



## **Personal Data Protection Policy**

Ref	IFPIM-30
Name	<b>Data Protection Policy</b>
Version	2.1
Effective Date	20/11/2019
Amended Date	21/09/2023
Approved by	Executive Committee : MB/PC
	Board of Directors : SN/PAZ/ AC
Next Review Date	Q4 2024
Status	In force

## Table of Contents

Definitions .....	3
1. Introduction to IFPIM .....	4
2. Purpose of the policy .....	4
3. Regulatory framework.....	4
4. Principles on data processing .....	5
5. Types of persons whose personal data may be collected (“Data Subjects”) .....	6
6. Types of personal data which may be collected .....	6
7. Source of personal data.....	7
8. Role of IFPIM: Data Controller or Data Processor .....	7
9. Personal data processing purpose.....	7
10. Provision of information on data processing .....	8
11. Rights of Data Subjects .....	9
12. Disclosure or transfer of personal data .....	10
13. Appointment of service providers .....	11
14. Personal data protection measures .....	11
15. Personal data retention.....	11
16. Data Protection Officer.....	12
17. Training on data protection.....	13
18. Personal data processing register .....	13
19. Employee private data.....	13
20. Reporting of breaches .....	14

## Definitions

The following definitions apply throughout this procedure:

- **IFPIM** or the **Company** means IFP Investment Management S.A.
- **Applicable Luxembourg Law** means, collectively, the Luxembourg laws, regulations and CSSF Circulars
- The **Board** means the Board of Directors of IFPIM
- The **Board Members** means the Members of the Board of Managers/Directors of IFPIM
- The **Senior Management** means the Senior Management Committee of IFPIM
- The **Internal Control Functions** mean the following IFPIM 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
- **Data 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 European Union or Member State law
- **CSSF** means Commission for the Supervision of the Financial Sector
- **CNPD** means National Commission for Data Protection
- **Data Processor** means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the Controller
- **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, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction

## **1. Introduction to IFPIM**

IFPIM is an Asset Management Company governed by the laws of the Grand-Duchy of Luxembourg.

IFPIM is authorized as:

- A UCITS Management Company under Chapter 15 of the Law of 17 December 2010 (the 2010 Law)

IFPIM is authorized to:

- Manage UCITS, i.e., perform the activities of:
  - Portfolio management
  - Fund administration
  - Marketing
- Provide the following services:
  - Wealth management services:
    - Discretionary portfolio management on a customer-by-customer basis
    - Investment advice

IFPIM may also be appointed by another investment fund or management company to provide the following types of services as a delegate:

- Portfolio management or investment advice
- Fund administration
- Fund marketing / distribution

## **2. Purpose of the policy**

This Personal Data Protection Policy (the “Policy”) defines how IFPIM 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
- Staff and secondees
- Key decision makers at IFPIM and the funds it manages
- Representatives of service providers

This Policy applies to IFPIM and the funds it manages.

## **3. Regulatory framework**

Applicable law and regulations in the context of personal data protection include (if not otherwise specified, laws and codes refer to the Luxembourg jurisdiction):

- 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
- UCITS Management Companies:
  - Law of 17 December 2010 relating to undertakings for collective investment (the “2010 Law”), and in particular Article 109 thereof
  - CSSF Regulation No 10-04 and in particular Articles 5 and 8 thereof
- 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 IFPIM Code of Conduct, Board Members, Senior Management and all IFPIM Staff commit to:

- Respect the general duty of confidentiality as a basic rule
- Respect personal data protection requirements
- Protect the information and data on IFPIM systems as well as any information and data transmitted thereto
- Ensure that any processing of information is carried out in a secure manner
- Keep records in accordance with Applicable Luxembourg Law.

To this effect, the Code of Conduct is signed for acceptance by every employee and directors, which means that a breach to the Code of Conduct represents a fault with respect to their professional obligations.

Staff and professionals who terminate their engagement with IFPIM are required to respect the confidential or privileged nature of information they have had access to, even after they have left, without any time limit.

IFPIM commits to ensure that personal data:

- Remain confidential, e.g. accessible only to those whose mission requires access to such data
- Are processed in a way that ensures protection against unauthorised or unlawful processing, accidental loss or damage.

## **5. Types of persons whose personal data may be collected (“Data Subjects”)**

In order to regularly conduct its business, IFPIM may need to collect, record, store, adapt, transfer and otherwise process information through which physical persons may be directly or indirectly identified (“Data Subjects”). These persons may include, inter alia:

- Staff and secondees (herein after referred to collectively as “Staff”), including members of Senior Management
- Candidate for positions at IFPIM
- Key decision makers at IFPIM and the funds it manages including:
  - The Board Members
  - Members of the Boards of the Funds managed by IFPIM
- Clients (including fund investors) and potential customers, their representatives, beneficial owners and ultimate beneficial owners
- Representatives of service providers and where relevant, their beneficial owners and ultimate beneficial owners.

## **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 like IP address, cookies and traffic data)
- 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 of investments, 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, reports of events)
- Advertisement and sales data.

## **7. Source of personal data**

IFPIM normally receives data through its business relationship with Data Subjects. IFPIM receives such information either directly from the Data Subjects or through Funds and/or sub-funds it manages, as well as placement and distribution agents, investment managers and/or advisors, depositary banks, central administration, registrar and transfer agents.

IFPIM may receive data from external sources, like in the case of AML/CFT database tools. These external sources may need to act in compliance with personal data protection requirements of their applicable jurisdiction, but IFPIM shall require that such data are provided in compliance with Applicable Luxembourg Law, as well.

In case of nominees subscribing to a Fund managed by IFPIM on behalf of a physical person, the data may be collected by the nominee. In those instances, 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 IFPIM: Data Controller or Data Processor**

IFPIM 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 IFPIM's behalf (e.g. Transfer Agent, payroll service provider).

IFPIM is not the Data Controller in respect to depositaries.

## **9. Personal data processing purpose**

IFPIM may only process personal data where:

- A Data Subject has given consent to the processing of his/her personal data for one or more specific purposes (written or oral declaration)
- Processing is necessary for the performance of a contract to which a 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 Data 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 Data Controller
- Processing is necessary for the purposes of the legitimate interests pursued by the Data Controller or by a third party (e.g., marketing, anti-fraud, processing of the customers or Staff 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, IFPIM processing of personal data will be strictly limited to the context of the performance of its business unless the Data Subject has given his/her specific consent to its use for other purposes and where processing of personal data is based on consent. In such case, the Data Subject has the right to withdraw his/her consent at any time.

IFPIM will always assure that personal data processing is limited to the extent needed to achieve the purposes for which data are collected.

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

- To operate and manage the fund
- To comply with any legal, tax or regulatory obligations applicable to IFPIM and its clients, including AML/CFT obligations
- For any other legitimate business interests

Clients are required to provide their personal data for statutory and contractual purposes. Failure to provide the required personal data or objection to such processing may result in IFPIM being unable to initiate or continue its relationship with the client.

## **10. Provision of information on data processing**

IFPIM shall provide information to Data Subjects on how their personal data are being used and for which purpose.

Such disclosure may be made available to Data Subjects through, *inter alia*,:

- A contract
- A notice
- The fund offering document
- The subscription form
- IFPIM website, where applicable

In certain contexts, such as meetings of governance bodies or other similar events, representatives of IFPIM or of its delegate(s) 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/events.

In such instances, the attendees shall be 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: <ul style="list-style-type: none"> <li>General Personal Data Processing Statement</li> <li>Cookie Policy</li> <li>Personal Data Processing Statement for fund investors</li> </ul>
Fund Investors	<ul style="list-style-type: none"> <li>In fund prospectuses: section on Personal Data Processing for fund investors</li> <li>In the subscription form: General Personal Data Processing Statement</li> <li>In the AML/CFT form: AML/CFT-specific Personal Data Processing Statement</li> <li>On the website: Personal Data Processing Statement for fund investors</li> </ul>
Direct clients	<ul style="list-style-type: none"> <li>In the contract: Personal Data Processing Statement for direct clients</li> <li>In the AML/CFT form: AML/CFT-specific Personal Data Processing Statement</li> <li>In case of recording of a call or conversation: oral request for authorisation to record the meeting; the consent may be recorded</li> </ul>
Staff	<ul style="list-style-type: none"> <li>In the employment agreement: a Personal Data Processing Clause</li> <li>In the Data Processing Statement for Staff</li> <li>In this Personal Data Processing Policy</li> </ul>
Delegates and other service providers	Either or both: <ul style="list-style-type: none"> <li>In the contract: Personal Data Processing Clause</li> <li>In a separate statement: Personal Data Processing Statements</li> </ul> The clause or statement may be calibrated as a function of the relevance of personal data to that service provider
Meeting participants	<ul style="list-style-type: none"> <li>In case of recording: oral request for authorisation to record the meeting; the consent may be recorded</li> </ul>

## 11. Rights of Data Subjects

IFPIM shall implement the rights granted to each Data Subject by the GDPR, including:

- The right of access:
  - The right to request confirmation whether or not his/her data are being processed, and when they are, 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 such transfer
- The right to rectification: whenever applicable, a Data Subject can require the Data Controller or appointed Data Processor to rectify inaccurate or incomplete personal data
- 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 the data were collected, or it is no longer lawful, or the data have 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; the Data Subject has objected to the Processing
- The right to withdraw consent: the right to withdraw his/her own consent at any time, if consent was the lawful ground for processing
- The right to object: the absolute right to object to the processing of personal data for direct marketing and a right supported by grounds for objecting for processing based on legitimate interests (e.g., the establishment, exercise or defence of legal claims) or performance of a task in the public interest
- Data portability: the right to receive the personal data in structured, commonly used and machine-readable format, or to have these data transmitted directly to another controller where technically feasible
- The right to complain either to the CNPD in Luxembourg or any other relevant data protection authority.

## **12. Disclosure or transfer of personal data**

IFPIM 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 it happens in an appropriate manner under 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 Staff data for the purposes related to labour contract management, etc.)
- The transfer of personal data is mandated by a judicial or administrative authority decision. However said decision originates from a jurisdiction outside the EU, 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.

IFPIM 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.

IFPIM and/or any of its delegates and service providers shall 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 releases and keeps current a list of Countries that are deemed to provide an adequate level of data protection.

IFPIM, 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, information related to Data Subjects as IFPIM and/or the Funds it manages reasonably determine. For avoidance of doubt, these include information which, in the reasonable determination of the discloser, are subject to be disclosed to competent authorities responsible for AML/CFT and pursuant to the Common Reporting Standard (CRS) as adopted by the OECD Council on 15 July 2014, as subsequently amended and implemented, and with reference 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, IFPIM shall engage service providers which comply with the GDPR or equivalent regulatory framework.

IFPIM will ensure that:

- Its contracts set out the service provider's specific obligations, including the processing of personal data only in accordance with IFPIM terms and/or
- Personal Data Processing Policy or equivalent document is obtained from the service provider, setting out how the service provider processes personal data

IFPIM performs due diligence and oversight on all of its service providers, including those who keep personal data on behalf of IFPIM. An important aspect of the due diligence on service providers is to ensure that they comply and continue to comply with the GDPR framework.

### **14. Personal data protection measures**

IFPIM implements appropriate administrative, technical, physical and security measures to:

- Meet the legal requirements on data processing
- Safeguard personal data against loss, theft and unauthorised access, use or alteration
- Keep personal data accurate, complete and up-to-date
- Ensure that service providers processing data on IFPIM behalf apply adequate security and safeguard measures
- Ensure that service providers have in place adequate organisational and technical measures which will allow IFPIM to comply with the GDPR requirements

### **15. Personal data retention**

#### *General rule*

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

In determining appropriate retention periods IFPIM 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.

IFPIM shall:

- Take all reasonable steps to destroy or erase 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 data from their systems when they are no longer required for the purpose(s) for which they were collected or to fulfil regulatory requirements

IFPIM may always keep data for a longer period if explicitly authorised by the Data Subject.

#### *Applications for job openings*

If a candidate applies to a positions for which he/she is not hired, IFPIM may keep the relevant personal data for a maximum of three (3) months after having declined the candidacy.

#### *Criminal records*

If IFPIM requests an extract of criminal record, the retention of the criminal record depends on the these scenarios:

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

#### *Data retention register*

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

## **16. Data Protection Officer**

IFPIM is not required to implement and does not have a Data Protection Officer (DPO) for the following reasons:

- IFPIM staff is below 150 units
- IFPIM does not process personal data on a large scale (directly or indirectly through external processors)

The person responsible for Personal Data Protection in IFPIM is the Compliance Officer.

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

## **17. Training on data protection**

IFPIM shall ensure that appropriate training is provided to its Staff on rules regarding the processing of personal data and their protection.

## **18. Personal data processing register**

IFPIM keeps a register of all personal data processing performed.

The register includes, inter alia, information on:

- The processing purpose
- 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 IFPIM in the data processing
- The department(s) of IFPIM accessing these data
- Other recipients of the data
- Whether the data relate to the main activity of IFPIM
- Whether the data are 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**

Staff are expected to use IFPIM systems and communications channels for the purpose of conducting IFPIM business, unless otherwise agreed in the employment contract of a given employee.

IFPIM understands that there might be occasions where Staff may need to use IFPIM systems and communications channels for private/personal reasons. These may include, for example, private telephone conversations and emails.

IFPIM expects the Staff to:

- Keep private use of IFPIM 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”)

IFPIM does not:

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

## **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 involved Data Subject, where required.