IRE AIFM

IRE AIFM HUB

General data protection policy

UPDATE

April 2020

Policy Owner	David Luksenburg (responsible conducting officer)
Policy Approver	Board of managers

Date of issue	**Version**	**Name**	**Title**
April 2020	1	David Luksenburg	Conducting officer

1. Introduction

This documents purports to fulfill the requirements ("the Requirements") of the rules laid down in:

- 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 ("GDPR").

2. Purpose

Within IRE AIFM HUB (the "AIFM"), all employees are expected to handle information with care. In particular, the security and confidentiality of all proprietary information and data processing, including personal confidential information, must be safeguarded in accordance with applicable laws and regulations.

In conformity with the Requirements, the purpose of this general data protection policy (the "GDP Policy") is to ensure that a comprehensive and documented GDP process specific is implemented at the level of the AIFM in order to manage the collection and processing of personal information on individuals within the context of the AIFM's activities and operational functions.

The aim of the present GDP Policy is to address the following items:

- Being transparent in what AIFM does with personal data of clients, suppliers, employees and business partners.
- Only processing personal data for specific business purposes.
- Only using sensitive data if necessary and where legally allowed.
- Making sure that personal data are up-to-date, complete and accurate.
- Informing clients, suppliers, employees and business partners about the purposes for which their personal data; are processed
- Allowing clients, suppliers, employees and business partners to obtain an overview of their personal data.
- Allowing clients, suppliers, employees and business partners to correct, delete or block their personal data.
- Protecting the personal data from unauthorized loss, alteration, disclosure or access.
- Only disclosing personal data to third parties in accordance with this GDP Policy.

3. Definitions

- **Personal data**: information, including facts and opinions, that identifies a natural person (individual) and is information which has a duty of confidence. This includes (but is not limited to):
    - Name;
    - Date of birth;

    - Post code;
    - Address (postal, email);
    - Phone numbers;
    - National insurance number;
    - Photographs, digital images etc.
    - Bank account numbers and details;
- **Sensitive personal data**: certain categories of information are classified as sensitive personal data and additional safeguards are necessary when sharing or disclosing this information in line with guidance and legislation. This includes (but is not limited to):
    - Physical and mental health or condition;
    - Social care;
    - Ethnicity and race;
    - Sexuality;
    - Trade union membership;
    - Political affiliations;
    - Religion or other beliefs;
    - Records relating to criminal charges and offences;
    - Genetic data;
    - Biometric data where processed to uniquely identify a person;
- **Processing**: the collective term for any action taken relating to personal or sensitive personal data, including obtaining, recording, storing, using, disclosing and destroying data.
- **Data subject**: the individual identified by the personal data collected.
- **Data controller**: the organisation that determines the need to collect personal data and the uses to which it will be put. The AIFM including its different internal functions is a data controller.
- **Third party**: any external person or organisation that is neither the data subject nor the data controller.
- **Non-Adequate Country:** shall mean a country that under applicable local law is deemed not to provide an "adequate" level of data protection (especially outside European Union).

4. Corporate governance and responsibilities

Everyone who works for or with the AIFM has some responsibility for ensuring data is stored, collected and handled appropriately.

Each staff member that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

Moreover, the below people have key areas of responsibility:

- The AIFM's board of managers (the "Board") is ultimately responsible for the implementation of the present GDP Policy, the approval of its periodical amendments, as well as ensuring that the AIFM meets its legal obligations.

- Mr Michel Batter, acting as data protection officer (the "Data Protection Officer") is responsible for:
    - Keeping the Board updated about data protection responsibilities, risks and issues;
    - Reviewing the GDP Policy, at least on an annual basis;
    - Ensuring all systems, services and equipment used for storing data meet acceptable security standards;
    - Arranging data protection training and advice for the people covered by this policy;
    - Handling data protection questions from staff and anyone else covered by this policy;
    - Dealing with requests from individuals to see the data that the AIFM holds about them (also called 'subject access requests');
    - Review of contracts or agreements with third parties that may handle the AIFM's sensitive data;
    - Approving any data protection statements attached to communications such as emails and letters.
- The AIFM's IT service provider:
    - Responsible to provide with the AIFM with services and equipment for storing and transferring electronical data and meeting acceptable security standards;
    - Performing regular checks and scans to ensure that security hardware and software is functioning properly.

5. Purpose for processing personal data

5.1 Legitimate business purpose

Personal Data shall be collected, used, stored or otherwise processed if necessary:

- within the framework of responsible, efficient and effective business management, specifically for the following activities:
    - Performing agreements assessing and accepting clients, entering into and executing of
      agreements with clients, business partners and suppliers as well as carrying out payment transfers and other financial transactions and recording and financially settling delivered services, products and materials to and from AIFL, including communication
      with individuals and other parties involved in contracts (beneficiaries, intermediaries) and responding to requests for (further) information from clients, business partners or suppliers, dispute resolution and litigation.
    - Relationship management and marketing for commercial activities including processing necessary for the development and improvement of AIFM services, client service and the performance of (targeted) marketing activities in order to establish a

relationship with a client and/or maintaining as well as extending a relationship with a client, business partner or supplier.
- Investment management activities of the AIFM in connection with the Annex IV of the Law of 12 July 2013 on alternative investment fund managers (portfolio management, risk management, administration or marketing activities).
- Compliance with legal obligations: this addresses the processing of personal data as necessary for compliance with laws, regulations and sector specific guidelines to which the AIFM is subject.

- to support the activities to safeguard and ensure the security and integrity of AIFM and/or the financial sector, including the following activities:
  - the identification, prevention and investigation of activities that may have a negative effect on AIFM, including but not limited to:
    - (attempted) criminal or otherwise negative conduct;
    - violations of (legal) regulations;
    - defending, preventing and tracing (attempted) (criminal or undesirable) conduct targeted towards the financial sector, AIFM, its clients and staff.
    - compliance with legal requirements, such as anti-money laundering and anti-terrorist financing regulations.

Where there is a question whether a processing of personal data is for one of the business purposes listed above, it is necessary to seek the advice of the appropriate Data Protection Officer before the processing takes place.

5.2 Individual consent

If a business purpose does not exist or if applicable local law so requires, the AIFM shall only process personal data with the individual's consent. If a business purpose does not exist and a specific processing is undertaken at the request of an individual, he is deemed to have provided consent to the relevant processing.

The individual shall be made aware of:

- The purposes of the processing for which consent is requested or shall be deemed to have been provided.
- Other relevant information necessary for the individual to make a conscious decision about the processing of his personal data (e.g. the nature of and categories of the processed data, the categories of third parties to which the data are disclosed (if any and how individuals can exercise their rights).

5.3 Denial or withdrawal of consent

The individual may both deny consent and withdraw consent at any time.

5.4 Limitations on processing data of dependants of individuals

The AIFM will process data of dependants (spouse, partner or child belonging to the household of the individual) of an individual if:

- The data were provided with the consent of the individual or the dependant; or
- Processing of the data is reasonably necessary for the performance of a contract with the individual; or
- The processing is required or permitted by applicable law and regulations.

6. Use for other purpose

6.1 Use of data for secondary purposes

Generally, personal data shall be used only for the purposes for which they were originally collected. Personal data may be processed for legitimate purposes of the AIFM different from the original purpose only if the original purpose and secondary purpose are closely related and only if use of data for secondary purposes is allowed under applicable law. Depending on the sensitivity of the relevant personal data and whether use of the data for the secondary purpose has potential negative consequences for the individual, the secondary use may require one or more additional measures such as:

- Limiting access to the data;
- Imposing additional confidentiality requirements;
- Taking additional security measures;
- Informing the individual about the secondary purpose.
- Providing an opt-out opportunity;
- Obtaining individual consent in accordance if required under applicable law.

6.2 Generally permitted uses of data for secondary purposes

It is generally permissible to use personal data for the following secondary purposes provided that appropriate additional measures are taken as described above:

- Transfer of the data to an archive; or
- Internal audits or investigations; or
- Implementation of business controls; or
- Statistical, historical or scientific research; or
- Dispute resolution or litigation; or
- Legal or business consulting or
- Insurance purposes.

6.3 Data Protection Officer advice

Before processing personal data for a secondary purpose, AIFM's staff members shall seek the advice of the Data Protection Officer.

7. Processing sensitive data

7.1 Specific purposes for processing sensitive data

The AIFM will process data only to the extent necessary to serve the applicable legitimate purposes.

The following categories of sensitive data may be collected, used or otherwise processed for one (or more) of the purposes specified below:

- Racial or ethnic data: the AIFM may process such information about individuals (i) for inclusion in client, supplier or business partner directories and (ii) for site access and security reasons and (iii) to comply with legal obligations (e.g. performing client due diligence screenings).
- Physical or mental health data; for assessing and accepting clients, entering into and executing an agreement with a client and for carrying out payment transfers and other financial transactions.
- Criminal data (including data relating to criminal behaviour, criminal records or proceedings regarding criminal or unlawful behaviour); for protecting the interests of the AIFM with respect to criminal offences that have been or, given the relevant circumstances are suspected to be, committed against AIFM or its employees.
- Social security numbers (or other identifying numbers, including passports numbers): for complying with legal obligations e.g. on client identification and authentication.

7.2 General purposes for processing of sensitive data

All categories of sensitive data may be processed only under (one or more of) the following:

- The individual has given his explicit consent to the processing thereof.
- As required by or allowed under applicable local law.
- For the establishment, exercise or defence of a legal claim.
- To protect a vital interest of an individual, but only where it is impossible to obtain the level of information;
- To the extent necessary to comply with an obligation of international public law (e.g. treaties).
- If the sensitive data have manifestly been made public by the individual.

7.3 Prior authorization of Data Protection Officer

Where sensitive data are processed based on a requirement of law other than the local law applicable to the Processing, or based on the consent of the individual, the processing requires the prior authorization of the appropriate Data Protection Officer.

8. Quantity and quality of data

8.1 No excessive data

The AIFM shall restrict the processing of personal data to those data that are reasonably adequate for and relevant to the applicable legitimate purposes. The AIFM shall take reasonable steps to securely delete personal data that are not required for these legitimate purposes.

8.2 Storage period

ING generally shall retain personal data only:

- For the period required to serve the legitimate purposes for which the personal data are processed; or
- To the extent reasonably necessary to comply with an applicable legal requirement; or
- As advisable in light of an applicable statute of limitations.

The AIFM may specify (e.g., in a minimum standard, notice or records retention schedule) a time period for which certain categories of personal data may be kept. Among others, all personal data processed with regards to any business agreement entered into by the AIFM will be kept for at least five years after the end of the business relationship.

Promptly after the applicable storage period has ended, the Data Protection Officer shall instruct that the Data to be:

- Securely deleted or destroyed: data printouts should be shredded and disposed of securely when no longer required.
- Anonymized; or
- Transferred to an archive (unless this is prohibited by law or an applicable records retention schedule).

8.3 Quality of data

Personal Data should be accurate, complete and kept up-to-date to the extent reasonably necessary for the applicable legitimate purposes for which the personal data are processed.

8.4 Accurate, complete and up-to-date data

It is the responsibility of the AIFM to keep the personal data of individuals accurate, complete and up-to-date. It is the responsibility of individuals to inform the AIFM regarding any changes to their Personal Data.

9. Individual information requirements

9.1 Information requirements

The AIFM shall inform Individuals through a data protection policy or notice about:

- The business purposes for which their data are processed.
- Other relevant information (e.g., the nature and categories of the processed data, the categories of third parties to which the data are disclosed (if any) and how Individuals can exercise their rights).

These information requirements are part of the legal wording of arrangements entered into by AIFM, with client, suppliers, business partners, employees and third parties.

9.2 Personal data not obtained from the individual

If applicable local law so requires, where personal data have not been obtained directly from the individual, the AIFM shall provide the individual with the information as set out in section 9.1:

- At the time that the personal data are recorded in an AIFM database; or

At the time that the personal data are used for a mailing, provided that this mailing is done within six months after the personal data are recorded in an AIFM database.

9.3 Exceptions

The requirements of section 9.2 may be set aside if:

- It is impossible or would involve a disproportionate effort to provide the information to individuals; or
- It results in disproportionate costs.

10. Individual rights of access, rectification and deletion

10.1 Rights of individuals

Every individual has the right to request an overview of his personal data processed by or on behalf of the AIFM. Where reasonably possible, the overview shall contain information regarding the source, type, purpose and categories of recipients of the relevant personal data. If the personal data are incorrect, incomplete or not processed in compliance with applicable law or this Policy, the individual has the right to have his data rectified, deleted or blocked (asappropriate). In addition, the individual has the right to object to the processing of his data on the basis of compelling grounds related to his particular situation.

10.2 Procedure

The individual should send his request to the contact person or contact point indicated in a potential relevant privacy statement. If no contact person or contact point is indicated, the individual may send his request to the AIFM using the contact details indicated in the general contact section of the local AIFM website.

Prior to fulfilling the request of the individual, the AIFM may require the individual to:

- Specify the type of personal data to which he is seeking access.
- Specify, to the extent reasonably possible, the data system in which the data likely are stored.
- Specify the circumstances in which the AIFM obtained the personal data; and
- Show proof of his identity; and
- In the case of a request for rectification, deletion, or blockage, specify the reasons why the personal data are incorrect, incomplete or not processed in accordance with applicable law or this policy.

10.3 Response period

Within four weeks of AIFM receiving the request, the Data Protection Officer or any other responsible function indicated in the relevant local complaints procedures shall inform the individual in writing either (i) of AIFM's position with regard to the request and any action the AIFM has taken or will take in response or (ii) the ultimate date on which he will be informed of AIFM's position, which date shall be no later than eight weeks thereafter.

10.4 Complaint

An individual may file a complaint if:

- The response to the request is unsatisfactory to the Individual (e.g. the request is denied); or
- The individual has not received a response; or
- The time period provided to the individual is, in light of the relevant circumstances, unreasonably long and the Individual has objected but has not been provided with a shorter, more reasonable time period in which he will receive a response.

10.5 Denial of requests

The AIFM may deny a request of an individual if:

- the request does not meet the requirements of sections 10.1 and 10.2;
- The request is not sufficiently specific.

- The identity of the relevant Individual cannot be established by reasonable means; or
- The request is made within an unreasonable time interval of a prior request or otherwise
  constitutes an abuse of rights. A time interval between requests of 6 months or less shall generally be deemed to be an unreasonable time interval.
- The request entails a blockage or deletion and the processing of the personal data is required by law.

11. Security and confidentiality requirements

11.1 Data security

The AIFM shall take appropriate commercially reasonable technical, physical and organizational
measures to protect personal data from misuse or accidental, unlawful, or unauthorized destruction, loss, alteration, disclosure, acquisition or access. To achieve this purpose, the AIFM has implemented the following:

- All print out personal data are kept in a locked filing cabinet;
- Employees should make sure paper and printouts are not left where unauthorised people could see them, like on a desk or printer.

- Electronical personal data should only be stored on designated physical server locked in a separate IT rack.
- Data are backed up (and encrypted) frequently, those backups should being tested on a monthly basis, in line with the AIFM's standard backup procedures.
- Personal data should never be saved directly to laptops or other mobile devices like tablets or
  smart phones;
- All servers and computers containing data should be protected by approved security software and a firewall;
- All emails exchanging personal data are encrypted (mail flow using TLS encryption during transmission);

11.2 Staff access

Staff members shall be authorized to access personal data only to the extent necessary to serve the applicable legitimate purposes for which the data are processed by the AIFM and to
perform their job.

Staff members who access personal data are subject to professional secrecy and confidentiality obligations.

12. Transfer of personal data to third parties

12.1 Transfer of personal data

The AIFM shall transfer personal data to a third party to the extent necessary to serve the applicable legitimate purposes for which the personal data are processed.

12.2 Third party contracts

Third party (other than government agencies or other public bodies) may process personal data only if they have a written contract or a commitment in a similar form (e.g. electronic) with AIFM. In the contract, the AIFM shall seek to contractually protect the data protection interests of the Individuals. All such contracts shall be drafted in consultation with or in accordance with guidelines provided by the appropriate Data Protection Officer. Individual business contact data may be transferred to a third party without a contract if it is reasonably expected that such business contact data will be used by the third party to contact the individual for legitimate business purposes related to the individual's job responsibilities with the relevant AIFM’s client, supplier or business partner.

12.3 Third party processor contracts

Third party processors may process personal data only if they have a written contract or a commitment in a similar form (e.g. electronic) with AIFM. Contracts with a third party processor who will handle personal data must include the following provisions:

- The processor shall process personal data only in accordance with AIFM's instructions and for the purposes authorized by the AIFM; and
- The processor shall keep the personal data confidential; and
- The processor shall take appropriate technical, physical and organizational security measures to protect the personal data; and
- The third party data processor shall not permit subcontractors to process personal data in connection with its obligations to AIFM without the prior written consent of AIFM (or: the processor warrants that the subcontractors will be compliant with the terms of the contract it has with AIFM); and
- The AIFM has the right to review the security measures taken by the third party processor and the third party processor shall submit its relevant data processing facilities to audits, due diligences and inspections by the AIFM or any relevant government authority; and
- The third party processor shall promptly inform the AIFM of any actual or suspected security breach involving personal data; and
- The third party processor shall take adequate remedial measures as soon as possible and shall promptly provide AIFM with all relevant information and assistance as requested by the AIFM regarding the security breach.

12.4 Transfer of data to a non-adequate country

This section sets forth additional rules for the cross-border transfer of personal data to a third
party located in a non-adequate country that must be complied with in addition to the other requirements set out in this policy. Personal data may be transferred to a third party located in
a non-adequate country only if:

- The transfer is necessary for the performance of a contract with the individual, for managing a contract with the individual or to take necessary steps at the request of the individual prior to entering into a contract, e.g., for processing orders; or
- A contract has been concluded between AIFM and the relevant third party that provides for safeguards at a similar level of protection as that provided by this Policy or the contract shall conform to any model contract requirement under applicable local law, if any; or
- The transfer is necessary for the conclusion or performance of a contract concluded in the interest of the Individual between AIFM and a third party; or
- The third party has been certified under the United States Safe Harbor Program or any other similar program that is recognized as providing an "adequate" level of data protection; or
- The third party has implemented binding corporate rules or a similar transfer control mechanism which provide adequate safeguards under applicable law, a copy of the binding corporate rules or evidence of the transfer control mechanism must be provided to the AIFM prior to the transfer taking place; or
- The transfer is necessary to protect a vital interest of the Individual; or
- The transfer is necessary in connection with legal proceedings, advice or rights; or
- The transfer is necessary to satisfy a pressing need to protect an important public

interest; or
- The transfer is required by any law or regulation to which the AIFM is subject; or
- The data that will be transferred is included in a public register.

13. Personal data information breach and reporting

13.1 Data protection risks

This policy helps the AIFM to protect from several data security risk such as (among others):

- Breach of confidentiality: information being disclosed inappropriately;
- Breach of security: inappropriate access to sensitive data by third parties;
- Failing to offer choice: individuals should be free to choose how the AIFM uses data relating to them;
- Reputational damage in case of breach.

13.2 Reporting of breaches

Where a data breach is likely to result in a risk to the rights and freedoms of data subjects, the AIFM must inform the National Commission for Data Protection ("CNPD") of the breach. In certain cases mentioned above, the AIFM must also inform the data subjects of the breach.