Opportunity Fund Management

Manual of procedures (incl. employee handbook)

History

Version	Release Date	Amended by	Reviewed by
1	21.11.2018	ESMC staff	Conducting Officers
2	03.10.2019	CT	Conducting Officers
3	16.10.2020	CT	Conducting Officers
4	31.12.2020	CT	Conducting Officers
5	20.12.2021	JL / BD	Conducting Officers
6	10.11.2023	JL	Conducting Officers
7	27.06.2024	JL	Conducting Officers

INTRODUCTION

About The Company

Opportunity Fund Management (the "**Company**" or the "**IFM**" ("Investment Fund Manager")) is a company incorporated under the laws of the Grand Duchy of Luxembourg having its registered office at 16, rue Robert Stümper, L-2557 Luxembourg, authorized and regulated by the Commission de Surveillance du Secteur Financier as UCITS Management Company and Alternative Investment Fund Manager as per respectively the amended law of 17 December 2010 and 12 July 2013.

The Company is an independent Management Company and forms part of the Eric Sturdza Group, a Swiss Banking group whose heritage in the private client arena provides a very unique point of view and consistently motivates the Company to put the investor at the heart of every key decision about their funds and portfolio managers. The Group's track record as expert selectors of portfolio management talent is testament to this ideal.

Private banking is a business of trust, understanding and respect, and these same traditional principles are applied to the asset management business. By understanding the client's individual needs, the Company can build trust and long-term relationships.

Our Vision

Our vision is to develop and enhance a distinctive brand and reputation as a leading boutique fund management company and to provide first class support to new and existing products, to ensure clients and investors receive the optimum levels of service.

Our Mission

To bring our vision to reality, our mission is to offer superior client focused investment products with a well-defined strategy of partnership with proven portfolio managers. We continually strive to provide our investors with class leading financial returns. Key to achieving this objective are our established partnerships with world renowned Investment Advisers. We pride ourselves on our speed and flexibility of execution and our operational excellence at every level of our organization, ensuring that we exceed our investors' expectations time after time.

Our Values

Our values are to ensure a comfortable and friendly working environment for all employees, with the flexibility to ensure that each employee is valued as an individual, with specific workloads tailored to individual considerations and requirements where possible. In addition to this, we ensure that all aspects of the business comply with the highest ethical standards, professionalism and integrity, with responsibilities completed with respect, skill, care and diligence, as well as to meet the regulatory requirements.

Purpose and Scope of the Employee Handbook (the "Handbook")

The purpose of this Handbook is to protect and enhance the Company's reputation for integrity by setting forth standards of conduct for you as an employee of the Company. The Company expects you to assume responsibility for ensuring that you abide by these standards.

The Handbook sets out employment policies that are fair, equitable and consistent with the skills and abilities of our employees and the needs of our business and are relevant to all employees of the Company. It reflects references to legal and regulatory requirements and will be updated where necessary and reviewed on an annual basis. It is not intended to be a comprehensive guide to every law, regulation or policy that could apply to the business of the Company and the absence of any references to specific laws, regulations or policies shall not absolve any employee from their responsibilities to the Company or from acting in the spirit of either this Handbook or any relevant law, regulation or policy. In addition, internal procedures have been implemented within the relevant teams and should be adhered to as required.

Responsibilities Concerning Changes to the Employee Handbook

The policies stated in this Handbook are subject to change at the sole discretion of the Company. In addition, the Company may implement additional policies in the future that will be deemed to be part of the Handbook. As an employee of the Company, it is your responsibility to ensure compliance with the contents of this Handbook and other policies and procedures which are/will be issued.

The Luxembourg Senior Management Team (the "Senior Management Team")

The Senior Management Team consists of the following personnel:

- Bertrand Didier: Conducting Officer Oversight;
- Hugo Vautier: Conducting Officer Risk; and
- Julien Lambert: Conducting Officer Compliance

Where the Senior Management Team has been referred to throughout this Handbook, it includes references to one member of the Senior Management Team. Should one member of the Senior Management Team receive any information referred to in this Handbook, notification should be made to the remainder of the Senior Management Team as soon as practically possible.

Compliance Officer and Responsable du contrôle du respect des obligations("RC")

The Compliance Officer and RC is Julien Lambert.

HR Personnel

The ultimate person responsible for any HR matters is Bertrand Didier.

In the first instance, please liaise with your Line Manager with regards to any HR queries. Alternatively, any HR matters may be discussed with HR Personnel.

Consequences of Abuse of the Handbook

Employees are required to act in accordance with established policies and procedures and to ensure that all of their activities on behalf of the Company are appropriate. Non-compliance with any of the relevant legislation, rules or guidance can lead to a breach, which may have to be reported to the relevant authorities, and could give rise to regulatory investigations. The penalties for violation include significant fines and suspension of license. Areas of non-compliance could lead to disciplinary action for the employee, which could result in dismissal for gross misconduct. The Company reserves the right to terminate its contractual relationship with connected parties where an employee has breached the Company's policies.

Monitoring and Review

The Company will monitor the effectiveness and review the implementation of all policies at appropriate intervals, considering their suitability, adequacy and effectiveness. Any improvements identified will be made at the subsequent annual review unless material, in which case they will be made as soon as possible and advised to all employees. Internal control systems and procedures will also be subject to regular review to provide assurance that they remain effective in accordance with regulatory and legal requirements.

Reporting to the Commission de Surveillance du Secteur Financier (the "CSSF")

The Company will ensure that the CSSF is advised of any material failure to comply with the provisions of the Regulations and the Rules in the Handbook and of any serious breaches of the policies, procedures or controls of the Company.

Acknowledging the Handbook

On joining the Company, you will be asked to complete the New Joiner Declaration form included in **Appendix 3** of this Handbook which includes confirmation that you have read the Handbook and that you understand and agree to abide by these requirements.

GENERAL TERMS OF EMPLOYMENT

The general terms of employment have been provided below. However, should your contract of employment differ, the information provided in your contract will prevail.

Personal Information

The employee consents to the Company procuring and processing their personal data and sensitive personal data, subject to the provisions of and in compliance with the Luxembourg Law of 2 August 2002 on the protection of persons with regard to the processing of personal data (Data Protections Law), as amended and the General Data Protection Regulations (GDPR) with effect from 25 May 2018 (as may be amended from time to time).

As part of the terms and conditions of employment the employee gives the Company permission to collect, retain and process information about them. This information will only be used so that the Company can monitor its compliance with the law and best practice in terms of equal opportunity and non-discrimination. The information which is held may be checked periodically to ensure that it remains up to date. You may request a copy of the personal data that is held by the Company about you.

Place of Work

Your place of work will be 16 rue Robert Stümper, Luxembourg, L-2557 in Luxembourg. The Company reserves the right to change the employee's place of work in accordance with its business needs subject to reasonable notice.

Hours of Work

Normal working days will be Monday to Friday inclusive with normal working hours from 9.00 am to 6.00 pm with an entitlement to a one hour break for lunch. The Company reserves the right to vary the hours of work in accordance with its business needs subject to reasonable notice. There may be the requirement to work outside of these hours, which may include requirements for travel, and the employee is therefore required to be flexible.

The European Working Time Directive sets a maximum working week of 48 hours. The Company may occasionally need the employee to work a working week longer than 48 hours. Such working would be very occasional and where possible with prior agreement.

Probationary Period

Your initial period of employment is subject to a probationary period of 6 months. During your probationary period, your performance and suitability will be assessed and, if it is satisfactory, your employment will continue with the Company. If your performance is not up to the required standard, or you are considered to not be suitable for the position, your employment with the Company will terminate. We reserve the right not to apply our capability and disciplinary policies during the probationary period.

Job Description

A detailed profile of the role and initial objectives will be agreed upon the commencement of employment between the parties, and thereafter subject to change from time to time. All employees will be required to undertake and perform additional tasks and duties as the directors of the Company or Senior Management Team may require from time to time.

Remuneration

Your basic salary is calculated per annum gross, and is payable monthly in arrears in twelve equal payments. All payments will be subject to deduction of tax and employee's Social Security

contributions. Salary payments will be made directly into each employee's bank account on or about the 25th day of each month.

Holidays

In addition to the normal Luxembourg public holidays, the employee is entitled to take an agreed number of days' holiday in each calendar year, the number to be agreed within the contract of employment. Holiday dates must be agreed in advance with the employee's Line Manager. The employee will be paid during their holidays under this clause in accordance with the Remuneration section in this Handbook. Holidays not taken in one calendar year may be carried forward into the next calendar year until 30 April, to a maximum of 5 days. Holidays accrue pro-rata during the calendar year.

The Company reserves the right to withhold any accrued holiday pay to which the employee may have become entitled should the employee fail to give proper notice of termination of their employment contract in the case of extended periods of sick leave or summary dismissal by the Company for gross misconduct.

The Company may implement specific closure dates at the office, with due notice, and the employee may be required to assign part of their holiday entitlement for that purpose.

Each employee has access to *e-days* that is an employee holiday tracking & absence management tool.

Study Leave

The Company supports study and examinations undertaken by all employees as relevant to their role. Study leave in relation to examinations is not an automatic entitlement and is subject to approval by your Line Manager and a member of the Senior Management Team based upon business requirements and individual circumstances. The amount of study leave is discretionary and is dependent on the level of the study/examination being taken. Study leave in addition to the agreed entitlement may be taken unpaid at the discretion of the Company.

Study Leave provided incorporates any time out of the office for workshops or study courses. Study leave is given for the first exam sitting (if on a working day only) but should anyone fail the exam, additional study leave and re-sits would need to be taken as holiday.

You are required to discuss and agree the amount of study leave with your Line Manager and a member of the Senior Management Team before signing up for the particular line of study.

Each employee has access to *e-days* that is an employee holiday tracking & absence management tool.

Sick Leave

If the employee is absent from work due to sickness or injury, they must inform their Line Manager by telephone by 9am on each day of absence giving an estimate of their date of return. In respect of an absence lasting two or fewer days, the employee need not generally produce a medical certificate unless specifically requested to do so by the Company.

If the employee's absence exceeds two consecutive days, they must produce a medical certificate stating the reason for absence and thereafter produce a like certificate each week to cover any subsequent period of absence. The Company may require the employee to provide medical evidence of their fitness to resume to work prior to doing so and to submit a medical examination by a registered medical practitioner nominated by the Company, and to agree to the medical practitioner providing a confidential report to the Company on request.

Each employee has access to *e-days* that is an employee holiday tracking & absence management tool.

Compassionate Leave

The Company is sympathetic and supportive in its requirement to provide compassionate leave. Compassionate leave may be granted at the discretion of a director or the Senior Management Team to assist employees in dealing with short term emergencies in relation to immediate family. The amount of time provided will be determined on a case by case basis and a request for compassionate leave should be discussed directly with your Line Manager who will take this forward should compassionate leave be required.

Each employee has access to *e-days* that is an employee holiday tracking & absence management tool.

Death and Disability Insurance

Death and Disability Insurance cover is provided on commencement of employment.

Discretionary Bonus

The Company may in its absolute discretion pay employees an annual bonus of such amount and subject to such conditions as the Company may determine from time to time to be notified to the employee.

Any bonus to the employee shall be purely discretionary and shall not form part of the employee's contractual remuneration. If the Company makes a bonus payment to the employee in respect of a particular financial year, it shall not be obliged to make subsequent bonus payments in respect of subsequent financial years of the Company.

Notwithstanding the above clause the employee shall in any event have no right to a bonus or a time-apportioned bonus if their employment terminates for any reason or they are under notice of termination (whether given by the employee or the Company) at or before the date when a bonus might otherwise have been payable.

Bonus payments are confidential and should not be disclosed to other employees.

Appraisals

A performance appraisal scheme is in place to evaluate the performance of each employee, at least once a year, in areas of core competency in terms of their role but also their interpretation and contribution to the core values, strategic objectives and general development of the organisation both on a day to day basis but also in the wider environment of acting with longer term perspective. The appraisal process provides an open discussion environment, allowing the employee the opportunity to assess their own development, both individually and in the context of the team, which, together with management input, can be used to establish and evaluate goals and objectives.

Expenses

The Company shall reimburse the employee for reasonable business-related expenditure, provided that the employee provides receipts and vouchers to support such expenditure if required.

The Company reserves the right to perform an audit of expenses and should it be found that any employee has claimed incorrectly this may be subject to the Company's Disciplinary Policy.

Deduction from Salary

The Company is entitled at any time during the employee's contract of employment to deduct by way of reimbursement from the employee's salary any overpayment of salary or expenses that have been paid to the employee for any reason.

Upon termination of employment, the Company is entitled to make any such deduction including but not limited to:

- deduction by way of reimbursement of any overpayment of salary or expenses that have been paid to the employee for whatever reason; and/or
- deduction in respect of any holiday taken by the employee in excess of their holiday entitlement;
- any other sums owed by the employee to the Company.

Changes in Personal Details

Employees must notify the Company of any change of name, address and contact details to ensure accurate information is maintained on the Company's records should contact be required outside normal working hours.

Restriction on Other Employment (Outside Business Interests "OBI")

Whilst employed by the Company, the employee may not, without prior written consent by the Conducting Officers, accept or fulfil any other employment, appointment or engagement inconsistent with its employment with the Company.

All employees must:

- disclose and seek approval of any existing OBI from the Conducting Officers on joining the Company (as requested in the New Joiner Declaration Form)
- obtain pre-approval from the Conducting Officers before entering into a new OBI
- notify the Conducting Officers of any OBI of connected persons
- confirm OBI when completing the Annual Declaration Form.

Examples of OBI

- Charity Work
- Other Directorships
- Employment other than by the Company (paid or unpaid)
- Receipt of commissions for business undertaken outside of the Company
- Engaging in any other activity that might:
    - Influence or conflict with the employee's decisions or actions in executing policies and procedures
    - Activity that may impair the employee's physical capacity to render proper and efficient service to the Company at all times
    - Activity that may interfere with the impartial performance or jeopardize the employee when undertaking a service to the Company.

The materiality of any potential conflicts, and whether they can be effectively managed, will be discussed with the Senior Management Team. Should the OBI not be approved, the employee will be prohibited from undertaking the proposed role.

Acceptable Use of Email, the Internet and the Telephone

All of the Company's IT facilities and information resources remain the property of the Company and not of particular individuals, teams or departments.

The Employee acknowledges that access to the Company's computer and telephone systems is provided for business purposes only. The Employee agrees to abide, at all times, with any relevant policy or procedure issued by the Company from time to time. Unauthorized use of e-mail or internal systems is a serious breach of discipline and may result in disciplinary action against the Employee including dismissal without notice or payment *in lieu* of notice.

Personal use of the Company's telephone is permitted for short calls and must not be used for long-distance and toll calls without the permission of the Senior Management Team.

Please refer to the separate Information Security Policy provided in the policies section of this handbook which provides further information.

Suspension

The Company may suspend the employee from their duties and/or exclude them from the Company's premises pending any investigation involving the Company provided that during any such period of suspension the employee shall be entitled to receive their remuneration in accordance with the Remuneration section.

Termination of Employment

The employee's employment is terminable by either party based on their length of time worked following the successful completion of a probationary period of six months. Termination with notice of your employment contract is subject to the compliance with the provisions of articles L. 124-1 *et seq.* of the Labour Code. Termination without notice of your employment contract is subject to the compliance with the provisions of article L. 124-10 of the Labour Code.

Return of Company Property

The employee shall return to the Company all property (whether original or copies) including, but not limited to, their identity or entry card, keys, access codes, notes, memoranda, correspondence, documents (paper or electronic), personal laptops and any other property belonging to the Company or any group affiliate of the Company in the employee's possession or which has come into the employee's possession.

Restrictions after Cessation of Employment

Following termination of employment for any reason, the employee will not for the period of 12 months thereafter directly or indirectly attempt to entice away or solicit any employee of the Company or any group affiliate of the Company.

Following termination of employment for any reason, the employee will not for a period of 12 months thereafter take any action to solicit or assist any other person to solicit any client or commercial connection of the Company or of any group affiliate of the Company by offering any service which directly or indirectly substitutes for a service currently or previously provided by the Company or a group affiliate of the Company.

The employee will not obtain, retain, source, pass on or utilise any information relating to the identity of any current, historic or prospective clients or customers of the Company or group affiliate of the Company or any such client or customers interest or investment in any of the Company's or group affiliate of the Company's services or products following cessation of employment with the Company.
Each of the undertakings contained in each paragraph of this clause shall be enforceable by the Company independently of each other and each shall not be affected by any illegality or invalidity of any such other undertaking.

The undertakings contained above within this section are considered by the parties to be reasonable in all circumstances. If one or more should be held invalid as an unreasonable restraint of trade or for any other reason whatsoever but would have been valid if part of the wording thereof had been deleted

or the period thereof reduced or the range of activities or area dealt with thereby reduced in scope, the said undertakings shall apply with such modifications as may be necessary to make them valid and effective.

POLICIES

This section of the Handbook contains the policies to be adhered to as an employee of the Company. Procedures to assist in the implementation of these policies have been separated out within the relevant teams. Both the policies and the procedures must be followed. If you are unclear about any aspect of these policies, you should seek guidance from your Line Manager.

CODE OF CONDUCT

All employees of the Company are responsible for exercising good judgment and applying high ethical standards to their work, and acting in accordance with the laws and regulations that govern the business, and the internal policies and procedures set out by the Company. They are also responsible for alerting the Senior Management Team to actual and potential violations of laws, regulations and breaches of internal policies or procedures.

The Principles of the Code of Conduct set out by the Company in line with relevant rules and regulations, to which all employees must comply with at all times, are as follows:

Integrity, honesty and fairness
In conducting its business activities, the Employee should act honestly, fairly, and in the best interests of clients and the integrity of the market.

Skill, Care and Diligence
In conducting its business activities, the Employee should act with due skill, care and diligence, and in the best interests of clients and the integrity of the market.

Capabilities
The Company has to employ effectively the resources and procedures which are needed for the proper performance of its business activities.

Information about Clients
The Employee must seek clients' information about their financial situation, investment experience and investment objectives relevant to the services to be provided.

Information for Clients
The Employee must make adequate disclosure of relevant material information in its dealing with clients.

Conflicts of Interest
The Company must try to avoid conflicts of interest, and when conflicts cannot be avoided, it should ensure that clients are fairly treated.

Compliance and Market Activities
The Employee must comply with all regulatory requirements applicable to the conduct of its business activities so as to promote the best interests of clients and the integrity of the market.

Client assets
The Employee must ensure that client assets are promptly and properly accounted for and adequately safeguarded.

Responsibility of Senior Management
The Senior Management of the Company should bear primary responsibility for ensuring the maintenance of appropriate standards of conducts and adherence to proper procedures by the Company.

Regulatory relations
The Employee must act in an honest and transparent manner with the CSSF and any other applicable regulators to which the Company or the Company's business activities are subject.

CODE OF ETHICS AND STANDARDS OF PROFESSIONAL CONDUCT

In addition, the Company has adopted the ALFI Code of Conduct (http://www.alfi.lu/sites/alfi.lu/files/ALFI-Code-of-Conduct.pdf), and every Employee should make sure that at every time the following standards are observed:

- Act with integrity, competence, diligence, respect, and in an ethical manner with the public, clients, prospective clients, employers, employees, colleagues in the investment profession, and other participants in the global capital markets.

- Act fairly and independently, and place the interests of clients above their own personal interests.

- Comply with all applicable laws, regulations, and the Fund's constitutional documents.

- Ensure that investors are properly informed, are equitably treated, and receive the benefits and services to which they are entitled. More precisely, the Employee must ensure that:
  - The information provided to investors about the Fund particularly with regard to the fund's investment objectives, risks and costs, is true, fair, timely and not misleading;
  - Investors are kept informed of matters relevant to their investment in a form and language that is clear and easy to understand;
  - Information relating to the Fund's financial situation and performance is prepared and disclosed in accordance with relevant accounting standards (e.g. Lux GAAP, IFRS);
  - Each investor complaint is reviewed and, if it is upheld, that redress is provided within a reasonable time;
  - Investors receive the benefits and level of services to which they are entitled as defined by law, contractual arrangements, and the fund's constitutional documents.

- Contribute to the maintenance, and improvement of an effective risk management process and appropriate internal control environment.

- Avoid, to the best of their ability, any potential or apparent conflict of interest and where a conflict of interest does arise, ensure appropriate disclosure. To this end, each Employee should make all reasonable efforts to avoid any circumstances that may give rise to a conflict of interest; where such a conflict arises, they should the procedures which are in place to address such conflicts on an arm's length basis and disclose these adequately as defined in the policies and procedures.

- Maintain and improve their professional competence and strive to maintain and improve the competence of other investment professionals.

Standards of Professional Conduct

The Company maintains the following Standards of Professional Conduct.

I. Professionalism

A. *Knowledge of the Law*

Employees must understand and comply with all applicable laws, rules, and regulations of any government, regulatory organization, licensing agency, or professional association governing their professional activities. The Company will provide suitable guidance/training to ensure all employees are aware of the laws, rules and regulations applicable to them within their role. In the event of conflict, employees must comply with the stricter law, rule, or regulation. Employees must not knowingly participate or assist in and must dissociate from any violation of such laws, rules, or regulations.

B. *Independence and Objectivity*
Employees must use reasonable care and judgment to achieve and maintain independence and objectivity in their professional activities. Employees must not offer, solicit, or accept any gift, benefit, compensation, or consideration that reasonably could be expected to compromise their own or another's independence and objectivity (see Gifts and Entertainment Policy).

C. *Misrepresentation*
Employees must not knowingly make any misrepresentations relating to investment analysis, recommendations, actions, or other professional activities.

D. *Misconduct*
Employees must not engage in any conduct involving dishonesty, fraud, or deceit or commit any act that reflects adversely on their professional reputation (or the reputation of the Company), integrity, or competence.

II. Integrity of Capital Markets

A. *Material Nonpublic Information*
Employees who possess material nonpublic information that could affect the value of an investment must not act or cause others to act on the information

B. *Market Manipulation*
Employees must not engage in practices that distort prices or artificially inflate trading volume with the intent to mislead market participants.

III. Duties to Clients

A. *Loyalty, Prudence, and Care*
Employees have a duty of loyalty to their clients and must act with reasonable care and exercise prudent judgment. Employees must act for the benefit of their clients and place their clients' interests before their employer's or their own interests.

B. *Fair Dealing*
Employees must deal fairly and objectively with all clients when providing investment analysis, making investment recommendations, taking investment action, or engaging in other professional activities.

C. *Suitability*

1. When Employees are in an advisory relationship with a client, they must:

    a. Make a reasonable inquiry into a client's or prospective client's investment experience, risk and return objectives, and financial constraints prior to making any investment recommendation or taking investment action and must reassess and update this information regularly.
    b. Determine that an investment is suitable to the client's financial situation and consistent with the client's written objectives, mandates, and constraints before making an investment recommendation or taking investment action.
    c. Judge the suitability of investments in the context of the client's total portfolio.

2. When employees are responsible for managing a portfolio to a specific mandate, strategy, or style, they must only make investment recommendations or take investment actions that are consistent with the stated objectives and constraints of the portfolio.

D. *Performance Presentation*
When communicating investment performance information, employees must make reasonable efforts to ensure that it is fair, accurate, and complete.

E. *Preservation of Confidentiality*

Employees must keep information about current, former, and prospective clients confidential unless:

1. The information concerns illegal activities on the part of the client or prospective client,
2. Disclosure is required by law, or
3. The client or prospective client permits disclosure of the information.

IV. Duties to Employers

A. *Loyalty*

In matters related to their employment, employees must act for the benefit of their employer and not deprive their employer of the advantage of their skills and abilities, divulge confidential information, or otherwise cause harm to their employer.

B. *Additional Compensation Arrangements*

Employees must not accept gifts, benefits, compensation, or consideration that competes with, or might reasonably be expected to create a conflict of interest with, their employer's interest unless they obtain written consent from all parties involved (see Gifts and Entertainment Policy).

C. *Responsibilities of Supervisors*

Employees must make reasonable efforts to ensure that anyone subject to their supervision or authority complies with applicable laws, rules, regulations, and the Code and Standards.

STAFF RECRUITMENT & BEHAVIOURAL POLICY

Employee Screening

To ensure the Company recruits employees of the required standard of competence and probity, the recruitment process of new employees includes the following:

- To obtain and confirm appropriate references at the time of recruitment
- To request information for any employee with regards to any regulatory action against them or action taken by a professional body
- To complete a World-check to confirm there are no sanctions imposed
- To obtain a Police Disclosure with regard to any criminal convictions
- To obtain information on any Outside Business Interests (see the section on Restriction on Other Employment)

In addition, all employees of the Company are required to provide the HR Personnel the following documentation on commencement of employment:

- Proof of identity: Copy of a valid Passport, duly certified
- Address verification: Utility Bill (within the last 6 months), original or certified copy
- Copies of professional qualifications (i.e. only those awarded by Professional bodies (e.g. CIMA, CISI, ACA, etc.), or, for School Leavers, educational qualifications)
- Confirmation of any professional memberships (information to be included on the New Joiner Declaration Form – **Appendix 3**).

Employees include any individual working for the Company under a contract of employment (including on a temporary basis). The separate Outsourcing Policy provides information with reference to individuals employed by service providers to which the Company's business is outsourced.

Professional Obligations

The Company places an emphasis on continued learning and development to enhance the training and knowledge of its employees, all of whom are required to understand the professional and legal

obligations owed to the Company both in the spirit and the letter of their contract of employment and this Handbook.

All employees are required to act in accordance with established policies and procedures and ensure that all of their activities on behalf of the Company are appropriate. Employees have a duty to ensure they maintain the required knowledge of any relevant legislation, rules or guidance and all policies and procedures in relation to their employment within the Company and to their individual role. Employees must ensure that any weaknesses or deficiencies in these areas on their own part or that of others are duly reported to the Senior Management Team and the Head of Legal and Compliance. An employee should not jeopardize the reputation or financial position of the Company. Should anything be identified that is not understood, it is the responsibility of the employee to advise their Line Manager who will arrange for the relevant knowledge and training to be provided.

All employees are subject to ongoing review of actions undertaken on behalf of the Company. Communications made on behalf of the Company should include your Line Manager to ensure adequate monitoring and supervision.

Previous Conduct, Activities and Offences

All directors and employees are required to disclose to the Conducting Officers any conduct prior to and during the course of their employment, if they have:

- Committed any offence (except for parking tickets where any liability to conviction of fixed penalty notice has been discharged upon payment of the ticket), and in particular any offence involving fraud or other dishonesty or involving violence in any jurisdiction;

- Breached any provision contained in the Law of 5 April 1993 on the financial sector, as amended or any regulatory Law in any other jurisdiction;

- Breached any enactment relating to money laundering or terrorist financing (including, for the avoidance of doubt, rules, instructions and guidance issued by the CSSF in relation thereto) in any jurisdiction;

- Breached any other enactment due to incompetence or malpractice within any financial business in any jurisdiction;

- Been declared "en désastre" or bankrupt in any jurisdiction;

- Engaged in any business practices (whether unlawful or not) which may appear to the Commission as deceitful or improper, that reflect discredit on method of conducting business or suitability to conduct business or been associated with any other business practices or otherwise conducted themselves in such a way as to cast doubt on their competence and soundness of judgment in any jurisdiction.

OPPORTUNITY FUND MANAGEMENT

DRESS CODE POLICY

About This Policy

The Company encourages everyone to maintain an appropriate standard of dress and personal appearance at work. The purpose of the dress code is to establish basic guidelines on appropriate clothing and appearance within the workplace, so that we:

- promote a positive and professional image;
- respect the needs of men and women from all cultures and religions;
- make any adjustments that may be needed because of disability;
- take account of health and safety requirements; and
- help Senior Management decide what clothing it is appropriate to wear to work.

Senior Management are responsible for ensuring that this dress code is observed and that a common sense approach is taken to any issues that may arise. Failure to comply with the dress code may result in action under our Disciplinary Policy and Procedure.

We will review our dress code periodically to ensure that it reflects appropriate standards and continues to meet our needs.

This policy does not form part of any employee's contract of employment and we may amend it at any time.

Appearance

While working for us you represent the Company with clients and the public. Your appearance contributes to our reputation and the development of our business.

It is important that you appear clean and smart at all times when at work, particularly when you may be in contact with clients, other business contacts or the general public.

All employees should wear smart business attire or business casual attire.

Any enquiries regarding the operation of our dress code (including whether an article of clothing is suitable to wear to work) should be made to your Line Manager.

OPPORTUNITY FUND MANAGEMENT

GOVERNANCE POLICY & DECISION MAKING PROCEDURES

About This Policy and Procedure

The Company describes here below in its decision-making policy and procedure its internal functioning, reporting lines and allocation of functions and responsibilities.

The general meeting of shareholders

The general meeting is the body that brings together all the shareholders of a legal person. The shareholders' general meeting has all necessary powers to perform or ratify acts of interest to the Company.

The Company has only one shareholder, this shareholder exercises all the powers conferred by the articles of association of the Company.

The Board of Directors

Duties of the Board of Directors

The Board of Directors is the executive body of the Company carrying out the management and administration duties. Its composition and powers are defined in the articles of association of the Company.

The Board of Directors of the Company:

- ensures that high standards of corporate governance are applied at all times;
- has good professional standing and appropriate experience and use best efforts to ensure that it is collectively competent to fulfil its responsibilities;
- acts fairly and independently in the best interests of the investors of the investment funds managed by the Company;
- acts with due care and diligence in the performance of its duties;
- ensures compliance with all applicable laws, regulations and with the constitutional documents of the investment funds managed by the Company;
- ensures that investors of the investment funds managed by the Company are properly informed, are fairly and equitably treated, and receive the benefits and services to which they are entitled;
- ensures that an effective risk management process and appropriate internal controls are in place;
- identifies and manages fairly and effectively, to the best of its ability, any actual, potential or apparent conflict of interest and ensure appropriate disclosure;
- act with honesty, integrity and independence of mind.

[ALFI Code of Conduct for Luxembourg investment funds[1]]

Management mandate

There are at least three Directors on the Board of Directors of the Company.

The Directors can be resident or non-resident.

[1] These principles are further detailed in the ALFI Code of Conduct for Luxembourg investment funds.

The Board members are appointed by the shareholders' general meeting for a maximum renewable term of 6 years.

[Articles of association of the Company]

The members of the Board of Directors must be of sufficiently good repute and sufficiently experienced in relation to the type of fund concerned and the investment strategies pursued by the managed funds.

[Section 4.1. CSSF Circular 18/698]

The members of the Board of Directors of the Company shall possess adequate collective knowledge, skills and experience to be able to understand the Company's activities, in particular the main risks involved in those activities and the assets in which the funds are invested.

To that end, the identity of these persons as well as every person succeeding them in office are communicated forthwith to the CSSF for approval.

This notification is accompanied by the following pieces of information:

- a recent curriculum vitae, signed and dated,
- a copy of the passport/identity card;
- a declaration of honor, as may be downloaded on the CSSF website (www.cssf.lu);
- if available in the jurisdiction of the person concerned, a recent extract of the criminal record and
- A table listing the professional activities and the mandates performed in the regulated and non-regulated entities, including, the mandates for which an approval was requested from a supervisory authority, and detailing the time spent on each activity or mandate. The form to be used can be downloaded on the CSSF website.

With regard to sufficient experience, the Directors and the permanent representative, in the case where a legal person has been appointed as director, respectively, have adequate professional experience gained through having already performed similar activities to a high level of responsibility and autonomy.

[Section 105 CSSF Circular 18/698]

Furthermore, every member of the Board of Directors of the Company dedicates the required time and attention to properly perform their duties. Consequently, they ensure that they limit the number of other professional engagements, in particular mandates held in other companies, to the extent necessary in order to perform their tasks correctly.

[Section 4.1.3. CSSF Circular 18/698]

Competencies of the Board of Directors

- **Management**

The Board of Directors manages the Company and is vested with the broadest powers to act in the name of the Company and to take any actions necessary or useful to fulfil the Company's corporate purpose, with the exception of the powers reserved to the general meeting of the shareholders.
The Board of Directors delegates the day-to-day management and representation of the Company to at least two conducting officers of the Company

These conducting officers could be Directors or not and their acts are binding on the Company towards third parties. The appointment, dismissal and competencies of these representatives are governed by the articles of association or by a decision from the Board of Directors.

- **Representation**

The Company shall be bound towards third parties in all circumstances by the joint signatures or the sole signature of any person(s) to whom such power may have been delegated by the Board of Directors within the limits of such delegation.
The Company can also be represented by the conducting officers for the daily management of the Company, or can be represented by a representative (proxy) within the context of a specific business-related act.

The conducting officers are in charge of the daily management and representation of the Company. Their acts are binding on the Company towards third parties, even if they exceed the powers entrusted to them (provided that the third parties act in good faith).

Board of Directors' meetings

The Board of Directors elects a chairperson from within its ranks. The means of convening the Board of Directors is determined by the articles of association. The Board of Directors meets at the frequency defined by the articles of association. Since the Board of Directors is a collegiate body, all of its decisions are taken following deliberations.

As stipulated in the articles of association and without prejudice to stricter legal provisions, the internal rules concerning the quorum and decisions taken by the Board of Directors are as follows:

- at least half of the members are present or represented;
- decisions are taken by majority vote of the members present or represented;
- in the absence of statutory provisions on the matter, the chair has the casting vote in the event of a split vote.

The meetings of the Board of Directors take place in principle at the registered office of the Company located in the Grand Duchy of Luxembourg (the country in which it is held determines the effective place of management of the Company) and in the presence of the Directors.

Meetings may also be held by teleconferencing or videoconferencing or by any other means of telecommunication which allows for their identification, are deemed present. Meetings held by such means of telecommunication are deemed to have taken place at the registered office of the Company.

As stipulated in the articles of association, the Board of Directors may, unanimously, adopt resolutions by circular means.

The conducting officers / the management committee

Duties of the conducting officers / management committee

By conducting officers, it is understood the persons who effectively conduct the business of the Company on a daily basis. The number of conducting officers is at least two.

The conducting officers must also fulfil the conditions as to good repute and professional experience required for the type of fund managed and the investment strategies pursued by the fund. To that end, the identity of each conducting officer as well as of every person succeeding him in office is communicated forthwith to the CSSF for approval.

[Article 102 (1) of the 2010 Law]

This notification is accompanied by the following pieces of information:

- a recent curriculum vitae, signed and dated;
- a copy of the passport/identity card;
- a declaration of honor, as may be downloaded on the CSSF website (www.cssf.lu);
- if available in the jurisdiction of the person concerned, a recent extract of the criminal record and
- a table listing the professional activities and the mandates performed in the regulated and non-regulated entities, including, among others, the mandates for which an approval was requested from a supervisory authority, and detailing the time spent on each activity or mandate, respectively. To this end, the form to be used can be downloaded on the CSSF website

With regard to required experience, the conducting officers have adequate professional experience gained through having already performed similar activities to a high level of responsibility and autonomy.

The CSSF is able to contact the conducting officers directly. These persons are able to provide all information that the CSSF deems essential for its supervision.
For the accomplishment of their tasks, the conducting officers permanently reside, in principle in Luxembourg. This does not however prevent the conducting officers from having their domicile in a place permitting them, in principle, to come to Luxembourg every day.

Having regard to the nature, scale and complexity of the activities of the Company, the CSSF may nevertheless agree, through a duly supported request for derogation made in advance, that only one of the conducting officers of the management company permanently resides in Luxembourg.

The conducting officers together with the Compliance Officer form the management committee. The members of this committee work together in close partnership to take all actions falling within the scope of their responsibilities.

The management committee is, amongst other, responsible for the following tasks, under the ultimate responsibility of the Board of Directors:

- to implement the general investment policy, for each managed investment fund, as defined, where relevant, in the constitutive documents of the investment fund (i.e. prospectus, management regulations or articles of association);

- to ensure and verify on a regular basis that the general investment policy and strategy implemented comply with and reflect appropriately the prospectus and the UCITS-KIID and/or the PRIIPs-KIID of each sub-fund and that the general investment policy and strategy are described in a transparent manner in the prospectus and, where appropriate, in the UCITS-KIID and/or in the PRIIPs-KIID;

- to oversee the approval of investment strategies for each managed investment fund;

- to ensure that valuation policies and procedures are established and implemented according to the requirements of the law;

- to ensure that the Company has a permanent and effective compliance function, even if this function is performed by a third party;

- to ensure and verify on a regular basis that the general investment policy, the investment strategies and the risk limits of each managed investment fund are properly and effectively

implemented and complied with, even if the risk management function is performed by third parties;

- to approve and review on a periodic basis the adequacy of the internal procedures for undertaking investment decisions for each managed investment fund, so as to ensure that such decisions are consistent with the approved investment strategies;
- to approve and review on a periodic basis the risk management policy and arrangements, processes and techniques for implementing that policy, including the risk limit system for each managed investment fund;
- to assess and periodically review the effectiveness of the policies, arrangements and procedures put in place to comply with the requirements of the law;
- to take appropriate measures to address any deficiencies;
- to review on a frequent basis, and at least annually, written reports on matters of compliance, internal audit and risk management indicating in particular whether appropriate remedial measures have been taken in the event of any deficiencies;
- to review on a regular basis reports on the implementation of investment strategies and of the internal procedures for taking investment decisions;

[Article 92 CSSF Circular 18/698]

- to implement strategies and guiding principles for central administration and internal governance through specific written internal policies and procedures;
- to ensure that the Company has the technical infrastructure and human resources necessary for performing its activity;
- to implement and follow-up the marketing policy and the distribution network of investment funds managed by the Company.
- to implement adequate internal control mechanisms designed to secure compliance with decisions and procedures at all levels of the Company (i.e. permanent compliance, internal audit and risk management functions).

[Article 91 CSSF Circular 18/698]

In order to fulfill its responsibilities, the management committee works in accordance with a method of operation adapted to the activities of the Company. Thus, for example, the conducting officers are in regular contact with each other and hold periodic meetings. These meetings are formalized in minutes, available in the premises of the Company in Luxembourg. It is important that the agenda of these periodic meetings of the conducting officers includes, amongst other, a discussion on the management information as defined in the box below.

[Section 4.2.3. CSSF Circular 18/698]

The management committee informs regularly, completely and in written the Board of Directors of the Company and the Board of Directors of investment funds managed by the Company.

[Section 4.2.3. CSSF Circular 18/698]

Definition of management information

The Company maintains in an adequate and orderly manner records of its activities and its internal organization.

To this end, the Company puts in place a Management Information enabling the monitoring of its activity and that of its delegates.

This Management Information covers, amongst others, the results of controls carried out on the activities of delegates, the analyses in the area of risk management, the incidents linked to the activity of collective management (significant and non-significant NAV errors, breaches of limits, valuation problems, problems of reconciliation, situations giving rise to conflicts of interest and to other problems), execution policy, complaints, minutes of previous meetings, etc.).

As the Management Information also provides information about the controls made on the delegated activities, the Company ensures that it receives from the delegates all necessary information in order to effect an efficient control of its delegates.

Finally, it is ensured that this Management Information is available in Luxembourg and preferably kept in a central database accessible at any time in Luxembourg.

[Section 5.5.1. CSSF Circular 18/698]

Allocation of tasks and responsibilities between of the conducting officers / within the management committee

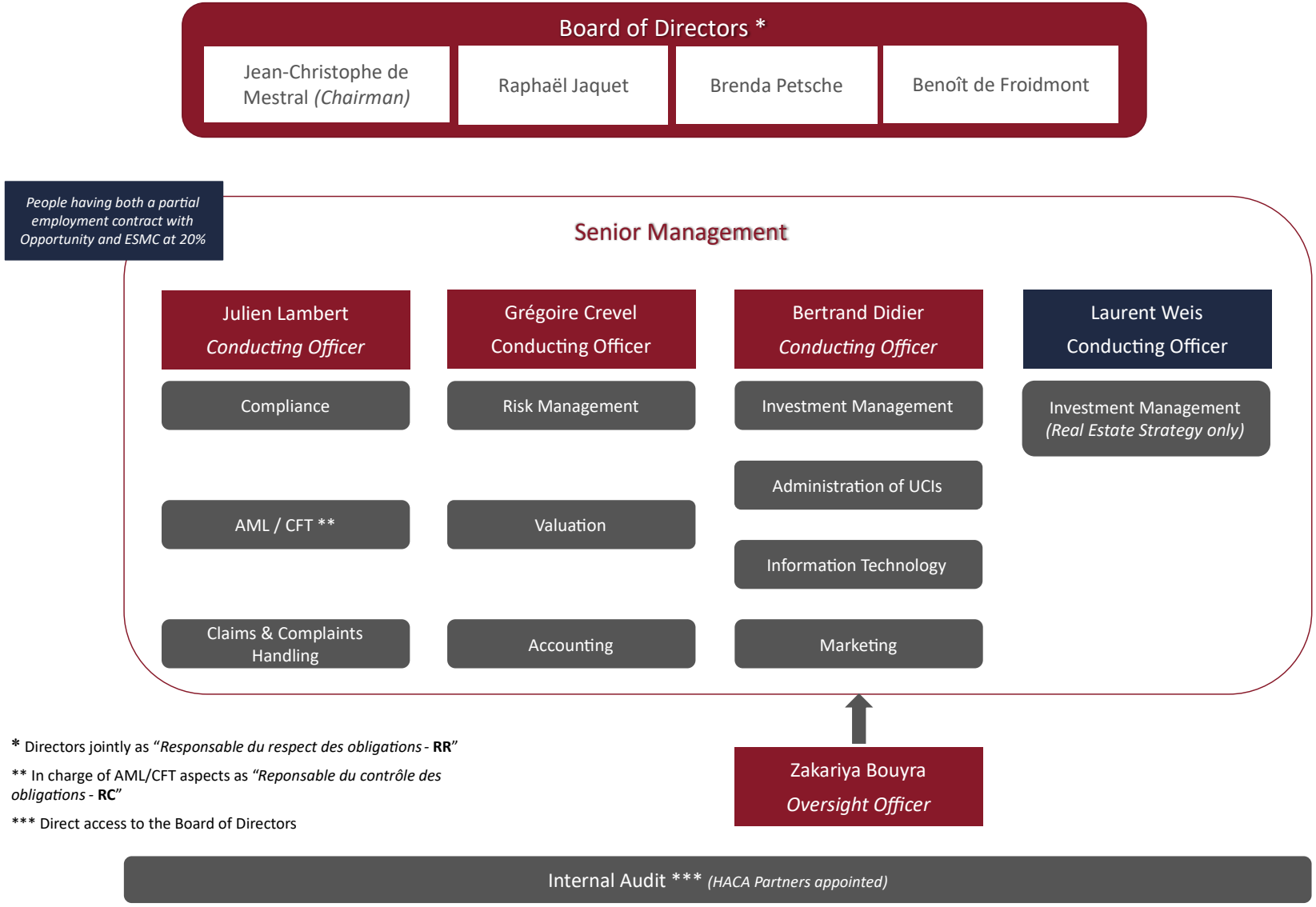
Within the framework of the management committee, each of the conducting officer is allocated specific responsibilities.

It cannot be allocated to the same conducting officer the functions of risk taking and of independent control of those same risks (i.e. the execution and/or the control of the risk management function and the function of investment management cannot be ensured by the same conducting officer, for instance).

This does not exclude the possibility for conducting officers to use on the basis of a service agreement the expertise and/or technical means existing at the level of other organizational/operational units existing at the group level to which the Company belongs to and/or at the level of third party having the capacities, quality and the authorizations required to provide the support requested in a reliable and professional manner.

OPPORTUNITY FUND MANAGEMENT

Appendix I – Organizational structure of the Company



* Directors jointly as "*Responsable du respect des obligations* - **RR**"

** In charge of AML/CFT aspects as "*Reponsable du contrôle des obligations* - **RC**"

*** Direct access to the Board of Directors

Appendix II – Reporting to the Conducting Officers & the Board of Directors of the Company

Function	Responsible person	Information or documents to report	Frequency to report	Addressees
Internal audit	Conducting Officer responsible for the Internal Audit Function	• Internal audit report	Annually	• Conducting officers • Board of Directors
Risk management (including investment compliance)	Conducting Officer responsible for the Risk Management Function	• Risk management report • Risk management activity report • OTC counterparties Due Diligence Report	Annually Monthly When new Counterparty appointed	• Conducting officers • Board of Directors • Conducting officers • Board of Directors • Conducting officers • Board of Directors
Compliance	Conducting Officer responsible for the Compliance Function	• Compliance report • Compliance activity report	Annually Quarterly	• Conducting officers • Board of Directors • Conducting officers • Board of Directors
Administration	Conducting Officer responsible for the Oversight of Delegated Activities	• Fund administration activity report and KPIs	Quarterly Yearly	• Conducting officers • Board of Directors • Conducting officers Board of Directors

		• Results from initial and annual due diligence on fund administration		

Portfolio management	Conducting Officer responsible for the Oversight of Delegated Activities	• Portfolio management activity report • Results from initial and annual due diligence on portfolio managers	Quarterly Yearly	• Conducting officers • Board of Directors
Marketing	Conducting Officer responsible for the Marketing Function	• Fund Distribution activity report (contains new/closed distribution relationships, sale volumes and rebates per distributor and distribution countries)	Quarterly	• Conducting officers • Board of Directors
Accounting & finance (including CSSF quarterly reporting)	Conducting Officer responsible for the Accounting Function	• Review of IFM profitability • Briefing at conducting officers meetings on CSSF reporting production	Quarterly Upon occurrence / Quarterly	• Conducting officers • Board of Directors
Legal services (including fund legal documentation and corporate life of the funds)	Compliance Officer	• Legal activity report	Yearly	• Conducting officers • Board of Directors
IT & infrastructure	Conducting Officer responsible for the Oversight of Delegated Activities	• IT & infrastructure activity report	Yearly	• Conducting officers • Board of Directors

Appendix III –Related actions to fulfil legal & regulatory requirements of the Company

Reference of requirement	Tasks	Person responsible	Frequency/ Date
1.	Establish, implement and maintain decision-making procedures The Conducting Officers and the Compliance Officer are in charge of establishing, implementing and maintaining this decision-making procedure as detailed below.	Conducting Officers Compliance Officer	Annually
1.	Establish, implement and maintain an organizational structure The organizational structure is available in **Appendix I**.	Conducting Officers Compliance function	Annually
1.	Clearly and in a documented manner specify reporting lines and allocate functions and responsibilities Please refer to **Appendix II** for allocation of functions & responsibilities and for related actions to fulfil legal & regulatory requirements.	Conducting Officers Compliance Officer	Annually
1.1.	Ensure compliance with all corporate law requirements regarding the general meeting of shareholders and the Board of Directors of the IFM The IFM has its own domiciliation and corporate secretarial services in charge of such activities and responsible for ensuring that legal requirements in these areas are met.	Compliance function	Ongoing
1.2.2.	Ensure that the Directors are of sufficiently good repute and are sufficiently experienced in relation to the type of fund concerned and the investment strategies pursued by the fund and to this end, communicate the identity of the Directors as well as of every person succeeding them in office the CSSF for approval The documents filed with the CSSF for obtaining relevant licenses demonstrates the repute and experience of the Directors. Any change in Directorship is submitted to the CSSF for prior approval.	N/A Compliance function	N/A Upon occurrence

	The Board of Directors is responsible for assessing the ongoing adequacy of Directors.	Board of Directors	Ongoing
1.2.2.	<u>Ensure that each director of the IFM dedicates the required time and attention to properly perform his duties</u> The documents filed with the CSSF for obtaining relevant licenses lists the number of mandates that each director holds. The Board of Directors is responsible for assessing the ongoing adequacy of Directors.	N/A Board of Directors	N/A Ongoing
1.2.3.1.	<u>Ensure that the Board of Directors of the IFM delegates the day-to-day management and representation of the IFM to at least two conducting officers of the IFM</u> The documents filed with the CSSF for obtaining relevant licenses lists the Conducting Officers (3) who have been approved by the CSSF.	N/A	N/A
1.3.1.	<u>Ensure that the conducting officers are of sufficiently good repute and are sufficiently experienced in relation to the type of fund concerned and the investment strategies pursued by the fund and to this end, communicate the identity of the conducting officers as well as of every person succeeding them in office the CSSF for approval</u> The documents filed with the CSSF for obtaining relevant licenses demonstrates the repute and experience of the Conducting Officers. Any change in conducting officers is submitted to the CSSF for prior approval. The Board of Directors is responsible for assessing the ongoing adequacy of Conducting Officers.	N/A Compliance function Board of Directors	N/A Upon occurrence Ongoing
1.3.1.	<u>Ensure that the conducting officers can be contacted by the CSSF directly and that they can provide all information that the CSSF deems essential for its supervision</u> The Conducting Officers have their domicile in a place that permit them, in principle, to come to Luxembourg every day.	N/A	N/A

1.3.1.	Ensure that the two conducting officers permanently reside in Luxembourg, unless CSSF exemption has been granted to one of the two conducting officers See previous point.	N/A	N/A
1.3.1.	Ensure that the conducting officers form a management committee, the members of which work together in close partnership to take all actions falling within the scope of their responsibilities A Conducting Officers Committee called "Management meeting" is established and meets at least on a monthly basis – Conducting Officers participate to this Committee; they can join by call. The Conducting Officers collaborate on an ongoing basis in a more informal manner.	Conducting Officers	At least monthly / Ongoing
1.3.1.	Ensure that the management committee is responsible to implement the general investment policy, for each managed investment fund, as defined, where relevant, in the constitutive documents of the investment funds The Conducting Officers will receive the reporting which will allow them to make sure that the general investment policy, for each managed investment fund, as defined, where relevant, in the constitutive documents of the investment funds, is correctly implemented.	Conducting Officers	Monthly / Ongoing
1.3.1.	Ensure that the management committee is responsible to ensure that valuation policies and procedures are established and implemented according to the requirements of the law The Conducting Officers will receive the reporting which will allow them to make sure that policies and procedures are established and implemented according to the requirements of the law.	Conducting Officers	Monthly / Ongoing
1.3.1.	Ensure that the management committee is responsible to oversee the approval of investment strategies for each managed investment fund See point above on investment policy.	See above	See above
1.3.1.	Ensure that the management committee is responsible to ensure that the IFM has a permanent and effective compliance function, even if this function is performed by a third party The documents filed with the CSSF for obtaining relevant licenses demonstrates the set-up of the Compliance Function within the IFM. The Conducting Officers are responsible to ensure that the IFM has a permanent and effective compliance function, even if this function is performed by a third party.	N/A Conducting Officers	N/A Monthly / Ongoing
1.3.1.	Ensure that the management committee is responsible to ensure and verify on a periodic basis that the general investment policy, the investment strategies and the risk limits of each managed		

	investment fund are properly and effectively implemented and complied with, even if the risk management function is performed by third parties The Conducting Officers will receive the reporting which will allow them to make sure that the general investment policy, the investment strategies and the risk limits of each managed investment fund are properly and effectively implemented and complied with.	Conducting Officers	Monthly / Ongoing
1.3.1.	Ensure that the management committee is responsible to approve and review on a periodic basis the adequacy of the internal procedures for undertaking investment decisions for each managed investment fund, so as to ensure that such decisions are consistent with the approved investment strategies The Conducting Officers review on a daily basis the fund compliance reports	Conducting Officers	Daily / Ongoing
1.3.1.	Ensure that the management committee is responsible to approve and review on a periodic basis the risk management policy and arrangements, processes and techniques for implementing that policy, including the risk limit system for each managed investment fund The IFM has at its disposal a risk manager as set forth in **Appendix I**. The Conducting Officers review on a monthly basis the fund risk management reports.	Conducting Officers	Monthly / Ongoing
1.3.1.	Ensure that the management committee is responsible to assess and periodically review the effectiveness of the policies, arrangements and procedures put in place to comply with the requirements of the law The Conducting Officers, together with the Head of Compliance, will regularly review the effectiveness of the policies, arrangements and procedures put in place to comply with the requirements of the law.	Conducting Officers Head of Compliance	As appropriate
1.3.1.	Ensure that the management committee is responsible to take appropriate measures to address any deficiencies The Conducting Officers take appropriate measures to address any deficiencies.	Conducting Officers	Monthly / Ongoing
1.3.1.	Ensure that the management committee is responsible to review on a frequent basis, and at least annually, written reports on matters of compliance, internal audit and risk management indicating in particular whether appropriate remedial measures have been taken in the event of any deficiencies The Conducting Officers review on a frequent basis, and at least annually, written reports on matters of compliance, internal audit and risk management indicating in particular whether appropriate remedial measures have been taken in the event of any deficiencies.	Conducting Officers	Annually / more frequently if appropriate

1.3.1.	<u>Ensure that the management committee is responsible to implement strategies and guiding principles for central administration and internal governance through specific written internal policies and procedures</u> The Conducting Officers, together with the Compliance Officer, will regularly review the effectiveness of the policies, arrangements and procedures put in place for proper central administration and internal governance	Conducting Officers Compliance Officer	As appropriate
1.3.1.	<u>Ensure that the management committee is responsible to ensure that the IFM has the technical infrastructure and human resources necessary for performing its activity</u> The documents filed with the CSSF for obtaining relevant licenses detail the technical infrastructure and human resources within the IFM.	N/A	N/A
	The Conducting Officer in charge of these functions is responsible to ensure that the IFM has the technical infrastructure and human resources necessary for performing its activity.	Conducting Officer in charge of IT, nfrastructure and HR	Ongoing
	They will report regularly on their functions to the Management Committee.	Conducting Officers	Annually / When needed
1.3.1.	<u>Ensure that the management committee is responsible to implement and follow-up the marketing policy and the distribution network of investment funds managed by the IFM</u> The Conducting Officer in charge of the marketing function is responsible to implement and follow-up the marketing policy and the distribution network of investment funds managed by the IFM.	Conducting Officer in charge of marketing	Ongoing
	They will report regularly on their functions to the Management Committee.	Conducting Officers	Monthly / When needed
1.3.1.	<u>Ensure that the management committee is responsible to implement adequate internal control mechanisms to secure compliance with decisions and procedures at all levels of the IFM (i.e. the permanent compliance function, the permanent internal audit function and the permanent risk management function)</u>		

	The documents filed with the CSSF for obtaining relevant licenses detail the organization of these functions within the IFM, which can be summarized as follows: (i) internal audit –function delegated to an external service provider; (ii) compliance – full time employee of the IFM and (iii) risk management – full time employee of IFM.	N/A	N/A
	The Conducting Officers in charge of these functions are responsible to ensure that the IFM has the mechanisms in place and human resources necessary for performing these activities. They will report regularly on their functions to the Management Committee.	Conducting Officers in charge of these functions Conducting Officers	Ongoing Monthly / Annually for internal audit
1.3.1.	Ensure that the management committee works in accordance with a method of operation adapted to the activities of the IFM. (e.g. conducting officers are in regular contact with each other and hold periodic meetings; meetings are formalized in minutes, available in the premises of the IFM in Luxembourg; agenda of these periodic meetings includes a discussion on the management information) A Conducting Officers Committee is established and meets on a monthly basis – Conducting Officers participate to this Committee; they can join by call. The Conducting Officers collaborate on an ongoing basis in a more informal manner.	Conducting Officers	Monthly / Ongoing
1.3.1.	Ensure that the management committee informs regularly, completely and in written the Board of Directors of the IFM and the Board of Directors of investment funds managed by the IFM Conducting Officers participate in the IFM and investment funds Board meeting where they report on their activities and findings.	Conducting Officers	Quarterly (IFM) / Semi-Annually (Funds)
1.3.1.	Ensure that the IFM maintains in an adequate and orderly manner records of its activities and its internal organization by setting up the "management information" (permitting the follow-up of its activity and that of its delegates) The Conducting Officers Committees are formalized in minutes, available in the premises of the IFM in Luxembourg including the reports submitted to them for review.	Conducting Officers	Monthly

1.3.1.	Ensure that the IFM receives from the delegates all necessary information in order to affect an efficient control of its delegates The content and the frequency of reports submitted to the IFM by the delegates, which allow for proper control of delegated activities, is regularly challenged.	Relevant staff; Conducting Officers	
1.3.1.	Ensure that the management information is available in Luxembourg and preferably kept in a central database accessible at any time in Luxembourg The management information is available in Luxembourg and is kept in a central database accessible at any time in Luxembourg.	Conducting Officer in charge of infrastructure	Ongoing
1.3.2.	Within the framework of the management committee, ensure that each conducting officer is allocated with specific responsibilities See **Appendix I.**	Board of Directors	Ongoing
1.3.2.	Ensure that it is not allocated to the same conducting officer the functions of risk taking and of independent control of those same risks (i.e. the execution and/or the control of the risk management function and the function of investment management cannot be ensured by the same conducting officer, for instance) See **Appendix I** which shows proper segregation of these functions between the Conducting Officers.	Board of Directors	Ongoing
1.3.2.	In case the conducting officers manage the activity of several management companies, ensure that the exercise of multiple functions by these persons does not prevent or does not potentially prevent to carry out any of their functions suitably, honestly and professionally N/A	N/A	N/A

OPPORTUNITY FUND MANAGEMENT

COMPLIANCE POLICY

The purpose of this Policy is to define the compliance rules and principles to be followed by the Company, as Management Company authorized under Chapter 15 of the Law of 17 December 2010 related to undertakings for collective investment and Alternative Investment Fund Manager as per the law of 12 July 2013.

1. Compliance Principles

At all times, the Company and its employees are required to apply and respect the following principles:

- Engage in and promote business and professional ethical conduct. Ethical rules are defined in the Company's Code of Ethics and Standard of Professional Conduct as well as the Code of Conduct;
- Comply with applicable legislation, internal rules and professional standards;
- Take all reasonable measures to protect confidentiality. Confidentiality and data protection rules are defined in the Confidential Information, Data Protection and Privacy Policies;
- Avoid any conflicts of interest. Conflict of Interest Rules are defined in the Conflict of Interest Policy;
- Protect the Company's assets;
- Protect the Client's best interests

2. Identification of Compliance Risks

Compliance risk is defined as "the risk of losses that an institution may suffer as a result of the failure to conduct its business in accordance with the rules in force".

The main compliance risks are defined, as follows:

Risk of breach of ethical rules

This refers to the risk of breach of ethical rules by the Company or its employees. Ethical rules are defined in the Company's Code of Ethics and Standards of Professional Conduct.
Legal and regulatory risks

This refers to the risk of non-compliance with applicable laws, regulations, and professional practices. This entails:

- Litigation risk: risk linked to the outcome of legal action,
- Contract/transaction risk: risk linked to misinterpretation or non-application of legal rules relevant to a contract or a transaction.
- Legislative risk: risk linked to changes in law and regulations.

Risk of sanctions

This refers to the risk of judiciary, administrative, or disciplinary sanctions, as a result of non-compliance with laws, regulations, rules, norms and/or contractual agreements.

Reputation risk

This refers to the risk of damage due to the Company's diminished worthiness and impaired reputation, resulting from true or false adverse publicity, failures in business practices and failures to comply with current laws and regulations.

Operational risk

This refers to certain aspects of operational risks, originating from or resulting in, one of the above risks.

3. Responsibilities and competencies

Responsibilities of the Board of Directors:

The Board of Directors is responsible for defining the compliance principles to which the Company has to adhere.
It has to demonstrate a clear commitment by ensuring that an appropriate policy is in place and that the compliance risks are managed appropriately and it must:

- Formally approve the Compliance policy set up by the Conducting Officers. The efficiency of implementation of this policy has to be evaluated on an annual basis by means of a status report provided by the Conducting Officers.
- The Board has to ensure that a permanent compliance function is established and authorized to contact the Board of Directors directly, as deemed necessary.

Responsibilities of the Senior Management;

The Senior Management under the ultimate responsibility of the Board of Directors of the Company must implement adequate internal control mechanisms and ensure a permanent and effective compliance function. It shall prepare a Compliance Policy, a Compliance Charter, Rules of Conduct or any additional procedures as necessary to achieve compliance.

The Conducting Officer in charge of the Compliance function shall supervise the compliance function.

The Compliance function will be performed by the Compliance Officer and his/her name has to be communicated to the CSSF as well as subsequent changes.

The responsibilities and the way in which the Compliance function is to operate shall be further laid down in a Compliance Charter.

4. Applicable laws

They include laws, regulation and professional standards related to:

- Laws, regulations and circulars governing access to the financial sector and performance of financial activities;
- The prevention of money laundering and terrorism financing;
- Confidentiality of information/banking secrecy;
- Professional ethics, including the protection of client interest (investor protection, client information, market integrity, etc.);
- Insider trading and market abuse;
- Internal code of conduct fostering an ethical environment, and best practice rules established by professional associations.

CONFIDENTIAL INFORMATION & PRIVACY POLICY

"Confidential Information" includes the following to the extent to which it is not in the public domain:

a) commercially sensitive information of the Company, its clients, suppliers or partners;
b) information relating to the pricing, marketing and strategic objectives of the Company's products;
c) technical information relating to the Company's business and the business of any other company in the Group; and
d) competitive and financial information concerning the business of the Company, its clients, suppliers or partners.

All employees must preserve absolute secrecy with regards to any confidential information, whether written or not, obtained in the course of their employment. This applies to information about clients or Funds, as well as other parties with whom they are dealing and to information about companies, activities, techniques and working practices of the group and in particular the Company; such information may be financial, personal, technical or operational. This also includes not discussing confidential information in public places or with those within the Company who are not entitled to know such information.

The requirement for confidentiality is a continuing obligation which remains in force after an employee has left the group, as detailed further within each employee's contract of employment.

All information obtained during the course of employment which is not generally available must be treated as confidential: it can only be treated as non-confidential if both the client or other Company or person whom it concerns, whether internal or external to the group and particular the Company, and the source from which the information originated have no objection to its disclosure, or the information is publicly available.

Employees of the Company must not disclose or discuss with other employees of the group confidential information relating to the transactions or activities of the Company unless those to whom they disclose such information have a proper need to know it for the purpose of their work. When such information is disclosed to a group employee outside of the Company, whether properly or accidentally, it must not be disclosed any further within the group or externally to the group.

For the avoidance of doubt, these provisions do not apply to information that could reasonably be considered to be in the public domain, or where the information that is disclosed is phrased in a manner that does not identify the information with or associate with any particular person. In addition, further exemptions to this policy exist for information that is disclosed to the CSSF as part of the Company's obligations to assist in the performance of their functions, as well as information that is reported to the appropriate authorities in respect of the detection, investigation or prevention of crime and criminal proceedings.

Employees are reminded of their responsibilities towards the protection of confidential client or fund information, as well as towards insider dealing, which must be strictly complied with at all times as set out in this Handbook.

HEALTH AND SAFETY POLICY

The Luxembourg Regulation on Health and Safety at Work (*Règlement grand-ducal du 4 novembre 1994 concernant les prescriptions minimales de sécurité et de santé pour les lieux de travail*) and the Labour Code require the Company to ensure, so far as is reasonably practicable, the health, safety and welfare at work of all its employees. This duty of care extends to other persons whilst they are on Company premises or affected by Company activities.

The Health and Safety Law also requires each employee to take reasonable care for their own health and safety as well as that of others in the workplace and to co-operate with the Company in respect of obligations imposed by the Health and Safety Law.

It is Company policy to provide and maintain safe and healthy working conditions, equipment and systems of works for all employees and third parties and the Company will do all that is reasonably practicable to prevent personal injury and damage to property.

Responsibility

The Company takes its commitment to health and safety very seriously and it is the responsibility of the Company and individual employees to ensure the Company remains in compliance with its obligations under the Health and Safety Law.

General Policy

The Company recognizes that they have specific duties and statutory requirements which include:

1. the provision and maintenance of premises and systems of work that are, so far as is reasonably practicable, safe and without risks to health;

2. arrangements for ensuring, so far as is reasonably practicable, safety and absence of risks to health, in connection with the use, handling, storage and transport of articles and equipment;

3. the provision of such information, instruction, training and supervision as is necessary to ensure, so far as is reasonably practicable, the health and safety at work of employees;

4. so far as is reasonably practicable as regards any place of work under our control, the maintenance of it in a condition that is safe and without risks to health and the provision and maintenance of means of access to and from it that are safe and without such risks; and

5. the provision and maintenance of a working environment that is, so far as is reasonably practicable, safe, without risks to health, and adequate as regards facilities and arrangements for employees' welfare at work.

To enable the Company to fulfill its duties and responsibilities as an employer, employees have a duty to exercise personal responsibility and to do everything within their power in the course of their employment to prevent ill health to themselves or others, including by:

1. taking reasonable steps to ensure their personal health and safety both in and outside of work and the health and safety of other persons who may be affected by an employee's acts or omissions at work;

2. cooperating with the Company so far as is necessary to enable the Company to fulfill its obligations under the Health and Safety Law;

3. complying with any health and safety instructions, training and/or directions issued by the Company;

4. immediately reporting any potential risk or hazard or malfunction of equipment to the Conducting Officers and

5. immediately reporting any accident suffered on Company premises to the Conducting Officers as soon as is practicable after the event so that details can be recorded in the accident log. All incidents should be reported however trivial they might appear.

MATERNITY / ADOPTION / PARENTAL LEAVE POLICY

All employees should take extra care with regard to health and safety issues at work during their pregnancy. There is some guidance available on the website, https://guichet.public.lu/fr.html.

DISCIPLINARY POLICY

Where informal discussion cannot resolve the matter or is not appropriate (i.e. seriousness of the allegation), formal steps will be taken under this policy.

The Disciplinary Policy provides a framework within which managers can work with employees to maintain satisfactory standards of conduct and encourage improvement where necessary.

The Company seeks to ensure that any disciplinary matter is dealt with fairly and that steps are taken to establish the facts and to give employees the opportunity to respond before any formal action is taken.

- The majority of minor conduct issues can often be dealt with without recourse to formal disciplinary action.
- Matters may be resolved between the employee and their Line Manager or the Senior Management Team.
- Where appropriate a note of any informal discussions will be placed on the employee's personnel file but will not be used for any future disciplinary hearing.
- No disciplinary action will be taken against an employee until a full investigation has been conducted.
- An employee is not normally dismissed for a first act of misconduct, provided it does not amount to gross misconduct, or the employee has not completed their probationary period.

There are 3 stages involved in the Disciplinary Policy.

- Stage 1: First Warning
- Stage 2: Final Warning
- Stage 3: Dismissal

Appeals

If the employee is not satisfied with any decision made under this policy they may appeal, in writing, within 5 working days, to the Head of Legal and Compliance in respect of a first or final warning and to the Managing Director in respect of dismissal. Wherever possible, appeals will be held within 5 working days of the appeal being made and, if conducted by someone previously involved in the case, a disinterested person Executive Director or line manager will be present throughout the proceedings. The appeal hearing will be by way of a review of the previous decision and not a new hearing.

GRIEVANCE POLICY

Grievances are concerns, problems or complaints raised by a staff member with their Line Manager or the Senior Management Team.

The Company recognizes that from time to time an employee may have grievances relating to their employment or relationships with colleagues that they wish to raise. In this respect, the Company encourages communication, initially between employees and their Line Manager, to ensure that questions and problems arising during the course of employment can, wherever possible, be resolved quickly and to the satisfaction of all concerned.

If the employee's grievance relates to their line manager, then the matter should be raised with the Conducting Officers.

Should an employee feel that a grievance is not being resolved satisfactorily in this informal way, they should raise the issue using the Company's formal Grievance Policy.

Should the grievance relate to disciplinary action, this should be progressed through the appeals procedure set out in the Company's Disciplinary Policy.

There is only 1 stage involved in the Grievance Policy and this is for the grievance to be put in writing and submitted to the Head of Legal and Compliance or, if it involves the Head of Legal and Compliance, to another Conducting Officer. Please refer to the Procedure for further information on how to proceed.

Appeals

If the grievance has not been resolved to the employee's satisfaction, an appeal may be made in writing to the Conducing Officer in charge of HR within 5 working days of the date on which the decision was published, stating full grounds for appeal. Wherever possible, appeals will be held within 5 working days of being made and, if conducted by someone previously involved in the case, a disinterested person will also review the case. The employee will be advised in writing, usually within 5 working days of the appeal meeting being held, of the decision. The decision of the person(s) hearing the appeal will be final.

INTERNAL CONTROL

Management and Supervision

Regular staff meetings will be held, and recommendations or issues raised during the meeting will be reported to those responsible.

All payment requests and payment of expenses and invoices by the Company must be reviewed and approved in accordance with the Company's Authorized Signatory List, as updated from time to time. Currency transactions will be checked by at least one authorized signatory prior to placement.

Any errors or breaches identified must be escalated to the Conducting Officer in charge of HR.

Segregation of Duties and Functions

All portfolio or trade information that is distributed externally, together with client reporting, such as weekly and monthly reports and website updates, must be reviewed by one alternative individual other than the preparer prior to issue. Any new material amendments should also be approved by the compliance team prior to release.

Client servicing and marketing individuals should not carry out portfolio operational aspects.

Information Management

Each employee has their own password to gain access to the computer. The password must be changed on a regular basis for security purposes and should not be disclosed to any other individual except for dedicated IT personnel. Disclosure of passwords may be subject to the Company's Disciplinary Policy.

Compliance

The Board of the Company has effective responsibility for compliance with the relevant Licensees Rules as released by the CSSF and the Law, and for the policy on review of compliance. The Board has appointed the Head of Legal and Compliance to be responsible for compliance within the Company and to report directly to the Board on a regular basis. The Head of Legal and Compliance must receive full co-operation from all staff and the appointment must be filled immediately should it become vacant.

Business Continuity and Contingency Plan

All records will be backed up electronically on a daily basis and the backup records will be kept at a secure offsite location for contingency purposes. Further details are included within the dedicated Business Continuity and Contingency Plan.

INFORMATION SECURITY POLICY

The Company takes its responsibilities in respect of Information Security (which includes Data Security and Cyber-Security) seriously. It has an obligation to keep the Data Commissioner informed of matters involving financial crime and other serious operational problems. Any serious or significant incident involving data loss, financial loss or denial of service type attacks, whether actual or prevented should be reported to the Data Commissioner in a timely manner.

It is the duty of all employees to protect information regardless of how it is formatted or processed. The policies and procedures in place serve to counter threats to the Company's data, to protect it from unauthorized access and to maintain confidentiality, integrity and availability of such data. Employees are required to read the Data Protection and Privacy Policy.

Information Security

The Company has identified that weaknesses, which include breaches of data security, client confidentiality provisions and fraudulent activity in the area of data security, expose significant risks, thereby resulting in potentially serious financial and reputational damage to the Company. To assist in mitigating these risks, the following have been implemented and must be adhered to by all employees:

- All devices are password protected;
- Restricted access using a key pad and swipe card to the Company's premises is maintained and an audit trail is reviewed on a periodic basis;
- Adequate supervision of all visitors on-site is performed;
- Filing cabinets and employee drawers are locked at night;
- Where an employee has placed confidential or sensitive information in its drawers, the drawers must be locked at night;
- A clean desk policy is enforced;
- Shredding bins are used for the disposal of confidential information;
- A Remote Desktop Server is in place for all employees to log onto the network securely;
- The Company does not disclose non-public information about its clients to anyone, except as permitted or required by law;
- Detailed procedures and controls are in place to identify and manage the risk of breaches of information security;
- Personal data relating to the Company's employees is maintained on a separate network drive, only accessible by authorized personnel;
- Confidentiality and non-disclosure agreements are put in place where the Company utilizes third parties to undertake certain functions;
- Employee training on measures to prevent, detect and respond to data security and cyber threats, appropriate to the security risks faced, is provided to staff on an annual basis, or more frequently if required.

Clean Desks

The Company takes the protection of data seriously and requires confidentiality across all aspects of the business. By enforcing a Clean Desk Policy, the Company maintains the security of all employee and client information and aims to assist employees with feeling more in control in a well-organized environment which in turn serves to provide a good impression of the Company.

As part of the Clean Desk Policy, all employees should adhere to the following:

- all employees are responsible for protecting documents and data from unauthorized access both internally and from external persons. This includes locking sensitive material away in the cabinets provided and ensuring that no data is left on desks or in unlocked drawers before leaving the office at the end of the day;
- desks should be kept free from paper and clutter as far as practicable;

- when leaving the desk for long periods of time during the day, employees should ensure their PC is locked and any sensitive information which should not be accessible by other employees is locked away. This includes post- it-notes, note pads, etc.;
- sensitive documentation that is no longer required must be placed in the shredding bins.

Outsourced IT Provider

The Company has appointed LAB Group ("LAB") as its IT provider and relies on LAB to define the relative data rules and procedures. However, the Company retains the responsibility for the implementation and periodic review of controls that address the risk of information held for the Company being inappropriately used or stolen, used for the purposes of fraudulent activity or for furthering financial crime and undertakes an annual review to obtain confirmation of the maintenance of controls.

Acceptable Use of IT Facilities

All of the Company's IT facilities and information resources remain the property of the Company and not of particular individuals, teams or departments[2] . This policy has been implemented to ensure IT facilities are used:

- legally;
- securely;
- without undermining the Company;
- effectively;
- in a spirit of co-operation, trust and consideration for others;
- so they remain available.

Internet Use

The internet should be used for business reasons and limited for personal use within hours of work. The Company does not wish to be too restrictive on the use of the internet but employees must ensure that time is not spent browsing the internet for personal use during normal working hours.

Employees must be aware that viruses can be imported and, although anti-virus software is in place, caution must be taken.

Obscenities/Pornography material is strictly prohibited and without restriction must not be written, published, viewed, bookmarked, accessed or downloaded.

Copyright:
Care must be taken to ensure use of software is legal in accordance with both the letter and spirit of relevant licensing and copyright agreements. Copying software for use outside these agreements is illegal and may result in criminal charges.

Security:
The Computer Misuse Act 1990 makes it a criminal offence to obtain unauthorized access to any computer (including workstations and PCs) or to modify its contents. Employees must not attempt to gain unauthorized access to information or facilities. If access to information resources is required, approval from the employee's line manager must be obtained, who in turn will contact the IT service provider if the access is permitted.

[2] In-house software: This is software written by staff or volunteers using the Company's equipment. It is the Company's property and must not be used for any external purpose. Software developers (and students) employed at the Company are permitted to take a small "portfolio" of such in-house software source code/executables, which they may have developed, for use in subsequent work, subject to agreement with the Senior Management Team.

Personal system passwords or other security details must not be disclosed to other staff, volunteers or external agents and employees must not use anyone else's login as this compromises the security of the Company. If an employee is aware of someone else knowing their password, the Head of Legal and Compliance must be advised and the employee must change it immediately[3].

PCs must be locked whilst an employee is away from their desk. It is the employee's responsibility to safeguard their PC and if any misuse occurs, disciplinary measures may apply, depending on severity. External hardware such as CDs / USB sticks must not be used unless authorisation from the Conducting Officer in charge of IT, Bertrand Didier, has been provided and must always be checked for viruses prior to being used on the Company's devices. Computer viruses are capable of destroying the Company's information resources.

Prior to recording or obtaining information about individuals, reference must be made to the Data Protection legislation to ensure adherence to all requirements. Further assistance should be obtained from the Head of Legal Compliance if required.

Electronic monitoring

The monitoring of internet activity can be undertaken by Senior Management without the necessity to obtain prior approval from the employee. However, prior to accessing any other information available within IT facilities for monitoring purposes or otherwise, (e.g. to monitor their working activity, working time, files accessed, reading of their email, files or folders within the S or P drives, etc.) , the employee must be notified of the purpose of the monitoring that could take place. Access without an employee's prior knowledge is not allowed unless:

- in the case of a specific allegation of misconduct, when the Senior Management Team can authorize accessing of such information when investigating the allegation
- when the IT Support section cannot avoid accessing such information whilst fixing a problem.

In such instances, the person concerned will be informed immediately and information will not be disclosed wider than is absolutely necessary. In the former case their access to IT facilities may be disabled pending investigation.

Email Use

Email messages must be written in accordance with Company format and should be thoroughly reviewed and checked for spelling errors prior to their release. Use of personal emails should be limited.

As all email correspondence represents the Company, actions must remain in the interest (and spirit) of the Company and it must not be left open to legal action (e.g. libel). Email has the same authority as any communication and care should be taken to ensure that it is not viewed as an informal means of communication.

Email inboxes should be reviewed by all employees at regular intervals during the working day. Emails should be saved on the network if relevant to other employees.

All electronic correspondence should be archived and kept and should not be deleted if of a business nature. There is not a requirement to keep hard copy paper files unless absolutely necessary.

[3] Personal passwords: Disclosure to other staff, volunteers or external agents:
This may be necessary in some circumstances. Such a practice is allowed only if sanctioned by the Senior Management Team after discussion with IT Support. If the password is disclosed for a one-off task, the employee must ensure that their password is changed (by contacting IT Support) as soon as the task is completed.

Emails should be regarded as published information; they are not confidential and can be read by anyone given sufficient levels of expertise.

Virus Attacks

Emails must only be opened if there is a reasonably good expectation of what it contains e.g. if the email attachment is from "report.doc" (e.g. this is normally shown in the title of the attachment) from an unknown person or an attachment from "explore.zip" from an unknown address, it should not be opened. If emails are received and look likely to be a virus, IT Support and the Head of Legal and Compliance should be advised immediately and warnings to other employees should not be sent by email by forwarding the message.

Email etiquette

Email signatures must be maintained in accordance with the Company procedures on formatting and should be set up automatically for external and internal signatures.

When publishing or transmitting information externally, employees must be aware that they are representing the Company.

The following points should be adhered to:

- If personal opinions are provided, they should be stated as such; Emails should remain constructive and should not be sent in a negative manner.

The person to whom the email is required should be addressed by name at the beginning of the message, especially if another group of people are being copied in. Subject headers should be clear and relevant to the recipient(s).

- Capitals (e.g. NOW) should be used sparingly as they are commonly perceived as 'shouting'.
- Unauthorized or careless use may result in legal action, (e.g., distribution of e-mails which may be offensive to an individual or to a man or woman could lead to sex discrimination claims;
- External e-mails should attach disclaimers.

Consideration should be given as to whether an alternative method of communication is more appropriate, for instance a phone call or meeting.

Use of Distribution Lists

Emails must only be sent to those it is meant for and should not be sent to large groups unless absolutely necessary. Unnecessary (or junk) email reduces computer performance and wastes data storage space.

Purchasing of Hardware/Software

Prior to purchasing hardware and software, approval must be provided by the Conducting Officer in charge of IT, Bertrand Didier.

Permission must be obtained from Head of Operations / IT Support prior to installing software (including public domain software[4]) on equipment owned and/or operated by the Company.

Telephone Use (Including Mobiles)

Personal use of the Company's telephone is permitted for short calls and must not be used for long-distance and toll calls without the permission of the Senior Management Team. Personal calls must be kept to a minimum.

[4] Public domain software or Freeware: This is software that is available free of charge, usually by downloading from the Internet.

To avoid disturbance to work colleagues, mobile phones can be kept on the desk but should be kept on silent/vibrate mode. Where possible, personal calls on a mobile phone should be taken outside of the main office.

Employees are not permitted to use the cameras on their mobile phones to take photographs of computer screens or other sensitive information.

Data transfer and storage on the network

Master copies of important data must be maintained on the Company's network and not on an employee's personal drive to ensure data is available to all staff as permitted.

Files which are accessible centrally should not be kept in an employee's personal drive unless there a good reason for doing so (i.e. you intend to amend them or you need to reference them and the central copies are to be changed or deleted) since this uses up data storage space unnecessarily.

Computer Server

The Company's computer server and storage hardware is located at Details of Labgroup, which has the following protection measures:

- Lightning protection
- Moisture detection
- Very early smoke detection
- Floor and ceiling fire suppression
- Power protection
- Internet connectivity resilience
- Building security protection

Personal Devices

References to the word "device" below include, but are not limited to, Android mobile phones, Windows mobile phones, any other smartphones, iPhones, iPads, tablets and laptops.

The use of a personal device in connection with the Company's business is a privilege granted to employees through approval of the Senior Management Team. The Company reserves the right to revoke these privileges in the event that users do not abide by the policies set out below.

The following policies are aimed to protect the integrity of the Company data and to ensure it remains safe and secure under the Company's control. Please note that there may be limited exceptions to these policies owing to device limitations between vendors.

Employees with personal devices must adhere to all terms and conditions in this policy to be allowed access to those Company services.

- Irrespective of security precautions mentioned here, employees are expected to use their device in an ethical manner.
- Access to data must lock itself with a PIN (personal identification number set by the employee).
- If left idle, the employee's device must automatically activate its PIN after a maximum time-out period of 5 minutes.
- In the event of loss or theft of the employee's device, the employee must inform the Company immediately.
- An employee's device may be remotely wiped if: (i) the employee loses the device; (ii) the employee terminates employment with the Company; (iii) the IT section detects a data or policy breach or virus; or (iv) if the employee incorrectly types their password 10 consecutive times.

- An employee's device may allow for only the remote wipe of the Company data.
- This means an employee's personal data is still vulnerable, and thus it is recommended for the employee to also set a device password and take additional security precautions.

Tampering
An employee using their device in ways not designed or intended by the manufacturer is not allowed. This includes, but is not limited to, 'jailbreaking' or 'rooting' a device.

Liability
A personal device can be connected to the Company infrastructure or services, but the employee is personally liable for their device and carrier service costs. Employees with personal devices are not eligible (except by prior agreement) for reimbursement of expenses for hardware or carrier services.

Access
Employees that purchase a device on their own that is not in line with the Company's standard approved device lists may not be able to or allowed to have their devices added to the Company's servers. It is highly recommended that the employee refers to the Company IT support to review approved devices. An employee's personal device is not permitted to connect to the Company infrastructure without documented consent from the Senior Management Team and the Company IT support. Furthermore, the Company reserves the right to disable or disconnect some or all services without prior notification.

Disclaimer
The Company hereby acknowledges that the use of a personal device in connection with the Company business carries specific risks for which the employee assumes full responsibility for reporting any incidents to the Senior Management Team. These risks include, but are not limited to, the partial or complete loss of data as a result of a crash of the operating system, errors, bugs, viruses, downloaded malware, and/or other software or hardware failures, or programming errors which could render a device inoperable.

Reporting Line to the Board

A clear reporting line has been established for information security incidents relating to a data privacy breach. Should any incidents occur, the Conducting Officer in charge of compliance must be notified without delay and will raise any material issues with the Board immediately or, if not material, will include in the Compliance Report provided to the Board on a quarterly basis.

OPPORTUNITY FUND MANAGEMENT

GIFTS AND ENTERTAINMENT POLICY

Offers of gifts and entertainment are common practice among business partners. However, offering or accepting gifts, entertainment or other benefits can be mistaken for improper payments. For this reason, all employees must not give or accept gifts, gratuities, favors or benefits if their value is reasonably believed to go beyond what could reasonably be considered as ethical and accepted business practices, or which may influence or appear to be influenced by the performance of their duties.

Usual business hospitality which is not of an excessive nature (for example: lunches, dinners, invitation to a sport event or similar) can be accepted by Directors and Employees during the course of business should they not exceed a maximum value of Euro 250 or currency equivalent.

Any gift or entertainment which costs in excess of Euro 250 or currency equivalent requires prior approval by the Conducting Officer in charge of compliance. Employees are required to complete the Form for Reporting of Gifts and Entertainment (**Appendix 2**). Directors are required to declare their hospitality at the subsequent Board meeting if it is above the aforementioned maximum amount.

The receipt or giving of cash gifts of any value is strictly prohibited.

Overriding principles

There are a number overriding principles defined below where any gift or hospitality must:

- not be made with the intention of influencing a third party or employee to obtain or retain business or a business advantage, or to reward the provision or retention of business or a business advantage, or in explicit or implicit exchange for favors or benefits;
- comply with local law;
- be given in the name of the organization, not in an individual's name;
- not include cash or a cash equivalent;
- be appropriate in the circumstances;
- be of an appropriate type and value and given at an appropriate time taking into account the reason for the gift;
- be given openly, not secretly;
- in any event, not be offered to, or accepted from, government officials or representatives, or politicians or political parties, without the prior approval of the Company's Head of Legal and Compliance.

The Company appreciates that the practice of giving business gifts varies between jurisdictions and regions and what may be normal and acceptable in one region may not be in another. The test to be applied is whether in all the circumstances the gift or hospitality is reasonable and justifiable. The intention behind the gift should always be considered.

What is not acceptable?

It is not acceptable for employees (or someone on their behalf) to:

- give, promise to give, or offer, a payment, gift or hospitality with the expectation or hope that a business advantage will be received, or to reward a business advantage already given;
- give, promise to give, or offer, a payment, gift or hospitality to a government official, agent or representative to "facilitate" or expedite a routine procedure;
- accept payment from a third party where it is known or suspected that it is offered with the expectation that it will obtain a business advantage for them;
- accept a gift or hospitality from a third party where it is known or suspected that it is offered or provided with an expectation that a business advantage will be provided by the Company in return;

- threaten or retaliate against another employee who has refused to commit a bribery offence or who has raised concerns under this policy;
- engage in any activity that might lead to a breach of this or any relative Company policy.

WHISTLEBLOWING POLICY

Whistleblowing is the disclosure by an employee of the Company of activities which indicate that regulatory misconduct in the form of one or more of the "failures" listed below may have taken place or is being, or likely to be, committed:

- potential regulatory violations
- accounting, internal accounting controls or auditing matters
- a danger to the health and safety of an individual
- market about or insider trading
- breach of (client) confidentiality or privacy
- theft
- fraud
- bribery or corruption
- deliberate covering up of information tending to show any of the above

The Company guarantees several rights, including protection from retaliation, for an employee who reports a concern in good faith, who provides information, who causes information to be provided or who otherwise assists in an investigation and who respects the confidentiality of the matter. It is immaterial whether the relevant failure took place overseas, or where the law applying to the relevant failure was not in the Grand Duchy of Luxembourg.

The Company will treat any activity which results in one of these failures being committed very seriously. There may be serious repercussions for any employee who is involved in any such failing, and also against the Company from an external body, such as the CSSF.

Internal Disclosures

On becoming aware that there has been, there is, or there is likely to be a failure as outlined above, it must be reported to the Senior Management Team and notified to the Company's Head of Legal and Compliance.

The Head of Legal and Compliance must immediately report any disclosure received to the Board of the Company (taking into consideration any members of the Board that have been identified as possibly being involved). All disclosures will be investigated fully and appropriate action will be taken.

The Company will act against any person willfully making false or malicious allegations. Otherwise, any individual making a disclosure in accordance with these procedures will be supported by the Company, and the matter may be dealt with confidentially if they so wish.

Consideration will be given to the ways in which the Company's procedures could be improved and strengthened in order to prevent the reoccurrence of such offences or breaches.

External Disclosures[5]

If the employee making the disclosure does not believe that the matter has been dealt with efficiently and adequately or believes that they are unable to report the matter internally they may seek to make an external disclosure. The whistleblower must have reasonable grounds to believe that the information and any allegations it contains are substantially true. He/she may also provide hard evidence by attaching documents to the whistleblowing report.

[5] www-cssf.lu

Before contacting the CSSF, employees of entities of the financial sector are requested to first use the whistleblowing procedures in their workplace, if there are any.

The CSSF will, in principle, only consider a written statement of information transmitted by e-mail to the following address: whistleblowing@cssf.lu If this is not possible, the employee may call Mr Marc Limpach, head of the legal department JUR-CE during office hours before transmitting a written statement. The telephone number of the departmental secretariat is: +352 26251 2757 (Ms Stéphanie Theis).

It should be noted that the CSSF is committed to protecting the whistleblower's identity within the limits of the applicable legislation. Neither the identity of the employee having blown the whistle, nor the identity of third parties who may be involved, will be disclosed to the entity concerned. The identity of the whistleblower or of third parties will only be disclosed in circumstances in which the disclosure becomes unavoidable in law (e.g. as a result of the CSSF's duty to inform the State prosecutor if the acts may constitute a crime or an offence, or in the context of criminal proceedings against the entity concerned in which case the whistleblower may, as the case may be, be called as a witness). Although it may perhaps not always be entirely excluded, despite all the precautions taken, that the employer may discover the whistleblower's identity by cross-checking information, the CSSF will make every effort to protect it. The CSSF does not audio record whistleblowing telephone calls.

Callers may be asked to provide their name and contact details but if they prefer they can remain anonymous. All information provided through the whistleblowing line will be assessed for consideration of further action. If further action is taken, a caller's details still remain confidential and no reference made to the fact that information has been received via the whistleblowing line.

A whistleblowing telephone line has been introduced by the CSSF to assist callers in reporting such information. **Whistleblowing line: +352 26 25 1 27 57** (please refer to the CSSF website for further details: https://whistleblowing.apps.cssf.lu/index.html?language=en). During normal working hours calls will be answered by a member of the CSSF. In their absence and outside of normal working hours, the line will revert to voicemail which will only be accessible to members of that team.

TRAINING AND COMPETENCY POLICY

Introduction

The Company operates in a specialist area within the Grand Duchy of Luxembourg market, and is pro-active in offering full training and support to continue to develop individuals to ensure that they are suitably aware of the business situation as well as having the correct skill set for their specific role. The Company adopts a culture that supports high standards of conduct and ethical behavior within the organisation, placing an emphasis on continued learning and development to enhance the training and knowledge of its employees, all of which are required to have knowledge of the professional and legal obligations they owe to the Company in the spirit and the letter of both their contract of employment and the Policies and Procedures in place within the Company.

This Policy has been enforced to implement and maintain quality standards through the provision of learning and development, appropriate to the nature and scale of the Company's business.

Performance Appraisal

To assess and monitor each individual employee's competence in their respective role, the Company undertakes a performance appraisal (the "appraisal) on at least an annual basis (or shorter periods as required) which incorporates a review of their individual performance and also in the context of their approach to the ethical considerations and standard of professional conduct adopted by the Company.

The formal appraisal process assesses and monitors ongoing competencies for each employee and monitors their progress, identifying training needs where required.

Training reviews

Review of training requirements should be undertaken at the outset of employment, as part of the appraisal process and on an ongoing basis.

The Company is responsible for evaluating the quality and effectiveness of training provided.

Fitness and Probity

All directors and employees of the Company are required to be adequate, fit and proper, competent, suitably experienced for the role that they undertake and have a track record of displaying soundness of judgment for fulfilling their role before being permitted to act on behalf of the Company.

New Employees

The Company's first priority for training and development is to ensure all new employees have the necessary skills and general understanding to perform the role for which they have been recruited. During the recruitment process, an initial assessment of a new employee's level of competence should be made so that the Company can identify any gaps in knowledge and potential areas for development.

Prior to a new employee becoming actively involved in day-to-day operations, on commencement of employment, new employees are required to complete the following:

- Chartered Institute for Securities & Investment's ("CISI") Integrity Matters test. An online integrity test designed to highlight dilemmas that may be faced within the workplace. It enables users to test their ability to make ethical decisions. However, if you have previously taken this test we will accept a copy of your certificate. A Procedure is available with instructions on how to proceed.
- Anti-Money Laundering Training for Financial Services Offshore – An online training programme and awareness test covering Anti-Money Laundering and the responsibilities on all staff under the latest legislation. A Procedure is available with instructions on how to proceed.

Existing Employees

It is the individual employee's responsibility to meet the obligations identified as part of the Training and Competency Policy and to highlight any additional requirements for training that have been omitted from the reviews and to ensure the training is carried out in a timely manner.

Ongoing: All employees must identify and receive comprehensive ongoing training to ensure competence for the duties undertaken in their role. Employees are required to focus on the broader development of their role and their career with the Company and to consider their eligibility for professional qualifications to support their personal and career development within the organisation. All employees must undertake Anti-Money Laundering Training on an annual basis.

Change of role: The Company's priority for training and development is to ensure newly promoted employees have the necessary skills and general understanding to perform the role for which they have been promoted.

Supervision

The Company is required to ensure that employees tasked with the responsibility of providing training and/or oversight to other colleagues have the necessary coaching and assessment skills and the appropriate technical knowledge and experience to undertake such supervision. The level of supervision should be in accordance with the specific employees' requirements and relative to experience, length within the role, etc.

Reporting to the Board

The Board of the Company is responsible for employee training. Sufficient management information should be provided to the Board on a periodic basis (the Company considers this to be on a half–yearly basis or more frequent if required) to enable the Board to effectively monitor and oversee the performance of their employees.

Support

To support the commitment to the development of the Company's employees, different methods of training and development have been identified:

- **On-the-job Training**

This type of training is provided at the place of work whilst an employee is undertaking the role. An experienced employee will serve as the trainer and provide the trainee with the required knowledge and technical expertise as required to fulfill their obligations. This will include coaching and support.

- **In-house Training**

  - Cross training – to cover another member of the team's duties
  - Self-learning - reading/research online
  - Documentation provided by colleagues (e.g. new regulations, email announcements, etc.)
  - Attendance at team meetings
  - Shadowing colleagues

- **External Training**

  - Training organizations – controlled learning events
  - Workshops
  - Lunch and Learns
  - Seminars
  - Webinars
  - Professional Studies – see the Qualifications Table (**Appendix 1**).

OPPORTUNITY FUND MANAGEMENT

DATA PROTECTION AND PRIVACY POLICY

The Company needs to collect personal information to effectively and compliantly carry out its everyday business functions and activities and to provide its products and services. Such data is collected from employees, clients and service providers and includes (but is not limited to), name, address, email address, date of birth, identification numbers, private and confidential information and sensitive information.

In addition, the Company may be required to collect and use certain types of personal information to comply with the requirements of the law and/or regulations, however the Company is committed to collecting, processing, storing and destroying all information in accordance with the General Data Protection Regulation (GDPR) (EU) 2016/679. In January 2012, the European Commission proposed a new regulation to bring a standard and consistent approach to the processing and sharing of personal information across the European Union. The General Data Protection Regulation ("GDPR") was approved by the European Commission in April 2016 and applies from 25 May 2018, centralising regulation across the 28 Member States of the European Union (EU) and updating data protection for the digital age. Any organisation processing personal data of data subjects in the EU will also need to comply with the GDPR.

The Company has developed policies, procedures, controls and measures to ensure maximum and continued compliance with the GDPR and its principles, including staff training, procedures, documents, audit measures and assessments. Ensuring and maintaining the security and safety of personal data belonging to the individuals with whom we deal is paramount to our ethos and the Company adheres to the GDPR and associated principles in its processes and functions.

The Company aims to be proactive not reactive in terms of data protection and in assessing changes and their impact from the start and designing systems and processes to protect personal information is at the core of our business.

BACKGROUND

The aims of the GDPR are to:

- give data subjects an increased level of control over their information – where data is being processed on the basis of consent, the data subject's consent now needs to be explicit;
- improve the protection of personal data by ensuring that data controllers and processors are safe custodians of data by promoting behavioral change;
- provide for enhanced oversight and supervision by increasing the powers of the regulators;
- the right to be forgotten – a data subject has the right to erase personal data that is incorrect or no longer relevant, including withdrawing consent;
- data portability – a data subject can request the transfer of their personal data.

PURPOSE

The purpose of this policy is to ensure that the Company is meeting its legal, statutory and regulatory requirements under the GDPR and to ensure that all personal data is safe, secure and processed compliantly whilst in use and/or being stored and shared by the Company. The Company is dedicated

to ensuring its compliance with the GDPR principles and understands the importance of making personal data safe within the organisation.

The GDPR includes provisions that promote accountability and governance and as such the Company has put comprehensive and effective governance measures in place to meet these provisions. The aim of such measures is to ultimately minimise the risk of breaches and uphold the protection of personal data.

SCOPE

The scope of the policy is to create a framework to ensure that staff deals with personal data in accordance with legal, regulatory, contractual and business expectations and requirements.

DUTIES AND PRINCIPLES OF PROCESSING

Article 5 of the GDPR requires that personal data shall be:

a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency').
b) collected for specified, explicit and legitimate purposes and not further processed in a manner incompatible with the purpose for which it was collected; further processing for archiving purposes, in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation').
c) adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed ('data minimisation').
d) accurate and, where applicable, kept up to date and reasonable steps must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which it is processed and is erased or corrected without delay ('accuracy').
e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed; personal data may be stored longer to the extent necessary for a historical or scientific purpose ('storage limitation').
f) processed in a manner that ensures its security appropriately, including protecting it against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

Article 5(2) requires that 'the controller shall be responsible for, and be able to demonstrate, compliance with GDPR principles' noted above ('accountability') in accordance with section 6(2)(g) and shows how it complies with the principles, detailing and summarizing the measures and controls that it has in place to protect personal information and mitigate the risks of processing such personal information.

OBJECTIVES

We are committed to the GDPR and its principles, along with associated regulations and/or codes of conduct laid down by the Supervisory Authority and local law. We are dedicated to ensuring the safe, secure, ethical and transparent use of all personal data and to upholding the highest standards of data processing.

The Company has set out below the objectives to meet the regulatory requirements of the GDPR and has developed measures, procedures and controls for maintaining and ensuring compliance.

The Company ensures that:

- the rights of individuals are protected with regards to the personal information known and held about them by the Company in the course of its business;

- it develops, implements and maintains a data protection policy, audit plan and training program for compliance with the GDPR;
- business practices, tasks and processes carried out by the Company are monitored for compliance with the GDPR and its principles;
- data is only obtained, processed or stored when it has met the lawfulness of processing requirements;
- it records consent at the time it is obtained and can evidence such consent to the Commissioner if requested to do so;
- clients feel secure when providing the Company with personal information and know that it will be handled in accordance with their rights under the GDPR;
- it maintains a continuous program of monitoring, review and improvement with regards to compliance with the GDPR and aims to identify gaps and non-compliance before they become a risk;
- it monitors the Commissioners and the GDPR updates, to stay abreast of updates, notifications and additional requirements;
- it has robust and recorded Complaints Handling and Breach Incident controls and has procedures in place for identifying, investigating, reviewing and reporting any breaches or complaints with regards to data protection;
- it has appointed the Head of Legal and Compliance who takes responsibility for the overall supervision and implementation of GDPR and its principles and remains informed on the regulations and how they relate to the Company;
- it has a dedicated audit and monitoring programme in place to perform regular checks and assessments on how the personal data the Company processes is obtained, used, stored and shared. The audit and monitoring programme utilises this policy and the GDPR itself to ensure continued compliance;
- it provides clear lines of reporting and supervision with regards to data protection compliance;
- it develops and maintains strict and robust data protection procedures and controls to ensure continued compliance with data protection law;
- it stores and destroys all personal information, in accordance with the GDPR timeframes and requirements;
- any information provided to an individual in relation to personal data held or used about them, will be provided in a concise, transparent, intelligible and easily accessible form, using clear and plain language;
- employees are made aware of their own rights under the GDPR through direct internal written notifications, together with training.

GOVERNANCE PROCEDURES

Accountability & Compliance

Due to the nature, scope, context and purpose of processing undertaken by the Company, it carries out risk assessments and information audits to identify, assess, measure and monitor the impact of such processing. We have also implemented adequate and appropriate technical and organizational measures to ensure the safeguarding of personal data and compliance with the GDPR and any codes of conduct that we have obligations under.

The Company processes activities are performed in accordance with the GDPR and that we have in place robust policies, procedures, measurers and controls for the protection of data. The Company operates a transparent workplace and works diligently to maintain and promote a comprehensive and proportionate governance program.

The Company's main governance objectives are to:

- educate its staff about the requirements under the GDPR and the possible impact of non-compliance;
- provide a dedicated and effective data protection training program for all staff;
- identify key senior stakeholders to support the data protection compliance program;
- allocate responsibility for data protection compliance and ensure that the Responsible Officer has sufficient access, support and budget to perform the role;
- identify, create and disseminate the reporting lines within the data protection governance structure.

The technical and organizational measures that the Company has in place to ensure and demonstrate compliance with the data protection laws, regulations and codes of conduct are detailed in this document and associated policies. These measures include:

- Data Protection and Privacy Policy
- Data Breach Policy and procedure
- Information Technology Policy and Procedures
- Outsourcing Policy & Due Diligence Procedures
- Clean Desk Policy
- Business Continuity Plan

We assume also that no Data Protection Impact Assessment (DPIA) is required as the Company do not process any sensitive data. In case a DPIA may be required in the future, we will use the DPIA checklist available for this purpose.

PRIVACY BY DESIGN

The Company operates a *'Privacy by Design'* approach and ethos, with the aim of mitigating the risks associated with processing personal data through prevention via the Company's processes, systems and activities. The Company has additional measures in place to adhere to this ethos, including:

Data Minimization

Under Article 5 of the GDPR, principle (c) advises that data should be *'limited to what is necessary'*, which forms the basis of our minimal approach. The Company only ever obtains, retains, processes and shares the data that is essential to carry out its services and legal obligations and will only keep it for as long as is necessary.

The Company's systems, employees, processes and activities are designed to limit the collection of personal information to that which is directly relevant and necessary to accomplish the specified purpose. Data minimization enables the Company to reduce data protection risks and supports its compliance with the GDPR.

Measures to ensure that only the necessary data is collected includes:

- electronic collection (*ie forms, website, etc.*) only have the fields that are relevant to the purpose of collection and subsequent processing. The Company does not include 'optional' fields, as optional denotes that it is not necessary to obtain;
- agreements with third parties (either in the Company's capacity as a controller or processor).

These agreements state that only relevant and necessary data is to be provided as it relates to the processing activity carried out;

- having documented destruction procedures in place where a data subject or third-party provides the Company with personal information that is surplus to requirement.

HARD COPY DATA

Due to the nature of its business, it is sometimes essential for the Company to obtain, process and share personal information which is only available in a paper format without pseudonymisation (copies of passports, proof of address, etc.). Where this is necessary, the Company utilizes a tiered approach to minimize the information it holds and/or the length of time that it holds it for:

- where the Company is the data controller, it will obtain a copy of the data and if applicable redact to ensure that only the relevant information remains (ie when the data is being passed to a third-party for processing and not directly to the data subject);
- when only mandatory information is visible on the hard copy data, the Company utilizes electronic formats to send the information to the recipient. The documents are password protected;
- recipients (i.e. the data subject, third-party-processors) are re-verified and their identity and contact details checked;
- the Responsible Officer authorizes the transfer and checks the file(s) attached;
- once confirmation has been obtained that the recipient has received the personal information, where possible (within the legal guidelines and rules of the GDPR), the Company destroys the hard copy data.

INFORMATION AUDIT

To enable the Company to fully prepare for and comply with the GDPR, the Company has carried out a company-wide data protection information assessment to better enable the Company to record, categories and protect the personal data that the Company holds and processes.

The audit has identified, categorized and recorded all personal information obtained, processed and shared by the Company in its capacity as a controller / processor and has been compiled on a central register which includes:

- what personal data the Company holds;
- where it came from;
- where it is held;
- who the Company shares it with;
- legal basis for processing it;
- what format(s) it is in;
- who is responsible for it;
- disclosures and transfers.

LEGAL BASIS FOR PROCESSING

At the core of all personal information processing activities undertaken by the Company, is the assurance and verification that the Company is complying with Article 6 of the GDPR and its lawfulness of processing obligations.

This legal basis is documented in the Company's information flow register and where applicable, is provided to the data subject (and the Commissioner, upon request) as part of its information disclosure obligations. Data is only obtained, processed or stored when the Company has met the lawfulness of processing requirements where:

- the data subject has given consent to the processing of their personal data for one or more specific purposes;
- 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 Company is subject;
- processing is necessary in order to protect the vital interest 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 Company;
- processing is necessary for the purposes of the legitimate interests pursued by the Company or by a third party (except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, eg where the data subject is a child).

RECORDS OF PROCESSING ACTIVITIES

As an organization with less than 250 employees, the Company maintains records of all processing activities where:

- processing personal data could result in a risk to the rights and freedoms of the individual;
- the processing is not occasional;
- it processes special categories of data;
- such records are maintained in writing, are provided in a clear and easy to read format and are readily available to the Commissioner, upon request.

DATA RETENTION AND DISPOSAL

The Company has defined procedures for adhering to the retention periods as set out by the relevant legal and regulatory requirements, as well as adhering to the GDPR requirement to only hold and process personal information for as long as is necessary. All personal data is disposed of in a way that protects the rights and privacy of data subjects (e.g. shredding, disposal as confidential waste, secure electronic deletion) and prioritizes the protection of personal data at all times.

Please refer to the Company's Data Retention Policy for full details of the retention, storage periods and destruction processes.

DATA SUBJECT RIGHTS PROCEDURES

Consent and the Right to be Informed

The collection of personal data is a fundamental part of the services offered by the Company. Specific measures and controls are in place to ensure that the Company complies with the conditions for consent under the GDPR.

The GDPR defines consent as 'any 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'.

Where processing is based on consent, the Company has reviewed and revised all consent mechanisms

to ensure that:

- consent requests are transparent, using plain language and are void of any illegible terms, jargon or extensive legal terms;
- it is freely given, specific and informed, as well as being an unambiguous indication of the individual's wishes;
- consent is always given by a statement or a clear affirmative action (positive opt-in) which signifies agreement to the processing of personal data;
- consent mechanisms are upfront, clear, granular (in fine detail) and easy to use and understand;
- pre-ticked, opt-in boxes are **never** used;
- where consent is given as part of other matters (ie terms and conditions, agreements, contracts) the Company ensures that the consent is separate from the other matters and is not a precondition of any service (unless necessary for that service);
- consent is always verifiable and the Company has controls in place to ensure that it can demonstrate consent;
- the Company keeps detailed records of consent and can evidence at a minimum:
  - that the individual has consented to use and processing of their personal data;
  - that the individual has been advised of the Company and any third party using the data;
  - what the individual was told at the time of consent;
  - how and when consent was obtained.

- the Company has ensured that withdrawing consent is as easy, clear and straightforward as giving it and is available through multiple options, including:
  - unsubscribe links in mailings or electronic communications;
  - opt-out process explanation and steps on the website via its privacy notice;
  - ability to opt-out in writing or by email.

- consent withdrawal requests are processed immediately and without detriment.

CONSENT CONTROLS

The Company maintains rigid records of data subject consent for processing personal data and is always able to demonstrate that the data subject has consented to the processing of his or her personal data where applicable. The Company also ensures that the withdrawal of consent is as clear, simple and transparent as it is to give consent.

Where the data subject's consent is given in the content of a written declaration which also concerns other matters, the request for consent is presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. All such written declarations are reviewed and authorized by the Responsible Officer or equivalent senior person prior to being circulated.

Consent to obtain, process, store and share (where applicable) is obtained in writing through:

- In writing
- Email
- Electronic (i.e. via website form)

Electronic consent is always by a non-ticked, opt-in action, enabling the individual to provide consent,

after the below information has been provided. This is then followed up with an email or written confirmation of the consent process. Privacy Notices are used in all forms of consent and personal data collection, to ensure that we are compliant in disclosing the information required in the GDPR in an easy to read and accessible format. Our privacy notice can be accessed via www.ericsturdza.lu.

ALTERNATIVES TO CONSENT

The Company recognises that there are six lawful bases for processing and that consent is not always the most appropriate option. We have reviewed all processing activities and only use consent as an option where the individual has a choice.

When reviewing the processing activity for compliance with the consent requirements, we ensure that none of the below are factors:

- Where we ask for consent, but would still process it even if it was not given (or withdrawn). If we would still process the data under an alternative lawful basis regardless of consent, we recognize it is not the correct lawful basis to use;
- Where we ask for consent to process personal data as a precondition of a service we are offering, it is not given as an option and consent is not appropriate;
- Where there is an imbalance in the relationship, i.e. with employees.

INFORMATION PROVISIONS

Where personal data is obtained directly from the individual (i.e. through consent, by written materials and/or electronic formats (i.e. website forms, subscriptions, email, etc.)), we provide the below information in all instances, in the form of a privacy notice:

- the identity and the contact details of the controller and, where applicable, of the controller's representative;
- the contract details of the Responsible Officer;
- the purpose(s) of the processing for which the personal information is intended;
- the legal basis for the processing;
- where the processing is based on Article 6(1) *"processing is necessary for the purposes of the legitimate interests of the controller or a third party"*, details of the legitimate interests;
- the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;
- the existence of the right to request access to and rectification or erasure of, personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability;
- where the processing is based on consent under points (a) of Article 6(1) or Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;
- the right to lodge a complaint with the Supervisory Authority.

The above information is provided to the data subject at the time the information is collected and records pertaining to the consent obtained are maintained and stored for 6 years from the end of the relationship, unless there is a legal requirement or legitimate interest to keep the information for longer, subject to balancing the legitimate interest against the individual's interests, rights and freedoms.

PRIVACY POLICY & NOTICES

Privacy Policy

The Company recognizes the differences between a Privacy Policy and Privacy Notice and ensures that we meet the regulatory, legal and best practice requirements for both formats. For the purposes of this document, we use the terms Privacy Policy to provide the business, its clients, service providers, staff and associated entities with our operational and organizational approach to protecting data and complying with the GDPR and any relevant data protection laws.

This document is our Data Protection and Privacy Policy and includes how we comply with GDPR principles, the manner in which we process data, guidelines and procedures for ensuring that data subject can exercise their rights and our approach to data protection by design and default. This policy provides details on how we apply the principles, what procedures we follow in compliance with the Regulation and any specific individual and/or departmental responsibilities, including those of the Responsible Officer (RO) and is fundamentally used as an internal reference document.

Our Privacy Notice is also available on our website, which also includes details about the cookies used on our site.

PRIVACY NOTICE

Our Privacy Notice is separate from our Data Protection and Privacy Policy and is provided to individuals at the time we collect their personal data (or at the earliest possibility where that data is obtained indirectly). Our Privacy Notice provides individuals with all the necessary and legal information about how, why and when we process their data, along with their rights and obligations.

Our Privacy Notice is designed to be a public declaration of how the Company applies the data protection principles to data that we process. It is provided to all individuals whose data we process (ie clients, employees, third parties, etc.) and contains only the information specific to the individual and as required by law. The notice is easily accessible, legible, jargon free and is available in several formats, dependent on the method of data collection:

- Via our website;
- Linked to or written in full in the footer of emails;
- Via employee written communications and recruitment materials.

Where we rely on consent to obtain and process personal information, we ensure that it is:

- Displayed clearly and prominently;
- Asks individuals to positively consent;
- Gives them sufficient information to make an informed choice;
- Explains the different ways we will use their information;
- Provides a clear and simple way for them to indicate they agree to different types of processing;
- Includes a separate unticked consent box for direct marketing.

PERSONAL DATA NOT OBTAINED FROM THE DATA SUBJECT

Where the Company obtains and/or processes personal data that has **not** been obtained directly from the data subject, the Company ensures that the information (if requested by the data subject) is

provided within 30 days of receipt of a request (except for advising if the personal data is a statutory or contractual requirement).

In addition to the information provided to the data subject, we also provide information about:

- the categories of personal data;
- the source the personal data originated from and whether it came from publicly accessible sources.

Where the personal data is to be used for communication with the data subject, or a disclosure to another recipient is envisaged, the information will be provided at the latest, at the time of the first communication of disclosure. Where the Company intends to further process any personal data for a purpose ***other*** than that for which it was originally obtained, we communicate this intention to the data subject prior to doing so and where applicable, process only with their consent.

Whilst we follow best practice in the provision of the information noted in the section of this policy headed Information Provisions, we reserve the right not to provide the data subject with the information if:

- they already have it and we can evidence their prior receipt of the information;
- the provision of such information proves impossible and/or would involve a disproportionate effort;
- obtaining or disclosure is expressly laid down by legislation to which our Company is subject and which provides appropriate measures to protect the data subject's legitimate interest;
- where the personal data must remain confidential subject to an obligation of professional secrecy regulated by Member State law, including a statutory obligation of secrecy.

EMPLOYEE PERSONAL DATA

As per the GDPR guidelines, we do not use consent as a legal basis for obtaining or processing employee personal information. Our HR policies have been updated to ensure that employees are provided with the appropriate information disclosure and are aware of how we process their data and why, together with information about their rights under the GDPR and how to exercise those rights.

RIGHT OF ACCESS

We have ensured that appropriate measures have been taken to provide information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 (collectively, The Rights of Data Subjects), relating to processing of the data subject in a concise, transparent, intelligible and easily accessible form using clear and plain language.

Such information is provided free of charge and is in writing, or by other means where authorized by the data subject and with prior verification as to the subject's identity (i.e. verbally, electronic).

Information is provided to the data subject at the earliest convenience, but at a maximum of 30 days from the date the request is received. Where the retrieval or provision of information is particularly complex or is subject to a valid delay, the period may be extended by two further months where necessary. However, this is only done in exceptional circumstances and the data subject is kept informed in writing throughout the retrieval process of any delays or reasons for delay.

Where we do not comply with a request for data provision, the data subject is informed within 30 days

of the reason(s) for the refusal and of their right to lodge a complaint with the Supervisory Authority.

SUBJECT ACCESS REQUEST

Where a data subject asks us to confirm whether we hold and process personal data concerning him or her and requests access to such data, we provide them with:

- the purposes of the processing;
- the categories of personal data concerned;
- The recipients or categories of recipient to whom the personal data have been or will be disclosed;
- if the data has or will be disclosed to a third country or international organization and the appropriate safeguards pursuant to the transfer;
- Where possible, the envisaged period for which the personal data will be stored,
- the existence of the right to request rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;
- the right to lodge a complaint with the Supervisory Authority;
- where personal data has not been collected by the Company from the data subject, any available information as to the source and provider;
- the existence of automated decision-making, including profiling and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

Subject Access Requests should be notified to the Responsible Officer as soon as received and a record of the request is noted. The type of personal data held about the individual is checked against our information audit to see what format it is held in, who else it has been shared with and any specific timeframes for access.

Subject Access Requests will normally be completed within 30 days and are provided free of charge. Where the individual makes the request by electronic means, we provide the information in a commonly used electronic format, unless an alternative format is requested.

Where we receive a Subject Access Request, the below process is followed:

- A letter or request must be dealt with promptly and usually within 30 days of receipt.

- The initial action of the member of staff will be to acknowledge to the client receipt of the request and to start a log detailing what action has been taken. The initial acknowledgement letter may include the request for further information. The member of staff should locate as much of the information as possible before forwarding the information request to the Head of Legal and Compliance.

- Where a client has asked for further information, then the 30 days will start when the information has been satisfactorily collated and circulated to the Responsible Officer, subject to any exemptions. This is why it is important to maintain the log. We will keep the client informed of progress.

- In certain circumstances there may be exemptions from any obligation to provide individuals with details of personal information about them which we have processed. An example would be a request to provide any Suspicious Transaction Reports.

- Once the client's Subject Access Request and all the information that we need to process the request has been supplied, the letter or request and the log shall be passed to the Head of Legal and Compliance to make sure that the request does not fall into the exception categories.

- The Compliance Team will then establish if any of the client information is covered by the exception categories, advise the member of staff accordingly and return to that member of staff the letter of request and the log suitably endorsed.

- The member of staff will then copy from the Company's files all the required information and submit these documents with a covering letter, the letter of request and the log to the Conducting Officers for approval.

- The package should be sent to the client by registered mail.

- The log and original letter of request and copy of the documents sent to the client should be passed to the Head of Legal and Compliance where they will be held in a central register for future reference.

DATA PORTABILITY

The Company provides all personal information pertaining to the data subject to them on request and in a format that is easy to disclose and read. We ensure that we comply with the data portability rights of individuals by ensuring that all personal data is readily available and is in a structured, commonly used and machine-readable format, enabling data subjects to obtain and re-use their personal data for their own purposes across different services.

We use the below formats for the machine-readable data:

- HTML
- CSV
- Word

All requests for information to be provided to the data subject or a designated controller are undertaken free of charge and within 30 days of the request being received. If for any reason, we do not act in responding to a request, we provide a full, written explanation within 30 days to the data subject or designated controller of the reasons for refusal and of their right to complain to the Supervisory Authority and to a judicial remedy.

All transmission requests under the portability right are assessed to ensure that no other data subject is concerned. Where the personal data relates to more individuals than the subject requesting the data/transmission to another controller, this is always without prejudice to the rights and freedoms of the other data subjects.

RECTIFICATION AND ERASURE

Correcting Inaccurate or Incomplete Data

Pursuant to Article 5(d) of the GDPR, all data held and processed by our Company is reviewed and verified as being accurate wherever possible and is always kept up to date. Where inconsistences are identified and/or where the data subject or designated controller informs us that the data we hold is inaccurate, we take every reasonable step to ensure that such inaccuracies are corrected with

immediate effect.

The Responsible Officer is notified of the data subject's or the data controller's requests to update personal data and is responsible for validating the information and rectifying errors where they have been notified. The information is altered as directed by the data subject or the data controller, with the information audit being checked to ensure that all data relating to the subject is updated where incomplete or inaccurate. Once updated, we add an addendum or supplementary statement where applicable.

Where notified of inaccurate data by the data subject or the data controller, we will rectify the error within 30 days and inform any third party of the rectification if we have disclosed the personal data in question to them. The data subject is informed in writing of the correction and where applicable, is provided with the details of any third party to whom the data has been disclosed.

If for any reason, we are unable to act in response to a request for rectification and/or completion, we always provide a written explanation to the requestor and inform them of their right to complain to the Authority and to a judicial remedy.

RIGHT TO ERASURE

Also known as *'The Right to be Forgotten'*, the Company complies fully with Article 5(e) and ensures that personal data which identifies a data subject, is not kept longer than is necessary for the purposes for which the personal data is processed. All personal data obtained and processed by the Company is categorized when assessed by the information audit and is either given an erasure date or is monitored so that it can be destroyed when no longer necessary.

These measures enable us to comply with a data subject's right to erasure, whereby an individual can request the deletion or removal of personal data where there is no compelling reason for its continued processing. Whilst our standard procedures already remove data that is no longer necessary, we will still follow a dedicated process for erasure requests to ensure that all rights are complied with and that no data has been retained for longer than is needed.

Where we receive a request to erase and/or remove personal information from a data subject, the below process if followed:

1. The request is allocated to the Responsible Officer and recorded on the Erasure Request Register.

2. The Responsible Officer locates all personal information relating to the data subject and reviews it to see if it is still being processed and is still necessary for the legal basis and purpose it was originally intended.

3. The request is reviewed to ensure it complies with one or more of the grounds for erasure:

    a. the personal data is no longer necessary in relation to the purposes for which it was collected or otherwise processed;
    b. the data subject has withdrawn consent on which the processing is based and where there is no other legal ground for the processing;
    c. the data subject objects to the processing and there are no overriding legitimate grounds for the processing;
    d. the personal data has been unlawfully processed;

e. the personal data must be erased for compliance with a legal obligation.

4. If the erasure request complies with one of the above grounds, it is erased within 30 days of the request being received.

5. The Responsible Officer writes to the data subject and notifies them in writing that the right to erasure has been granted and provides details of the information erased and the date of erasure.

6. Where the Company has made any of the personal data public and erasure is granted, we will take every reasonable step and measure to remove public references, links and copies of data and to contact related controllers and/or processors and inform them of the data subjects requests to erase such personal data.

If for any reason, we are unable to act in response to a request for erasure, we always provide a written explanation to the individual and inform them of their right to complain to the Supervisory Authority and to a judicial remedy. ***Such refusals to erase data include:***

- Exercising the right of freedom of expression and information.
- Compliance with a legal obligation or the performance of a task carried out in the public interest.
- For reasons of public interest in the area of public health.
- For the establishment, exercise or defense of legal claims.

RIGHT TO RESTRICT PROCESSING

There are certain circumstances where the Company restricts the processing of personal information, to validate, verify or comply with a legal requirement of a data subject's request. Restricted data is removed from the normal flow of information and is recorded as being restricted on the information audit. Any account and/or system related to the data subject of restricted data are updated to notify users of the restriction category and reason. When data is restricted it is only stored and not processed in any way.

The Company will apply restrictions to data processing in the following circumstances:

- Where an individual contests the accuracy of the personal data and we are in the process of verifying the accuracy of the personal data and/or making corrections.
- Where an individual has objected to the processing (where it was necessary for the performance of a public interest task or purpose of legitimate interests), and we are considering whether we have legitimate grounds to override those of the individual.
- When processing is deemed to have been unlawful, but the data subject requests restriction as oppose to erasure.
- Where we no longer need the personal data, but the data subject requires the data to establish, exercise or defend a legal claim.

The Responsible Officer reviews and authorises all restriction requests and actions and retains copies of notifications from and to data subjects and relevant third parties. Where data is restricted, and we have disclosed such data to a third party, we will inform the third party of the restriction in place and the reason and re-inform them if any such restriction is lifted.

Data subjects who have requested restriction of data are informed within 30 days of the restriction

application and are also advised of any third party to whom the data has been disclosed. We also provide in writing to the data subject, any decision to leave a restriction on processing. If for any reason, we are unable to act in response to a request for restriction, we always provide a written explanation to the individual and inform them of their right to complain to the Supervisory Authority and to a judicial remedy.

OBJECTIONS AND AUTOMATED DECISION MAKING

Data subjects are informed of their right to object to processing in our Privacy Notices and at the point of first communication, in a clear and legible form and separate from other information. We provide opt-out options on all direct marketing material and provide an "unsubscribe" form where processing is carried out on line. **Individuals have the right to object to:**

- Processing of their personal information based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling).
- Direct marketing (including profiling).

Where the Company processes personal data for the performance of a legal task, in relation to our legitimate interests or for research purposes, a data subject's objection will only be considered where it is on 'grounds relating to their particular situation'. We reserve the right to continue processing such personal data where:

- we can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual;
- the processing is for the establishment, exercise or defense of legal claims.

Where we are processing personal information for direct marketing purposes under a previously obtained consent, we will stop processing such personal data immediately where an objection is received from the data subject. This measure is absolute, free of charge and is always adhered to.

Where a data subject objects to data processing on valid grounds, the Company will cease the processing for that purpose and advise the data subject of cessation in writing within 30 days of the objection being received.

OVERSIGHT PROCEDURES

Security and Breach Management

Alongside our "Privacy by Design" approach to protecting data, we ensure the maximum security of data that is processed, including as a priority, when it is shared, disclosed and transferred. Our Information Security Policy and Procedures provide the detailed measures and controls that we take to protect personal information and to ensure its security from consent to disposal.

We carry out information audits to ensure that all personal data held and processed by us is accounted for and recorded, alongside risk assessments to the scope and impact a data breach could have on data subject(s). We have implemented adequate and appropriate technical and organizational measures to ensure a level of security appropriate to the risk.

Whilst every effort and measure is taken to reduce the risk of data breaches, the Company has dedicated controls and procedures in place for such situations, along with the notifications to be made to the Commissioner and data subjects (where applicable).

Please refer to our Data Breach Policy and Procedures for specific protocols.

INFORMATION SECURITY POLICY AND PROCEDURE

The Company takes its responsibilities in respect of Information Security (which includes Data Security and Cyber-Security) seriously. It has an obligation to keep the National Data Protection Commission ("NDPC") informed of matters involving financial crime and other serious operational problems. Any serious or significant incident involving data loss, financial loss or denial of service type attacks, whether actual or prevented should be reported to the Security Officer in a timely manner.

It is the duty of all employees to protect information regardless of how it is formatted or processed. The policies and procedures in place serve to counter threats to the Company's data, to protect it from unauthorized access and to maintain confidentiality, integrity and availability of such data.

Information Security

The Company has identified weaknesses that could result in breaches of data security; client confidentiality provisions and fraudulent activity in the area of data security expose significant risks thereby resulting in potentially serious financial and reputational damage to the Company. To assist in mitigating these risks, the following have been implemented and must be adhered to by all employees:

- All devices are password protected in accordance with the Company's password policy;
- Restricted access using a key pad and swipe card to the Company's premises is maintained and an audit trail is reviewed on a periodic basis;
- Adequate supervision of all visitors on-site is performed;
- Filing cabinets and employee drawers are locked at night and keys are kept in a key safe with number lock;
- A clean desk policy is enforced;
- Shredding bins are used for the disposal of client data;
- A Remote Desktop Server is in place for all employees to log onto the network securely;
- The Company does not disclose non-public information about its clients to anyone, except as permitted or required by law;
- Detailed procedures and controls are in place to identify and manage the risk of breaches of information security;
- Personal data relating to the Company's employees is maintained on a separate network drive, only accessible by authorized personnel;
- Confidentiality and non-disclosure agreements are put in place where the Company utilizes third parties to undertake certain functions;
- Employee training on measures to prevent, detect and respond to data security and cyber threats, appropriate to the security risks faced, is provided to staff on an annual basis, or more frequently if required.

To monitor and test the information security processes put in place by the Company, the following have also been undertaken:

- Review of Cyber Security Measures by Labgroup following change of IT Service Providers

PASSWORDS

Passwords are a key part of protection strategy and are used through the Company to secure information and restrict access to systems. We use a multi-tiered approach which includes password at user, device, system and network levels to ensure a thorough and encompassing approach. Whilst

passwords are also directly related to information security and access control, the Company recognizes that strong, effective and robust password controls and measures are imperative to the protection and security of personal information.

Passwords afford a high level of protection to resources and data and are mandatory requirements for all employees and/or third parties requiring access to any resource that requires a password.

RESTRICTED ACCESS AND CLEAN DESK POLICY

The Company may on occasion and at its discretion, place all or part of its files onto a secure computer network with restricted access to all/some personnel data. When implemented, access to personal information will only be granted to the person / department that has a specific and legitimate purpose for accessing and using such information.

The Company operates a zero-tolerance clean desk policy and does not permit personal data to be left unattended on desks or in meeting rooms, or in visible formats, such as unlocked computer screens or on fax machines, printers, etc. Access to areas where personal information is stored (both electronic and physical) is on a restricted access basis with secure controlled access functions throughout the building. Only staff authorised to access data or secure areas can do so. All personal and confidential information in hard copy is stored safely and securely.

TRANSFERS AND DATA SHARING

The Company takes proportionate and effective measures to protect personal data held and processed by us at all times, however we recognize the high-risk nature of disclosing and transferring personal data and as such, place an even higher priority on the protection and security of data being transferred. Data transfers within the UK and EU are deemed less of a risk than a third country or an international organization, due to the GDPR covering the former and the strict regulations applicable to all EU Member States.

All data being transferred is recorded so that tracking is easily available and authorization is accessible. We only conduct transfers of personal data where there are adequate levels of protection in place. Such transfers are reviewed by the Responsible Officer. The Company only transfers personal data outside of the EEA if data transfer agreements are in place satisfying data transfer requirements under data protection law.

Appropriate Safeguards

The Company restricts transfer of personal data to those that are legally binding or essential for the provision of our business obligations or in the best interest of the data subject. In such instances, we develop and implement appropriate measures and safeguards to protect the data, during the transfer and for the duration it is processed and/or stored in a third country or international organization.

Such measures include ensuring that the rights of data subjects can be carried out and enforced and those effective legal remedies for data subjects are available.

Transfer Exceptions

The Company does not transfer any personal information to an organization without obtaining authorization from the Supervisory Authority and the appropriate safeguarding measures; unless one of the below conditions applies. ***The transfer is:***

- made with the explicit consent of the data subject, after having been informed of the possible risks and the absence of an adequacy decision and appropriate safeguards;
- necessary for the performance of a contract between the data subject and the Company or the implementation of pre-contractual measures taken at the data subject's request;
- necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the Company and another natural or legal person;
- necessary for important reasons of public interest;
- necessary for the establishment, exercise or defense of legal claims;
- necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent;
- made to a jurisdiction providing equivalent protection of personal data.

Where the above transfer must take place for legal and/or legitimate reasons and the conditions above have not been satisfied, the Supervisory Authority is notified of the transfer and the safeguards in place, prior to it taking place. The data subject in such instances is provided with all information disclosures pursuant to Article 13 and 14, as well as being informed of the transfer, the legitimate interests pursued, and the safeguards utilized to affect the transfer.

AUDITS AND MONITORING

This policy contains measures and methods used by the Company to protect personal data, uphold the rights of data subjects, mitigate risks, minimize breaches and comply with the GDPR and associated laws and codes of conduct. In addition to these, we also carry out regular audits and compliance monitoring processes with a view to ensuring that the measures and controls in place to protect data subjects and their information are adequate, effective and compliant at all times.

The Responsible Officer has overall responsibility for assessing, testing, reviewing and improving the processes, measures and controls in place and reporting improvement action plans to the Senior Management where applicable. Data minimization methods are frequently reviewed and new technologies assessed to ensure that we are protecting data and individuals to the best of our ability.

All reviews, audits and ongoing monitoring processes are recorded by the Responsible Officer and copies provided to Senior Management and are made readily available to the Supervisory Authority where requested.

The aim of internal data protection audits is to:

- ensure that the appropriate policies and procedures are in place;
- verify that those policies and procedures are being followed;
- test the adequacy and effectiveness of the measures and controls in place;
- detect breaches or potential breaches of compliance;
- identify risks and assess the mitigation actions in place to minimize such risks;
- recommend solutions and actions plans to Senior Management for improvements in protecting data subjects and safeguarding their personal data;
- monitor compliance with GDPR and demonstrate best practice.

TRAINING

Through our strong commitment and robust controls, we ensure that all staff understand, have access to and can easily interpret the data protection requirements and its principles and that staff have

ongoing training, support and data protection requirements. Staff are required to undertake annual training from a compliance perspective to understand the risks to the organization (both financial and reputation) as well as the risk to themselves and the care they need to take in handling personal data, why there are certain policies and procedures in place and most importantly of all why they need to comply with those policies.

PENALTIES

The Company understands its obligations and responsibilities under the GDPR and comprehends the severity of any breaches under the GDPR. We respect the Supervisory Authority's authorization under the legislation to impose and enforce fines and penalties where we breach the GDPR, fail to mitigate the risks where possible and operate in a knowingly non-compliant manner.

DEFINITIONS:

"Supervisory Authority" means the National Commission for Data Protection or in French, *"Commission Nationale pour la Protection des Données"* - https://cnpd.public.lu/en.html.

"Commissioner" means the Data Commissioner appointed by the Supervisor Authority.

"consent" of the data subject means 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 a person that, alone or jointly with others determines the purposes and means of the processing of any personal data, and for the avoidance of doubt, includes a processor or any other person, where the processor or other person determines the purposes and means of processing personal data.

"controller's representative" means a person designated by the controller in writing.

"data subject" means the identified or identifiable individual to whom the personal data relates.

"the GDPR" means 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.

"personal data" means any information relating to an identified or identifiable individual.

"processor" means an individual or other person that processes personal data on behalf of a controller and includes a secondary processor within the meaning of the GDPR.

"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, together with further or continued processing of personal data and profiling

"profiling" means any form of automated processing or personal data consisting of the use of personal data to evaluate certain personal aspects relating to an individual, including aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements.

"recipient" means any person to which the personal data is disclosed, but excludes any public authority receiving the personal data in the context of the exercise or performance of its functions with any enactment.

"Responsible Officer" means an individual designated responsible for overseeing data protection strategy and implementation to ensure compliance with the GDPR requirements.

"third party" means a person other than the data subject, controller or processor or a person who, under the direct authority of the controller or processor is authorised to process personal data.

APPENDIX 1 - QUALIFICATIONS TABLE

This table is not intended to be a comprehensive list of all qualifications and all training available but is more of a guide to the recommended level of qualifications.

	LEVEL			
FUNCTIONS	**Administrator**		**Management**	
Compliance	ICA International Advanced Certificate in Compliance ACAMS	4	ICA International Diploma in Governance, Risk and Compliance ACAMS	6
Finance / Accounting	CIMA Certificate in Business Accounting ACCA - Foundations in Accounting - FA1 Recording Financial Transactions	4 4	ACCA – Chartered Certified Accountant CIMA Advanced Diploma in Management Accounting CIMA: Chartered Management Accounting CFA: Chartered Financial Analyst	6 6 6 6
Financial Advisers[6]	Refer to the Commission's "Table of Acceptable Qualifications for Financial Advisers"[7]		Refer to the Commission's "Table of Acceptable Qualifications for Financial Advisers"[8]	
Marketing	CIM Level 3 Introductory Certificate in Marketing CIM Level 4 Certificate in Professional Marketing	3 4	CIM Level 6 Professional Diploma in Marketing	6
Operations	ICSA Certificate in Offshore Finance and Administration (COFA)	4	ICSA Diploma in Offshore Finance and Administration (COFA)	6
Risk	CISI Risk in Financial Services Qualification	3	ICA International Diploma in Governance, Risk and Compliance, Professional Risk Manager (PRM™) Designation (graduate level), Financial Risk Manager (FRM), Chartered Financial Analyst (CFA).	6
Trading	CFA Investment Management Certificate CISI's Capital Markets Programme	3 3	CISI Investment Advice Diploma[9]	6

	GENERAL
LEADERSHIP & MANAGEMENT	CMI Level 3 Certificate in First Line Management CMI Level 5 Certificate in Management and Leadership
DIRECTORS	Level 6 IOD Company Direction Programme
SPECIFIC	Salesforce Bloomberg
ALL	AML Training – level specific to role Integrity Matters Cyber Security Awareness Training GDPR Compliant and Data Protection Training Microsoft Office Suite (Excel, Word, Outlook, PowerPoint, Visio, etc.)

[6].

[7] [www.cssf.lu website details dealing with Investment/Pages/Training-and-Competence.aspx

[8] [www/cssf.lu website details dealing with Investment/Pages/Training-and-Competence.aspx

[9] http://www.cisi.org/bookmark/genericform.aspx?form=29848780&URL=investmentadvicedipl

APPENDIX 2 - FORM FOR REPORTING OF GIFTS OR ENTERTAINMENT

In accordance with the Gifts Policy issued by Opportunity Fund Management, all employees are required to disclose the gifts or inducements received or given by them with a monetary value over Euro 250. Cash gifts of any value are not permitted.

Name of Employee receiving/giving* the Gift/Entertainment
Name of recipient (if giving the Gift/Entertainment)[10]
Nature of Gift/Entertainment
Business Reason for Gift / Entertainment[11]
Date of Receipt /provision of Gift/Entertainment
Estimated Value (report only if it is in excess of Euro 250)

***Delete as appropriate**

Requested by:	**Authorised by:**
Signature:	Signature:
Name:	Name:
Date:	Date:

[10] The gift may be given in the name of the organisation or the name of an individual (as appropriate).

[11] The gift must not be made with the intention of influencing a Third Party or Employee to obtain or retain business or a business advantage, or to reward the provision or retention of business or a business advantage, or in explicit or implicit exchange for favours or benefits

APPENDIX 3 - NEW JOINER / ANNUAL DECLARATION FORM

NAME:		JOINING DATE:	

By completing this form, I confirm that I have read, understood and agree to adhere to, all regulatory policies applicable to me as referred to in Opportunity Fund Management's AML and Anti-Bribery Manual (the "manuals") and all content in the Employee Handbook. I understand and agree that the policies and procedures described in the manuals and the Employee Handbook (as amended from time to time) form part of an integral part of my contract of employment and failure to observe or adhere to them may constitute misconduct and may render me liable to disciplinary proceedings, including the cessation of my employment.

I understand and acknowledge that a number of the policies may require me to make disclosures to the Compliance Officer on an on-going basis. I confirm that the policies detailed below have been provided to the Compliance Officer on commencement of employment (as applicable), and I have no further matters to disclose.

- Personal (Staff) Dealing*
- Outside Business Interests e.g. other employment, directorships

In addition, by completing and returning this New Joiner Declaration, I confirm that I am aware of my responsibilities under the relevant legislation for the following and have disclosed/will disclose any suspicions as required:

- Anti-Money Laundering Legislation
- Bribery and Corruption legislation

Continuing Professional Development ("CPD")

I am a member of a Professional Body as detailed below and am required to complete the stated number of hours. I can confirm that I am personally responsible to ensure completion of the required number of hours and report to the Compliance Officer on an annual basis.

Name of Professional Body:		Membership Number:	
CPD hours required per annum:		CPD hours already obtained for the current year:	

SIGNATURE		DATE:	

*Confirmation of all holdings and brokerage/investment accounts must accompany this form by completion of the Staff Dealing Reporting Form.