal Data where such Personal data are processed for direct marketing which includes profiling to the extent that it is related to such direct marketing or 2) on grounds relating to his or her particular situation where the Processing is based on the legitimate interests pursued by FARAD I.M. or by a third party.

- Free access:
    - On request, the data subject may obtain confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the related information in accordance with article 15 of GDPR;
    - Provide a copy of the personal data undergoing processing to the data subject. For any further copies requested by the data subject, FARAD I.M. may charge a reasonable fee based on administrative costs. Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information is provided in a commonly used electronic form.

- Rectification & Erasure:
    - On request or when the personal data are no longer necessary (without any request),

personal data must be erased, without any undue delay;

- Provide access to data subject on its personal data and make rectification;
- Data subject have the right to have incomplete personal data completed, including by means of providing a supplementary statement;
- Erase personal data without undue delay where one of the following grounds applies:
  - the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
  - the data subject withdraws consent on which the processing is based and where there is no other legal ground for the processing;
  - the data subject objects to the processing subject to automatic decision and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to automatic decision;
  - the personal data have been unlawfully processed;
  - the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject.

- Portability:
  - Transfer of personal data is permitted without any possibility for FARAD I.M. to interfere;
  - This transfer must be done through a structured manner.

- Not be subject to automatic decision:

  Restriction of processing

  Restrict processing of personal data collected by FARAD I.M. in the following case:

  - The Data subject has not given its consent to automated processing. Data subject may require to not be subject to a decision based solely on automated processing, including profiling which affect significantly or produce legal effect to the Data subject, unless it is necessary for entering into, or performance of, a contract between the Data subject and FARAD I.M.
  - Upon request of the Data subject, FARAD I.M. may restrict the processing of the Personal Data of the Data Subject when one of the following applies:
    - The accuracy of the Personal data collected by FARAD I.M. is contested by the Data Subject for a period sufficient to enable FARAD I.M. to verify the accuracy of the personal data;
    - The processing is unlawful and the Data subject opposes the erasure of the Personal data and requests the restriction of their use instead;
    - FARAD I.M. no longer needs the Personal Data of the Data subject for the purposes of the processing, but they are required by the Data Subject for the establishment, exercise or defence of legal claims;
    - The Data subject has objected the processing pursuant to article 21(1) of GDPR and the verification on whether the legitimate grounds of FARAD I.M. override those of the Data subject is pending.

Where processing has been restricted under the above paragraph, such personal data , with the exception of storage, is only processed with the data subject's consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest of the European Union or a member state of the latter.

A data subject who has obtained restriction of processing pursuant to paragraph 1 is informed by the data controller before the restriction of processing is lifted.

- The Data subject has informed FARAD I.M. of its objection on grounds relating to his or her particular situation, at any time in the processing of Personal Data concerning him or her which is based on the legitimate interests pursued by FARAD I.M. or by a third party, including profiling based on those provisions and FARAD I.M. cannot demonstrate compelling legitimate grounds for the processing which override the interests, rights and freedoms of the Data subject or for the establishment, exercise or defence of legal claims.
- The Data subject has informed FARAD I.M. of its objection on the processing of Personal data where such Personal data are processed for direct marketing which includes profiling to the extent that it is related to such direct marketing. In this case, Personal data is no longer be processed for such direct marketing.

Respect of these rights is not in opposition with the legal obligations of FARAD I.M. (e.g. retention of information).

3.2.2 Relation between FARAD I.M. and other controller or processors

Each time FARAD I.M. enters in a contract or any other legal act with a client, third party, delegate or service providers, FARAD I.M. identifies whether the latter party act as controller or processor and specify its related obligations.

Where processing is to be carried out on behalf of FARAD I.M., FARAD I.M. uses only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of GDPR and ensure the protection of the rights of the data subject.

FARAD I.M. does not authorize the processor to engage itself with another processor without prior specific or general written authorisation of FARAD I.M. In case of general written authorisation, the processor informs FARAD I.M. of any intended changes concerning the addition or replacement of other processors, thereby giving FARAD I.M. the opportunity to object to such changes.

FARAD I.M. governs the processing by a processor by including within the contract or other legal with the concerned processor:

- the subject-matter and duration of the processing;
- the nature and purpose of the processing;
- the type of personal data and categories of data subjects, and
- the obligations and rights of the controller.

Furthermore, the contract or legal act provides, in particular, that the processor:

- processes the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by Union or Member State law to which the processor is subject; in

such a case, the processor informs the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest;

- ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;
- takes all measures related to security of processing in accordance with article 32 of GDPR;
- taking into account the nature of the processing, assists FARAD I.M. by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of FARAD I.M.'s obligation to respond to requests for exercising the data subject's rights laid down in Chapter III of GDPR;
- assists FARAD I.M. in ensuring compliance with the obligations related to security of processing pursuant to security of processing, Data protection impact assessment and prior consultation (articles 32 to 36 of GDPR) taking into account the nature of processing and the information available to the processor;
- at the choice of FARAD I.M., deletes or returns all the personal data to FARAD I.M. after the end of the provision of services relating to processing, and deletes existing copies unless other applicable laws to FARAD I.M. require storage of the personal data;
- makes available to FARAD I.M. all information necessary to demonstrate compliance with the obligations laid down in GDPR and contributes to audits, including inspections, conducted by FARAD I.M. or another auditor mandated by FARAD I.M.

3.2.3. Relation between FARAD I.M. and the competent authority

FARAD I.M. and, where applicable, their representatives, cooperate, on request, with the supervisory authority in the performance of its tasks under GDPR.

In case of personal data breach, FARAD I.M. will notify the CNPD within a 72 hours' time slot, meaning that FARAD I.M. has the necessary procedure to alert, investigate, detect, and solve the breach.

The notification to the CNPD includes the following information:

- description of the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
- communication of the name and contact details of contact point where more information can be obtained;
- description of the potential consequences of the personal data breach;
- description of the measures taken or proposed to be taken by FARAD I.M. to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Where, and in so far as, it is not possible to provide the aforementioned information at the same time, the information may be provided in phases without undue further delay.

The employees of FARAD I.M. in charge of the aforementioned notification document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken.

Communication to the Data subject

Where the breach of personal data is likely to create a high risk for the rights and freedoms of a natural person, FARAD I.M. when acting as controller communicates the Personal data breach to the data subject without undue delay.

The communication to the Data subject describe, in clear and plain language, the nature of the Personal data breach and contains at least:

1. the name and contact details of the data protection officer or data protection person of contact from whom additional information can be obtained;
2. a description of the likely consequences of the personal data breach;
3. a description of the measures taken or proposed by the controller to remedy the breach of personal data, including, where appropriate, measures to mitigate any negative consequences.

The communication to the Data subject is not required if any of the following conditions are met:

- FARAD I.M. has implemented appropriate technical and organisational protection measures, and those measures were applied to the Personal data affected by the Personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;
- FARAD I.M. has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred is no longer likely to materialise;
- it would involve disproportionate effort. In such a case, FARAD I.M. instead makes a public communication or similar measure whereby the Data subjects are informed in an equally effective manner.

The CNPD having considered the likelihood of the personal data breach resulting in a high risk, may require FARAD I.M. to communicate the Personal data breach to the Data subject in the event such communication has not been made.

3.2.4. Transfer of personal data

In the case of data transfer, FARAD I.M. recommends to its employees the use of any means enabling protection of data (scrambling, pseudonymization and encryption).

In the event, FARAD I.M. has to transfer personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation, FARAD I.M. refers to and apply the provisions set out in the Chapter V of GDPR.

3.3. FARAD I.M. privacy framework

FARAD I.M.'s data privacy framework isbuilt according to technical and organizational measures in order to protect the interest of the data subject.

- Safeguard measures: FARAD I.M. and its employees have to ensure that the determination of the means for processing of personal data, includes 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. The measures take into account the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures

ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.

IV. Security of processing operations

4.1 Security

Given the size, organisation, cost of implementation and activity of FARAD I.M. implements appropriate technical and organisational measures, when applicable, to ensure a level of security appropriate to the risk, including when appropriate:

- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
- a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

In assessing the appropriate level of security, FARAD I.M. takes in particular account of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed. This section of the Policy only addresses security issues relating to personal data. It does not cover security of the building, business continuity or any other aspects of security.

FARAD I.M. takes steps to ensure that its employees having access to personal data do not process them except on instruction of FARAD I.M. or required by applicable laws and regulation.

Examples of situations where potential data protection breaches could occur include:

- Employees misusing personal information in their possession;
- Ex-employees being sent information after they have stopped working for the Company;
- Personal passwords being provided to non-authorized users; and
- Giving away information to third parties about colleagues or clients over the phone.

4.2 Mitigation of data breach

FARAD I.M. has implemented security measures designed to mitigate data protection breaches via a secure computer system where access to information is controlled by function, password protection policies, a clear desk policy and entry control policies.

- Employees must adhere to the following:
    - To keep information secure, computer screens must be locked at all times, when not in use;
    - Personal passwords must not be given to anybody else;
    - Approval must be sought before creating a database holding personal client information; and
    - Information must not be released to other group companies or to any other third party without consideration of who is making the request and reasons for the request. Approval should be sought from Team Managers, Client Directors and / or the Data Protection Officer, as appropriate.

Any creation of a filling system (a structured set of personal data which are accessible according to specific criteria) is subject of a prior request to the Data Protection contact person of each Company of FARAD I.M. Employees must apply the appropriate measure to protect this filling system.

FARAD I.M. ensures that all employees familiarise themselves with the security measures in place at FARAD I.M. to prevent data protection breaches.

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, the controller , prior to the processing, carries 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.

4.3 Confidentiality

Confidentiality forms part of our agreement with clients to whom we have a duty of care to keep information confidential and only disclose it in certain limited circumstances, such as under due process of law or as part of a regulatory requirement. Personal data must not be transferred to an external party without the consent of the subject, except if mandatory by law.

- Employees must consider the following:
    - The content of email correspondence and who may be party to that information (particularly in the event that the email is misdirected);
    - The shredding of confidential waste where appropriate;
    - The appropriateness of using of the Company or client Headed Paper when sending out correspondence;
    - The content of answering machine messages;
    - The usage of fax header sheets; and
    - Authenticating customer identity before carrying out customer instructions.

Where anyone within FARAD I.M. considers that it would be appropriate to disclose personal or confidential information in a way contrary to the confidentiality policy, or where an official disclosure request is received, this must only be done with the authorization of the Managing Director. All such disclosures will be documented.

4.3.1. Data Recording, Storage and Disposal

FARAD I.M. implements adequate measures in order to ensure that:

- All personal data captured at FARAD I.M. is recorded and stored on secure servers.
- All personal data are stored for a period that is justified by business reasons and in compliance with GDPR and other relevant legislation as the case may be (including paper and electronic records).
- After the retention period has expired, when applicable, all confidential documentation must be called back from storage (if applicable), reviewed for content, confirmed for destruction and shredded before being disposed of.
- The destruction of any confidential or other documentation in relation to regulated (or client related) business or transactions (including where transactions or business does not take place or proceed) can only take place with “four-eyes” oversight, including line management or above approval.

- Confidential information on Investors and originals that would be difficult to obtain again (such as well-informed investor forms) are kept in a safe under the direct control of the Management.
- Customer Due Diligence files are kept in a secure storage area under the direct control of the Management.