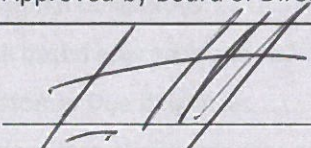
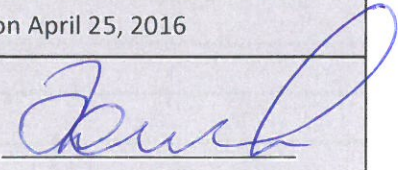


ANTI-MONEY LAUNDERING /
FIGHT AGAINST TERRORISM / ANTI
CORRUPTION / WHISTLE BLOWER POLICY
and
KNOW YOUR CUSTOMER POLICY
Alfa Asset Management (Europe) S.A.
2015 – 2016

Approved by Board of Directors at the meeting on April 25, 2016


Sandi Nemet
Authorised Manager


Egor Zhelezov
Authorised Manager

Contents

1	1. Introduction	4
1.1	Preamble.....	4
1.2	Scope of application.....	4
1.3	Acronyms	4
2	background	5
2.1	Definitions.....	5
2.1.1	Money laundering.....	5
2.1.2	Predicated offense	5
2.1.3	Terrorism financing.....	6
2.1.4	Act of corruption.....	6
2.1.5	Ultimate Beneficial Owner (UBO)	6
2.1.6	Politically exposed person (PEP)	7
2.1.7	Shell bank.....	7
2.1.8	Risk based approach	7
2.1.9	Risk assessment:	7
2.1.10	Equivalent jurisdiction.....	7
3	Relevant rules and regulations.....	7
3.1	Current rules and regulations include (but are not limited to):	8
3.1.1	European Directives and regulations:.....	8
3.1.2	Luxembourg Laws and regulations:.....	8
3.1.3	Applicable CSSF circulars (and amendments):.....	8
3.1.4	Financial Action Task Force (FATF) statements and their respective application in Luxembourg,	9
4	Personal responsibility:	9
5	Professional obligations:	10
5.1	Risk based approach and risk analysis.....	10
5.2	Customer Due diligence:.....	11
5.2.1	Performance, timing, updating and documenting of Customer Due Diligence (CDD).....	11
5.2.2	Performance of CDD	11
5.2.3	Timing of CDD	12
5.2.4	Updating CDD	13
5.2.5	Documenting CDD.....	13
5.3	Monitoring of clients	13
5.3.1	Complex operations or unusual / suspicious activities	14
5.3.2	AML/CTF blacklists, sanctions, control and PEP lists	14
5.4	Prohibited and refused relationships	15
6	Cooperation with authorities.....	15

7	Whistle blower policy:.....	16
8	Internal and external controls and audit	17
9	Ongoing training, recruitment and awareness	17
9.1	AAME employees and collaborators are required to participate to ongoing training programs related to AML/CTF.....	17
9.2	Recruitment.....	18
10	Update and approval of the procedure:	18
11	Document retention policy	18
12	Appointment of officers:.....	19

1 1. Introduction

1.1 Preamble

This internal AML/FT policy and procedure is part of the Action Plan for Financial Sector Professionals ("PSF") under Luxembourg law against money laundering, counter corruption and the financing of terrorism whose purpose is to raise awareness for all shareholders, directors, staff, contractors, sub-contractors and external consultants working on behalf and for the account of the company Alfa Asset Management (Europe) S.A. (hereinafter "AAME") and to the extent necessary, any member of any subsidiaries or branches AAME.

Foreseen the dynamic regulatory environment of Luxembourg and the enlarged scope of compliance, the present procedure aims to create awareness, safeguard the reputation of Alfa Asset Management (Europe) S.A. (AAME) and to protect the firm as well as the persons of contact from the risk of being used for money laundering, for terrorist financing or for the completion of corrupt acts.

Being AAME a supervised entity by Luxembourg' Commission of Surveillance of the Financial Sector (CSSF), policies and procedures are in place and in effect with the objective to ensure that the relevant customer due diligence measures are correctly and completely applied as well as to specify the professional diligences to be performed by AAME, its subsidiaries and entities under its control, as well as staff in such entities and relevant staff from third parties when acting as representatives of AAME in bases of legal contracts and/or agreements.

In addition to the legal and regulatory obligations which bound AAME, its shareholders, its directors and its employees, AAME has strong ethical values which enforce as compliance culture in the working environment and in every relation in which AAME is involved.

1.2 Scope of application

The procedure and policy set herein are part of the working contracts of every employee of AAME and will include the scope of every AML/CTF legal duties (customer due diligence, AML/CTF/KYC risk analysis, client acceptance, on-going monitoring, PEP/blacklist screening, training, cooperation with the financial intelligence unit and other authorities), as well as related duties imposed by rules and regulations to AAME.

1.3 Acronyms in use

The following list of Acronyms aims to guide the reader all through the document.

AAME = Alfa Asset Management (Europe) S.A. and staff members

AML = Anti-Money Laundering

AMLRO = AML Reporting Officer

CAC = Client Acceptance Committee

CCRO or CCO: Chief Compliance and Risk Officer

CDD = Customer Due Diligence

CSSF Commission of Surveillance of the Financial Sector in Luxembourg

CTF = Counter Terrorism Financing

EDD = Enhanced Due Diligence

FATF = Financial Action Task Force

FIU = Financial Intelligence Unit (Luxembourg responsible authority for the fight against ML/TF, "cellule de renseignement financier du parquet")

ML = Money Laundering

PEP = Politically Exposed Person(s)

TF = Terrorism Financing

SDD = Standard Due Diligence

RPFC = Responsible person for compliance within the Board of Directors

RDD = Reduced Due Diligence

UBO = Ultimate Beneficial Owner (as defined in relevant AML/CTF legislation)

2 Background

2.1 Definitions

2.1.1 Money laundering

We understand money laundering as the processing of criminal proceeds with the aim of disguising or concealing their illicit origin.

The illicit origin of the assets must be sourced in a primary offence recognised as such by the law in order to be considered as money laundering.

The above-referred process is commonly conducted in 3 stages:

- Placement: act of inserting the assets into the financial system.
- Layering: series of operations meant to difficult the tracking of the origin of the funds (various movements of accounts or various selling of financial instruments).
- Integration: act of reinsertion of assets into the economy by acquisition of products or services.

AAME staff if committing or participating in money laundering when they have:

- Knowingly facilitated by any means, the false justification of the origin of the goods forming the object or product, whether direct or indirect, or constituting a pecuniary advantage derived from any one or more of the primary offenses;
- Knowingly assisted in an investment transaction, concealment or conversion of property forming the subject or the direct or indirect product of primary offenses or constituting a pecuniary advantage derived from one or more of these offenses;
- Acquired, held or used the goods forming the subject or the direct or indirect product or constituting any financial benefit derived from one or more primary offenses, knowing, at the time they received, that it came from a relevant offense or participation in one or more of them.

Similar appreciation of the conduct is taken to those who negligently appear to be willingly blind to any of the actions herein taking place.

2.1.2 Predicated offense

List of crimes, felonies or misdemeanours which local laws consider as source of proceeds which integration to the economy are money laundering.

Some example of such violations are (non-exhaustive list):

- Forgery of currency and products
- Violation of the environment legislation
- Murders and grave physical harm
- Kidnapping, unlawful detention and hostage taking
- Trafficking of stolen goods

- Trafficking of migrants
- Forgery
- Extortion
- Smuggling
- Breaches of fiduciary trust, fraudulent bankruptcy and swindling
- Insider trading and market manipulation
- Public and private corruption
- Crimes and offences with criminal conspiracy
- Abduction of minors
- Sexual exploitation of minors
- Pimping
- Drug trafficking
- Offences of terrorism and terrorist financing
- Frauds against financial interests of the State and international institutions
- Violation of legislation on weapons and ammunition
- Tax related crimes as defined by local legislation, when applicable.

2.1.3 Terrorism financing

In legislative terms, “financing terrorism” designates any act defined under Article 135-5 of the Penal Code. In other terms, terrorism financing can be defined as the action of voluntarily directing assets to support or facilitate planning, preparation or/and execution of acts of terrorism.

In practical terms, TF is the use of resource, independently of their origin, to facilitate, promote, cooperate or somehow make possible the perpetration of acts of terror or the dissemination of an ideology of terror.

Whenever a suspicion of potential financing of terrorism arise, the AMLRO should be informed immediately for further actions.

2.1.4 Act of corruption

An act of corruption or a corrupted act makes reference to any action committed by a public or a private person in order to obtain an unfair advantage or illegitimate profit or position by utilising economic means, influence (or access to a person of influence) or force.

The corrupt act does not necessarily need to obtain the unlawful advantage or create unfair conditions.

In summary corruption consist in a behaviour where a person offers or is solicited, approved or received, promises, gifts or presents, for the purpose of performing or refraining from any act of obtaining favours or specific benefits. Corruption is said to be passive when coming from the corrupt, it is called active when it is the fact of the briber.

2.1.5 Ultimate Beneficial Owner (UBO)

Natural person(s) who ultimately own(s) or control(s) the customer and/or the natural person(s) on whose behalf a transaction or activity is being conducted.

The concept of Ultimate Beneficial Owner has three basic aspects to be taken into consideration and the holder of any of such aspects is to be considered as UBO and shall complete this declaration.

- a. **Ownership:** Legally possess, directly or indirectly, the right of property (or partially possess such rights) over the assets, goods, valuables, royalties, rights or any other comprised in the specific relationship.
- b. **Benefit:** Be able to claim or be the ultimate person who profits (or partially benefits) from the assets, rights, good, values royalties or rights or their proceeds.
- c. **Control:** Be granted by right or agreement with the possibility of deciding over the utilisation, assignment or some sort of disposition over the assets, goods, valuables, royalties, rights or any other comprised is the specific relationship.

2.1.6 Politically exposed person (PEP)

“Politically exposed person(s)” refer to natural persons who are or have been entrusted with prominent public functions (and immediate family members or persons known to be close associates of such persons) and who are acting outside of the frame of the entrusted duties applicable to such functions.

The relevant regulations include some examples of such functions and the relationship which will provide them the status of PEP or close associate.

For further details on the treatment of structures involving a PEP and the identification of PEP, please contact the AMLRO.

2.1.7 Shell bank

“Shell bank” means a bank that has no physical presence in the country in which it is incorporated and licensed, and which is unaffiliated with a regulated financial group that is subject to effective consolidated supervision.

Physical presence means meaningful mind and management located within a country. The existence simply of a local agent or low level staff does not constitute physical presence.

2.1.8 Risk based approach

The Risk based approach refers to the decision to apply a specific rule to a situation as a result of an assessment of the potential risk involved in the same and considering the obligations imposed by rules and regulations applicable at the time of such assessment.

2.1.9 Risk assessment:

A risk assessment is the collection and analysis of relevant data in order to produce an objective profile of a person, entity, jurisdiction, product or situation, with the aim of understanding the risk involved in the relationship.

The scope of a risk assessment is limited to the type of risk that such assessment explicitly mentions to have taken into consideration.

2.1.10 Equivalent jurisdiction

An equivalent jurisdiction is a jurisdiction considered as having AML/CTF laws and regulations similar in their content to the ones contained in the relevant regulation.

2.1.11 “Whistle-blower”, is a person who reports a wrongful, unethical or unlawful behaviour, misconduct internally or externally.

3 Relevant rules and regulations

Following Luxembourg’s hierarchy of relevant rules and regulations, the following is a summary of applicable law and regulation, which can be replaced or amended by relevant authorities without the immediate need to update the procedure unless a new obligation, a stricter requirement or a further provision calls for such update.

Rather than focusing on replicating the content of existing laws, the present procedure aims to explain the relevant obligations and firm’s reinforcements of the professional obligation applicable to AAME and its staff members (AAME).



3.1 Current rules and regulations include (but are not limited to):

3.1.1 European Directives and regulations:

1st Anti money laundering Directive, (91/308/EEC). As amended.

2nd Anti money laundering Directive, (2001/97/EC). As amended.

3rd Directive Anti money laundering, (2005/60/EC). As amended.

4th Directive Anti money laundering, (2015/849/EC).

AML Regulation (2015/847/EC).

3.1.2 Luxembourg Laws and regulations:

Law from 12 November 2004 (as amended)

Law from 27 October 2010

Grand Ducal Regulation from 1 February 2010

Grand Ducal Regulation from 29 October 2010

CSSF Regulation 12-02

3.1.3 Applicable CSSF circulars (and amendments):

CSSF 15/609

11/529 on the risk analysis in the context of the fight against money laundering and financing of terrorism (AML / CFT);

11/528 on the abolition of the transmission to the CSSF suspicious transaction reports regarding potential money laundering or terrorist financing;

13/556 - Entry into force of CSSF Regulation N° 12-02 of 14 December 2012 on the fight against money laundering and terrorist financing - repeal of Circulars CSSF 08/387 and CSSF 10/476;

06/274 - Entry into force of Regulation (EC) No 1781/2006 of the European Parliament and of the Council of 15 November 2006 on information on the payer accompanying transfers of funds;

3.1.4 Financial Action Task Force (FATF) statements and their respective application in Luxembourg,

On quarterly bases the FATF produces statements highlighting AML related issues which include the list of jurisdictions presenting a higher risk for Money Laundering and it is anticipated that in the future such statements will be extended to jurisdictions with issues regarding the control of terrorist financing.

Such statements and subsequent circulars or regulations produced by Luxembourgian authorities for local implementation are a dynamic part of this procedure and are to be considered as integral part of the same.

From time to time, the FATF amends or revise the current list of recommendation to be followed at international level, whenever this occurs, new rules and regulations may be produced in that sense.

4 Personal responsibility

Every staff member of AAME is responsible for the fight against money laundering, the counter of terrorist financing, the detection and exposure of corruption acts and therefore all staff members are to follow this procedure, to inform supervisors or the AMLRO regarding any activity potentially linked to the actions mentioned herein and if no action is taken, staff members are encouraged to be a whistle blower in protection of the market.

Notice: To receive a copy of the aforementioned legal texts or regulations, as well for a latest version of each regulation, please contact the Chief Compliance Officer for further details.

4.1 Roles and responsibilities

Every single employee or board member of AAME has the responsibility of complying with the law, policies and procedures, in specific with AML/CTF/KYC and Counter corruption related areas, as well as the legal obligation to use their knowledge for the avoidance of been involved or facilitate the use of AAME in the financing of any illegal action, but in particular the ones cover under the scope of this policy.

According to specific hierarchy levels, tasks and responsibilities, different staff members will perform different tasks and will commit to further responsibilities in order to ensure compliance, to protect the firm and to protect the financial market.

The ultimate responsibility for compliance seats with authorised management, daily management, heads of department (referred herein as **senior management**), the board of directors and the shareholders of **AAME** according to the scope of the decision made.

This responsibility does not include the individual responsibility of each member of AAME staff, nor responsibilities assigned to third parties when the relevant regulation appoints or admits the transfer, partial, limited or total of such responsibility(ies).

- 4.1.1 All staff members shall observe this policy and when applicable report to superiors or the AMLRO of any conduct which could potentially harm AAME.
- 4.1.2 Client facing staff are the first line of protection of AAME and is to them to provide information, use their knowledge and help in the prevention of criminal activities taking place in connection to AAME or its employees.
- 4.1.3 Control functions are to communicate with client facing persons and to verify the information/document provided in order to ensure coherence and to serve as a second line of defence.
- 4.1.4 Compliance and risk are responsible to communicate potential risk, to provide advice to senior management or to perform an enhanced oversight in order to raise alerts and to stimulate compliance awareness and compliance in decisions made by senior management and directors.
- 4.1.5 Senior management and directors are the ultimate responsible of the business conduct and shall ensure compliance when taking decisions.
- 4.1.6 Internal audit works as a further line of defence in order to verify that controls, procedures and conducts were according to the expected and effective.
- 4.1.7 External audit is to perform an enhanced protection as a vigilant of all the procedures and conducts performed but all internal parties.
- 4.1.8 The regulator is there to produce effective measures in order to limit the risk appetite of particular when such risk puts in danger the stability of the system or the transparency and fairness of the market, and to take actions when participants fail to comply with the rules and frameworks established.

5 Professional obligations

Luxembourg rules and regulations include a number of professional obligations which AAME follows.

Those obligations include:

- 1) Risk Based approach and risk analysis
- 2) Vigilance obligations including customer due diligence (CDD);
- 3) Having an appropriate internal organisation, being audited (internally and externally) and creating an appropriate compliance culture, awareness and training program.
- 4) Cooperation with authorities and regulators, including whistle blower policies;

In development of such professional obligations AAME perform the following controls, risk identifiers, risk mitigation plans and specific measures (as applicable):

5.1 Risk based approach and risk analysis

Operating in a global economy and accessing to global markets are activities regulated.

Nevertheless, no activity can be considered as risk free.

Understanding the conditions of the market and the risk profile of the targeted clients of AAME, certain activities will be performed in the frame of a risk based approach, in which main risk such as risk of TF, ML or corruption will be analysed from a regulatory and from a reputation base approach.

This analysis will be a collection of factors that together with the services provided, may generate mitigation actions and other action plans as considered appropriate by senior management.

The analysis of the specific risk applicable to a business relationship may generate a further level of control, a specific action or a number of operations which will represent the mitigation of the detected risk.

Every time that a particular risk related to a product or a business relationship appears, the same will be analysed in order to see the potential impact of such risk and if needed to create an action plan.

The risk level should be in line with the level of due diligence applied and the depth of knowledge of the client.

5.2 Customer Due diligence

Due diligence refers to the information and documents required to properly identify the client and will be in line with the legal requirements for the verification of the information provided.

The basic types of Due Diligence are:

Reduced Due Diligence: Set of reduced measures aimed to properly identify a client whenever the risk has been deemed as low and the legal and regulatory conditions to apply such reduction are met.

Standard Due Diligence: Set of measures aimed to properly identify a client whenever the application of Simplified Due Diligence is not possible and no risk factors call for the enhancement of Due Diligence.

Enhanced Due Diligence: Set of measures aimed to properly identify a client whenever in presence of risk factors requiring a deeper knowledge of the client or when a legal and regulatory provision requires such measures.

Due diligence Risk level	Simplified Due Diligence	Standard Due Diligence	Enhanced Due Diligence
Low	✓	✓	✓
Medium	x	✓	✓
High	x	x	✓

Legend:

x: Excluded by the relevant regulation

✓: Applicable if conditions set in the relevant regulations are met

As shown above, there is a correlation between the risk and the level of due diligence applicable which may vary according to several considerations.

The specific measures to be taken in a case-by-case base will vary in accordance with the specificities of the case but in no event will go against the prohibitions set in the table above.

For more detailed information, refer to the CCRO.

5.2.1 Performance, timing, updating and documenting of Customer Due Diligence (CDD)

CDD refers to the identification and verification of identity of clients, beneficial owners, representatives, relevant related parties and the identification of potential relevant risks affecting the business relationship.

According to the risk level, CDD can be simplified, standard/normal or enhanced.

5.2.2 Performance of CDD

CDD implies the obligation of collecting information and documents relevant to the client identification and rating of the client and the business relationship.

For this propose, AAME has put in place a series of systems, teams and tools for gathering and analysis of information and documents aimed to create a client profile.

To achieve this aim, the following should be considered:

1. Identifying and verifying the client's identity on the basis of documents, data or information obtained from a reliable and/or independent source, as applicable, according to the risk level of the customer and the type of due diligence required. Such information/documents may vary on a case-by-case basis but at all times should provide comfort regarding the understanding of the client, structure, beneficial ownership and profile as applicable.
2. Identifying and verifying the identity of the client's main representatives on the basis of documents, data or information obtained from a reliable and independent source, as applicable, according to the risk level of the customer and the type of due diligence required.
3. If UBO(s) is/are identified, relevant documents and pieces of information shall be gathered in order to clearly identify and verify the identity of such person/people in accordance to the risk level and the type of due diligence to be applied in each case.
4. Obtaining information on the purpose and intended nature of the business relationship as well as determining whether the client is acting on its own behalf or on behalf of a third party.
5. Conducting ongoing monitoring of the business relationship including scrutiny of transactions (when the nature of the services provided involve transactions) undertaken throughout that relationship to ensure that the transactions being conducted are consistent with the acquired client knowledge, its commercial activities and risk profile, including, where necessary, the source of the funds and ensuring that the documents, data and information held are up-to-date.

In accordance with the relevant regulation, due diligence should be performed in all cases and will include the above-mentioned elements.

When the client identification process cannot be duly completed, AAME employees or sub-contractors should:

- Not engage into a business relationship;
- Not execute the transaction;
- End the existent business relationship;
- Stop the internal process of client acceptance and continuance;
- Consider to notify the AMLRO to initiate a potential communication with the FIU (see "Cooperation with the authorities" chapter).

5.2.3 Timing of CDD

Clients evolve and change over time. In order to respond to this reality, AAME adapts its systems to react to new information, documents or relevant finding both for the acceptance and continuance of client relationships.

To ensure that relevant information and documents correspond to the current situation of the client, CDD must be performed or updated according to a number of rules which are described here below:

1. When **establishing** a business relationship,
2. A CDD must be applied on all clients, independently of the amount involved. The point described in Article 3 (1) (b) of the Luxembourg AML amended law of 12th November 2004 about occasional transactions of 10 000€ or any lower threshold set by the relevant regulation with a client (in one operation or in various operations which appear to be linked) does not apply.

3. At **any appropriate time** based on a risk assessment (in the event of high risk criteria occurring, significant transactions etc.),
4. When there is a **suspicion** of ML or TF,
5. When there are **doubts** about the veracity or adequacy of previously obtained customer identification data.

The CDD must be applied to all our clients, i.e. all clients for which we have currently at least one opened assignment and to all types of services independently of the fees' level.

The client acceptance process involves the identification and the verification of the identity of the client, ultimate beneficial owners and the client representatives and must be finalised before engaging into a business relationship as per the applicable law in accordance with to the pre-assessed risk level.

The purpose of the business relationship and the determination of whether or not the client is acting on its own behalf is an integral part of the CDD.

Any exception to this rule should be explicitly contained in the relevant regulation and the decision to apply such provision should be documented in the client's file.

5.2.4 Updating CDD

In respect of the professional obligations of the firm, client information (and relevant verification documents) should be kept up-to-date.

The compliance of the client file shall be reviewed in accordance to the following cycle of reviews or whenever new information comes to the knowledge of the engagement team:

- High risk clients' files have to be reviewed on an annual basis.
- Medium risk clients' files have to be reviewed every 2 years.
- Low risk clients' files have to be reviewed every 3 years.

Triggering facts which may prompt a review (and further update if necessary) of the client's file include:

1. New relevant information comes to the knowledge of the client relationship team;
2. When considered appropriate by the CCRO or by a senior management decision;
3. When the circumstances of the service or further services require an update of the information on file.

5.2.5 Documenting CDD

The Client acceptance and continuance process has been developed to analyse and store the result of the analysis of KYC/AML/CTF and relevant risk rating, knowledge and data as well as to document the formal acceptance of each client based on various factors (including AML/CTF).

This tool groups together a number of systems which integrate and cooperate in the client acceptance and client continuance process as well as interact with different working tools used by relevant teams.

5.3 Monitoring of clients

As part of the monitoring process of CDD, teams are required to perform the necessary duties and conduct business in compliance with applicable laws and regulations.

Sanction and name screening are integral part of the client acceptance process as well as the monitoring of clients. Therefore, the firm provides the necessary tools and systems to ensure such control at all times.

As systems, AAME has decided to outsource such control to OEPEXIA PSF S.A. (OPEXIA) supervised by the CSSF under the registered I00000092, which supervision was verified at the moment of the production of the current procedure and will be updated on regular bases.

This system includes specific obligations of control and reporting which are to be produced by OPEXIA and which relevant persons in AAME will have access to in order to comply with the control obligations applicable to AAME.

Transactions considered out of the profile of the client will be scrutinised, analysed and submitted for senior management approval.

In this case, regardless the decision to perform or reject the operation, documentation of the decision shall be stored in the appropriate software for control of documentation.

Operations, transactions or orders which raise a reasonable doubt of being linked with corrupt acts, financing of terrorism or money laundered should be brought to the attention of the AMLRO for further analysis.

In case a suspicious activity report is filed (or to be filed), please refer to the appropriate section of this procedure and please make specific attention to the criminal and civil implications delivered for not following the channels of communication and secrecy specified for the situation.

AAME employees and directors are hereby made aware of the statutory obligation to not disclose to the client, a third party or any none authorised party partial or complete information related or connected to a potential suspicious activity report or the process of the analysis of the appropriateness of such reporting. This limitation cannot interfere with the cooperation with authorities, nor with the functions and attributes of the AMLRO and support team.

5.3.1 Complex operations or unusual / suspicious activities

The ongoing monitoring duty implies the detection (according to the services provided) of complex operations or unusual / suspicious activities by taking into account:

- The size of the amounts involved;
- The type of clients;
- Their profile;
- The information available;
- Other factors considered as relevant by the technical team.

The level of understanding of the transactions will be determined by the specific services provided and in accordance to the access to the information required to perform such service.

Whenever there is a potential suspicion regarding a client, activity or transaction, reference is made to the guidelines laid down in the appropriate section (Cooperation with authorities).

5.3.2 AML/CTF blacklists, sanctions, control and PEP lists

The names of clients, UBOs, relevant proxy holders and appropriate related parties shall be screened using the tools provided by the firm and the result analysis and documentation of this process is to be considered as part of the Client Acceptance process.

Additionally, an automatic system is in place to ensure the monitoring and trigger a re-assessment of the client and a potentially update of the file as applicable.

The name screening system is updated regularly with the latest information provided by the service provider in cooperation with the provider of the tool to handle potential matches.

AAME might create a series of internal lists which will not necessarily mean the imposition of a sanction, blacklisting or any other restrictions and therefore the actions related to such list will be documented according to internal practice.

In case of a match, the engagement team in cooperation with AMLCT will perform the appropriate investigation to determine whether it is a real match or a false positive.

In case of real match, an assessment should be produced and documented in order to determine further actions to be taken.

5.4 Prohibited and refused relationships

In the cases in which the relevant regulation prohibits entering into business relationship with a client or a type of client, AAME will not accept the client and will refrain from performing transactions with such prohibited individual or entity. As a matter of example, it is prohibited to establish or maintain a business relationship with shell banks.

Whenever a decision to refuse a client is made, the AAME AUTHORISED MANAGEMENT of the respective Line of Service should be made aware. The AAME AUTHORISED MANAGEMENT will inform the AMLRO on this event and provide the reasons of such refusal.

The AMLRO should keep a log of all prohibited and refused business relationships together with the reasons for such refusal.

6 Cooperation with authorities

Every member, employee, collaborator or subcontractor of AAME, its affiliates and subsidiaries is legally required to fully cooperate with the Luxembourg authorities responsible for fighting money laundering, corruption and terrorism financing. For the fulfilment of this obligation, the company had set in place this specific procedure. This procedure will vary according to the level of seniority of each staff member.

Whenever any staff member knows, suspects or has reasonable grounds to suspect that money laundering, corruption or terrorist financing, may, might or has occurred, this information should be transmitted to the relevant supervisor (is applicable) and the AMLRO should be made aware of these situations in order to centralise communication.

In coordination with senior management, the AMLRO will develop an action plan.

Is to highlight that such action plan is a business strategy to adapt to the potential risk and does not interfere with the independence of the AMLRO as well as it does not conflict with his capability to inform authorities proactively and rapidly.

The MLRO is the appointed channel to communicate with the authorities.

Each party involved in this process must ensure confidentiality of every piece of information or documents related to the operation ensuring that no third party, nor the client are made aware of the suspicious, the actions decided or the process to follow.

All staff members should be aware of the criminal implications of communicating information or documents to third parties and the implications of informing the client or negligently handling documents or information.

Any breach of confidentiality must be immediately communicated to the AMLRO and Authorised management for appropriate actions.

Documentation/information should be handled to the MLRO and the decisions taken will be documented at each stage of the process.

In case of knowledge or suspicion of ML or TF, the assignment or transaction should not be executed before informing the FIU and obtaining their instructions.

An instruction by the FIU to block the execution of one or more operations is valid for a maximum period of 3 months from the date of the communication of the instruction to the professional. Nevertheless, this period may be extended by written order by one month each time, with the understanding that the total duration may not exceed six months. Where the instruction is communicated orally, it must be followed by a written confirmation within 3 business days, otherwise the effects of the instruction cease on the third business day at midnight.

The above procedure does not overrule the general obligation of staff members to cooperate with authorities in terms of the relevant regulation and does not conflict anyhow with the whistle blower policy.

7 Whistle blower principles and policy

Whenever and staff member comes to the conclusion that a situation is worth to be informed to AAME in term of the potential commission any of the situation under whistle-blower definition in the procedure, the person is encouraged to follow the disposition contained in this chapter and in applicable rules and regulations.

AAME encourage employees and staff members to follow up in the situations and potential risk brought to the attention of the AMLRO or CCRO.

Limited by the confidentiality and secrecy rules applicable to the steps, decisions and operations of the escalation of suspicious activities, if employees are aware that no action was taken in regards to a situation worth to be brought to the attention of authorities, they may use or their legal right and obligation of acting as a whistle blower.

Before bringing to the attention of the any third party any situation, employees should attend to raise the issue internally in order to allow the responsible person to take actions in the matter.

Employees which happen to detect a corrupted action or a facilitation of ML or TF within AAME shall immediately report the situation to the AMLRO or the board of directors for disciplinary actions and to immediately create applicable action plans and controls to bring the situation under control and to comply with applicable laws and regulations.

The encouragement and protection of whistle-blowers cannot conflict at any point with the general obligations of labour law, professional secrecy and should be always align with the principles of *bona fides* and shall provide **AAME** with the option of taking actions against any potential breach which is not clearly defined as structural and official firm's conduct.

7.1 Whistle blowing communication procedure and workflow

The whistle-blower, may skip the normal line of communication and refer directly to the AMLRO and/or to the board of directors in order to produce a report in the situation.

Once the whistle-blower has produce the report, both the board of directors and authorised management will ensure that no negative action is taken against the person who reported the situation within the frame of this section of the policy.

Every report should be produced in written to facilitate follow up and shall be as specific as possible in order to facilitate the internal investigation of the issue.

When receiving a report in the frame of this section, the received has ten (10) working days to set up a time frame for action and communicate such timeframe to the whistle-blower, this time frame cannot exceed twenty-five (25) working days counted from the next working day after the expiration of the 10-day time frame for initial response.

If the whistle-blower has sufficient ground to believe that no action was taken, he is free to continue with the legal options available and will endeavour to show with his/her/their actions that was in the search of justice and not with the aim of unlawfully harming AAME, the market or any particular individual or group of individuals.

8 Internal and external controls and audit

AAME has set a number of internal controls and test which include the use of service providers such as OPEXIA, ICARE and PwC Luxembourg.

To ensure the commitment of AAME with regulatory requirements, ethical behaviours and controls, AAME has created a reinforced 5 layers' control system.

AAME has selected top tier firms to fulfil every process or system provided by a third party and has put in place a team of specialist in order to better fulfil and further comply with regulatory and AAME expectations.

The 5th layers process can be described as follows:

- Layer 1. AAME sales team, acting as a first control point by deciding rules and regulations to be
- Layer 2. AAME Compliance team
- Layer 3. OPEXIA has been selected as a service provider to facilitate some of the externalisation of functions applicable to AAME, and being a well-established PSF was chosen for their specific high quality and controlled services.
- Layer 4. Internal Audit ICARE
- Layer 5. External audit PwC Luxembourg

OPEXIA is a service provider in charge of putting in place controls and facilitating advice to organise the internal structure and ensure the provision of systems, services and works flows for the control and operation of AAME.

ICARE has been appointed as internal auditor for AAME which the obligation to report and raise any potential issue to the attention of AAME for handling.

PwC Luxembourg was appointed as external auditor and therefore results in a 5th layer of control to ensure the process, the adequacy of systems and procedures and the compliance with regulatory requirements.

For specific matters AAME may call upon other professionals to assist in the better structuring and fulfilment of the compliance commitment and compliance culture.

9 Ongoing training, recruitment and awareness

9.1 AAME employees and collaborators are required to participate to ongoing training programs related to AML/CTF.

The training and awareness program must include:

- A regular ongoing training program on addressing particularly, but not exclusively, to the client-facing staff and to the staff in charge of AML/CTF compliance. The purpose of the program is to inform or remind relevant staff about the up-to-date status of the following topics:
- AAME's AML/CTF procedures;
- Different aspects of the laws and duties regarding AML/CTF;
- Professional Standards related to AML/CTF;
- Examples of operations susceptible of being linked to ML/TF and instructions how to proceed if a suspicious case is indicated.

According to the function, the staff will be trained and made aware of the applicable AML/CTF regulations and duties.

- The firm will use appropriate channels to distribute information and raise awareness regarding AML/CTF matters.
- Relevant employees and collaborators (subcontractors, contractors, third parties, etc.) of AAME are to undertake training on yearly bases.
For employees specific AAME training will be provided, while for collaborators there will be the option to provide AAME with evidence or comfort regarding such training.

9.2 Recruitment

Potential candidates will be required to agree to a screen of their names against black and control lists.

Additional parts of the process can be externalised and report shall be presented by the service provider.

If the activity of on boarding of personnel happens to be performed by AAME directly, this will be done in subjection to Luxembourg labour, anti-money laundering and applicable legislations.

Employees will be requested to follow necessary steps, controls and actions required by laws and regulations applicable at the time and additionally will be requested police clearance certificate from the countries in which they have resided in the last 3 years' prior their candidature.

Every new joiner will be presented with the necessary policies and provided with relevant training in matters applicable to their position within the first 3 months from the first day of effective work.

The failure to comply with the above from the new joiner is a serious labour misconduct which may generate termination of the working contract.

10 Update and approval of the procedure:

The present procedure should be revised in yearly bases and updated whenever appropriate.

For updates in citation, and not material changes the update can be performed immediately with the double approval of the CCRO and one authorised manager of AAME.

For further or material updates or modification, this will be presented to the board of directors for approval.

In yearly bases all changes will be presented to the board of directors for their final approval, or in case in which during a year no change was performed, this situation will be brought to the attention of the board of directors.

11 Document retention policy

All documents related with Client Acceptance and continuance will be kept for a period of five (5) years from the end of the business relationship with the customer or after the date in which the occasional transaction was performed.

Exceptionally, **AAME** may store the information and supporting documents for a longer period due to specific potential risk characteristics of the client or the relationship as per decision of the CAC.

Personal data for persons of contact, including service providers, contractors, employees and other will be kept for the same period.

Other information will be kept based on the applicable law and regulation for that matter to the maximum foreseen by the law and in accordance with the paragraphs above.

If no other information is giving by relevant rules and regulations the five (5) years' document retention policy should apply.

12 Appointment of officers:

The present appointment is to be approved by the Client Acceptance Committee and the Board of Directors will only produce a post fact ratification or amendment.

Approval and update: DD, MM, YYYY

Date of approval by CAC, DD, MM, YYYY

Date of approval by Board of directors: DD, MM, YYYY

Chronological log of updates

Updated section	Comment on update	producer	Approver	Date of approval