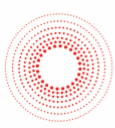

GRAVITY | PRIVATE WEALTH

Anti-Money Laundering and Anti-Terrorist Financing Policy

File Information

Responsible Unit	Date of issue	Publication No
Regulatory Compliance & AML	01/10/2025	v.2

Archive History

Publication No	Date	Description of Modifications
v.1	01/11/2024	Original Edition
v.2	01/10/2025	Updated version in compliance with Circular C721

Board of Directors Approval

Board of Directors	Meeting Date
Approved v.2	01/10/2025

Table of Contents

1. Introduction

Gravity Private Wealth Ltd (hereinafter the "Company") is an Investment Firm incorporated and registered under the laws of the Republic of Cyprus, with registration number HE 442079. The Company is authorized and regulated by the Cyprus Securities and Exchange Commission ("CySEC") under license number 447/24.

The Company recognizes the risks posed by money laundering and terrorist financing and takes appropriate measures to address these risks, taking into account various risk factors, such as those related to its clients, the complexity of their transactions and the range of products and services it provides.

In this context, the Company establishes the Anti-Money Laundering and Anti-Terrorist Financing Policy (hereinafter the "Policy"). The purpose of the Policy is to ensure the existence of adequate procedures, systems and controls, properly updated to identify, prevent and deter any activity related to Money Laundering and Terrorist Financing.

The Company evaluates the Policy at least annually, and whenever a relevant need arises, and takes appropriate measures to address any identified weaknesses.

2. Institutional and Supervisory Framework

2.1. Institutional framework

The Policy has been prepared in accordance with the following laws, regulations, directives and guidelines:

- The Prevention and Suppression of Money Activities Law 188(I) 2007, including the amendments made thereof 58(I)/2010, 80(I)/2012, 192(I)/2012, 101(I)/2013, 184(I)/2014, 18(I)/2016, 13(I)/2018, 158(I)2018, 81(I)2019, 13(I)/2021, 22(I)/2021 and 61(I)/2021 (the "AML Law");
- The Directive for the Prevention of Terrorist Financing issued by the Cyprus Securities and Exchange Commission ("CySEC" or the "Commission") (the "AML Directive"), as subsequently amended;
- The Directive (EU) 2018/1673 of the European parliament and of the council of 23 October 2018 on combating money laundering by criminal law establishing the minimum rules concerning the definition of criminal offences and sanctions in the area of money laundering (the "6th AML Manual");

- Other laws and regulations of the Republic of Cyprus, issued from time to time, applicable to this Policy;
- Risk Factor Guidelines, issued by the Joint Committee of the European Supervisory Authorities;
- Risk Factor Guidelines and other Guidelines issued by the Financial Action Task Force (FATF);
- The Implementation of the Provisions of the Resolutions or Decisions of the United Nations Security Council (Sanctions) and of the Decisions and Regulations of the Council of the European Union (Restrictive Measures) Law 58(I) of 2016, as subsequently amended.

2.2. Definitions

Term	Definition
AML/CFT	Means Anti-Money Laundering and Countering the Financings of Terrorism.
Business relationship	Means a business, professional or commercial relationship which relates to the professional activities of the Company.
CIF	Means a Cyprus Investment Firm.
Client	A Client is a person, legal or natural, to whom the Company provides, intends to provide or has provided investment services in the course of carrying on a regulated activity and as those are defined in the Investment Services and Activities and Regulated Markets Law of 2017, as amended.
Alternate AML and Compliance Officer	Means the person who will be appointed by the Company to act as the Company's AML and Compliance Officer, in the case the latter's absence.
High-risk third country	Includes any third country identified by the European Commission, which demonstrates strategic deficiencies in their national AML/CFT regime that pose significant threats to the financial system of the European Union.
MOKAS	Means the Unit for Combating Money Laundering.
Senior Management	Means an officer or employee with enough knowledge of the Company's Money Laundering and Terrorist Financing risk exposure and sufficient seniority to take

Term	Definition
	decisions affecting its risk exposure, and need not, in all cases, be a member of the Board of Directors.
PEPs	A person is considered to be a Politically Exposed Person (PEP) if, among others: a) Is head of state, head of government or state official such as a minister, deputy or b) Assistant minister; c) Is a member of parliament; d) Is a member of the governing bodies of political parties; e) Is a member of supreme court, constitutional court or of other high-level judicial bodies whose decisions are not subject to further appeal, except in exceptional circumstances; f) Is a member of court of auditors or of the boards of central banks; g) Is an ambassador, Commercial attaché or Army officer; h) Is a member of the administrative, management or supervisory bodies of State-owned enterprises; i) Directors, deputy directors and members of the board or equivalent function of an international organisation; and j) Mayors. "Persons known to be close associates" of PEPs include the following: a) Any natural person who is known to have joint beneficial ownership of legal entities or legal arrangements, or any other close business relations, with a person referred to in the above categories, b) Any natural person who has sole beneficial ownership of a legal entity or legal arrangement which is known to have been set up for the benefit de facto of the person referred to the above categories.

Term	Definition
	None of the aforementioned categories shall be understood as covering middle ranking or more junior officials. "Immediate family members" are also considered a PEP and include the following: a) The spouse of the PEP or the person with whom the PEP cohabits for at least one year, b) The children of the PEP and their spouses or the persons with whom they cohabit for at least one year, the parents of the PEP.
UBO	Any natural person(s) who ultimately owns or controls the Client and / or the natural person(s) on whose behalf a transaction or activity is being conducted and includes at least: a) In the case of corporate entities, the natural person(s) who ultimately owns or controls a legal entity through direct or indirect ownership of a sufficient percentage of the shares or voting rights or ownership interest in that entity, including through bearer shareholdings, or through control via other means, other than a company listed on a regulated market that is subject to disclosure requirements consistent with Union law or subject to equivalent international standards which ensure adequate transparency of ownership information. A shareholding of 25% plus one share or an ownership interest of more than 25% in the Client held by a natural person shall be an indication of direct ownership. A shareholding of 25% plus one share or an ownership interest of more than 25% in the Client held by a corporate entity, which is under the control of a natural person(s), or by multiple corporate entities, which are under the control of the same natural person(s), shall be an indication of indirect ownership. b) In the case of trusts, all following persons: ▪ The settlor; ▪ The trustee(s); ▪ The protector, if any;

Term	Definition
	▪ The beneficiaries, or where the individuals benefiting from the legal arrangement or entity have yet to be determined, the class of persons in whose main interest the legal arrangement or entity is set up or operates; ▪ Any other natural person exercising ultimate control over the trust by means of direct or indirect ownership or by other means. c) In the case of legal entities, such as foundations and legal arrangements similar to trusts: The natural person holding equivalent or similar positions to the person referred to the above paragraph.
Legal person	Means any entity having legal personality under the applicable law, except for states or public bodies in the exercise of state authority and for public international organisations person.
Property	Means assets of any kind, whether corporeal or incorporeal, movable or immovable, tangible or intangible, and legal documents or instruments in any form, including electronic or digital, evidencing title to, or an interest in, such assets.

2.3. Basic concepts

According to article 3(1) of the 6th AML Manual, the money laundering of criminal activities is carried out through the following acts:

a) The conversion or transfer of property with the knowledge of the fact that it comes from criminal activity or from an act of participation in such activity with the purpose of concealing or covering up its illegal origin or providing assistance to anyone involved in this activity to avoid legal consequences of his actions,

b) The concealment or concealment of the truth, regarding the nature, origin, disposal, dealing or use of property or the place where it was acquired or located or the ownership of the property or related rights, knowing the fact that this property comes from criminal activity or from an act of participation in such activity,

c) The acquisition, possession or use of property, knowing, at the time of acquisition or at the time of possession or use, of the fact that the property derives from criminal activity or from an act of participation in such activity.

Money laundering from criminal activities also exists when the activities from which the property to be laundered originates have taken place in the territory of another state, since these would be a basic offense if they were committed in Cyprus and are considered punishable, according to the legislation of that state.

2.4. Criminal activity – basic offences

According to article (2) of the 6th AML Manual:

'*criminal activity'* means any kind of criminal involvement in the commission of any offence punishable, in accordance with national law, by deprivation of liberty or a detention order for a maximum of more than one year or, as regards Member States that have a minimum threshold for offences in their legal systems, any offence punishable by deprivation of liberty or a detention order for a minimum of more than six months. In any case, offences within the following categories are considered a criminal activity:

a) Participation in an organised criminal group and racketeering, including any offence set out in Framework Decision 2008/841/JHA;
b) Terrorism, including any offence set out in Directive (EU) 2017/541 of the European Parliament and of the Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism;
c) Trafficking in human beings and migrant smuggling, including any offence set out in Directive 2011/36/EU of the European Parliament and of the Council (2) and Council Framework Decision 2002/946/JHA;
d) Sexual exploitation, including any offence set out in Directive 2011/93/EU of the European Parliament and of the Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography;
e) Illicit trafficking in narcotic drugs and psychotropic substances, including any offence set out in Council Framework Decision 2004/757/JHA;
f) Illicit arms trafficking;
g) Illicit trafficking in stolen goods and other goods;
h) Corruption, including any offence set out in the Convention on the fight against corruption involving officials of the European Communities or officials of Member States of the European Union and in Council Framework Decision 2003/568/JHA;
i) Fraud, including any offence set out in Council Framework Decision 2001/413/JHA;
j) Counterfeiting of currency, including any offence set out in Directive 2014/62/EU of the European Parliament and of theDirective (EU) 2017/541;
k) Counterfeiting and piracy of products;

l) Environmental crime, including any offence set out in Directive 2008/99/EC of the European Parliament and of the Directive 2011/36/EU of the European Parliament and of the Council of 5 April 2011 on preventing and combating trafficking in human beings and protecting its victims,or in Directive 2009/123/EC of the European Parliament and of the Council Council Framework Decision 2002/946/JHA;

m) Murder, grievous bodily injury;

n) Kidnapping, illegal restraint and hostage-taking;

o) Robbery or theft;

p) Smuggling;

q) Tax crimes relating to direct and indirect taxes, as laid down in national law;

r) Extortion;

s) Forgery;

t) Piracy;

u) Insider trading and market manipulation, including any offence set out in Directive 2014/57/EU of the European Parliament and of the Directive 2011/93/EU;

v) Cybercrime, including any offence set out in Directive 2013/40/EU of the European Parliament and of the Council Framework Decision 2004/757/JHA.

3. Roles and responsibilities

3.1. *Responsibilities of the Board of Directors*

The Board of Directors (the "Board") has the overall responsibility to define and oversee the implementation of all relevant arrangements that ensure compliance with the applicable AML/CFT legislation and the effective management of the Company. As a part of overall responsibility, the Board shall:

a) Determine, record and approve the general policy principles of the Company in relation to AML/CFT and communicate them to the AML and Compliance Officer;

b) Appoint a AML and Compliance Officer and an Alternate AML and Compliance Officer and determine their duties and responsibilities, which are recorded in this Policy;

c) Approve the Policy, which is communicated to all employees of the Company, that manage, monitor or control in any way the Clients' transactions and have the responsibility for the application of the practices, measures, procedures and controls that have been determined;

d) Identify the member of the management body, who will be responsible for the implementation of the AML Law and of the applicable directives and/or circulars and/or regulations including any relevant acts of the European Union;
e) Ensure that all requirements of the AML Law and of the AML Directive are applied, and assure that appropriate, effective and sufficient systems and controls are introduced for achieving the abovementioned requirement;
f) Ensure that the AML and Compliance Officer, any persons employed in the Regulatory Compliance & AML Department and any other person who has been assigned with the duty of implementing the procedures for AML/CFT, have complete and timely access to all data and information concerning Clients' identity, transactions' documents and other relevant files and information maintained by the Company so as to be fully facilitated in the effective execution of their duties;
g) Ensure that all employees are aware of the person who has been assigned the duties of the AML and Compliance Officer, the Alternate AML and Compliance Officer as well as the AML and Compliance Officer's assistants, to whom they report any information concerning transactions and activities for which they have knowledge or suspicion that might be related to Money Laundering and Terrorist Financing;
h) Establish a clear and quick reporting chain based on which information regarding suspicious transactions is passed without delay to the AML and Compliance Officer, either directly or through the latter's assistants and notifies accordingly the AML and Compliance Officer for its explicit prescription in the Policy;
i) Ensure that the AML and Compliance Officer as well as the Alternate AML and Compliance Officer have sufficient resources, including competent staff and technological equipment, for the effective execution of their duties and responsibilities;
j) Assess and approve the annual AML report and take all action as deemed appropriate under the circumstances to remedy any weaknesses and/or deficiencies identified.

Designation of AML and Compliance Officer

The Company appoints, by decision of the Board, the AML and Compliance Officer to ensure compliance with its obligations regarding the prevention of the use of its systems for the legalization of proceeds from criminal activities and the financing of terrorism.

The AML and Compliance Officer is the responsible officer who ensures the correct and adequate implementation of this Policy, to whom the other executive officers report any transaction that is considered

unusual or suspicious of money laundering, as well as any event of which they become aware, due to their competence, and which could be an indication of criminal activity.

The appointment of the AML and Compliance Officer is carried out based on criteria such as ethics, integrity, reputation, scientific competence, experience in relevant tasks and knowledge of the Company's operations.

3.2. Responsibilities of the AML and Compliance Officer

The duties of the AML and Compliance Officer are the following:

- Designs the internal practice, measures, procedures and controls relevant to AML/CFT and describes and allocates the appropriateness and limits of responsibility of each department involved. It is provided that, the above include measures and procedures for the prevention of the abuse of new technologies and systems providing financial services, for the purpose of Money Laundering and Terrorist Financing (e.g. services and transactions via the internet or telephone), as well as measures so that the risk of Money Laundering and Terrorist Financing is appropriately considered and managed in the course of daily activities of the Company with regards to the development of new products and possible changes in the Company's economic profile;
- Develops and establishes the Client Acceptance Policy and submits it to the Board for consideration and approval;
- Monitors and assesses the correct and effective implementation of the Policy, to be decided by the Board, in relation to the prevention of Money Laundering and Terrorist Financing, applies monitoring mechanisms in order to assess the level of compliance of the departments and employees of the Company;
- Gives guidance for corrective measures where necessary and informs the Board if needed;
- Receives information, in a written report form, "Internal Suspicion Report", from the Company's employees regarding suspicion of Money Laundering or Terrorist Financing Activities, attached in the Annex II;
- Evaluates and examines the abovementioned information by reference to other relevant information and discusses the circumstances with the person(s) who made the report, and;
    - In the case where the AML and Compliance Officer decides to notify MOKAS, they should electronically do so through the web application goAML at http://www.law.gov.cy/Law/MOKAS/MOKAS.nsf/All/8D5B6DF6DC5D5815C2257BE1002A2848?OpenDocument

- If it is decided, after examination, that there is no need for notifying MOKAS, the reasons for such decision should be explained in the "Internal Evaluation Report" (Annex III);

- Acts as the first point of contact with MOKAS, upon commencement and during an investigation as a result of filing a report to MOKAS;
- Detects, records and evaluates, at least on an annual basis, all risks arising from existing and new Clients, new financial instruments and services and updates and amends the systems and procedures applied by the Company;
- Ensures the preparation and maintenance of the lists of clients categorised following a risk based approach, according to the details mentioned in the law and ensures the updating of the said lists of all new and existing clients when additional informaiton is obtained;
- Verifies that the third party with whom the Company intends to rely on for the application of the client identification and due diligence measures, is an Obliged Entity, as defined under Section 2a of the AML Law and gives his/her written approval for the said reliance, which should be kept in the personal file of the third party;
- Ensures that the Company's branches and subsidiaries (if any) that operate in countries outside the European Economic Area, have taken all necessary measures for achieving full compliance with Client Identification, Due Diligence and Record Keeping Procedures;
- Provides advice and guidance to employees on subjects related to Money Laundering and Terrorist Financing;
- Determines the Company's departments that need further training and education for the purpose of preventing Money Laundering and Terrorist Financing and organizes appropriate training sessions/seminars;
- Prepares and applies an annual staff AML training program;
- Assesses the adequacy of the education and training provided;
- Prepares and submits timely to the Commission the Monthly Prevention Statement regarding the Prevention of Money Laundering and Terrorist Financing;
- Prepares and submits to the Board and subsequently to CySEC the Annual Report of the AML and Compliance Officer;
- Responds to all requests and queries from MOKAS and the Commission and provides them with all requested information;
- Maintains a registry which includes any reports submitted internally to the AML and Compliance Officer, as well as any reports to MOKAS;
- Assesses and approves the Clients' requests for transfer of assets;

- Maintains a registry with the data/information of the third parties, that the Company relies on for the application of Client identification procedures and Client due diligence measures according to the AML Law and the AML Directive.

3.3. Annual AML Report

The Annual AML Report prepared by the AML and Compliance Officer is a significant tool for assessing the Company's level of compliance with the relevant obligations laid down in the AML Law and the AML Directive. The Annual AML Report shall be prepared and be submitted to the Board for approval within two months from the end of each calendar year (i.e. the latest by the end of February each year).

The Annual AML Report, after its approval by the Board, should be submitted to CySEC together with the minutes of the Board meeting, during which the Annual AML Report has been discussed and approved. It is provided that the said minutes shall include the measures decided for the correction of any weaknesses and/or deficiencies identifies in the Annual AML Report and the implementation timeframe of these measures. The submission to CySEC shall be made within twenty days from the date of the relevant meeting, and no later than three months from the end of the calendar year (i.e. the latest by the end of March), and shall be submitted electronically (online) in PDF format via the web portal of CySEC.

The Annual AML Report deals with Money Laundering and Terrorist Financing preventive issues pertaining to the year under review and, as a minimum, covers the following:

a) Information for measures taken and/or procedures introduced for compliance with any amendments and/or new provisions of the AML Law and the AML Directive which took place during the year under review;
b) Information on the inspections and reviews performed by the AML and Compliance Officer, reporting the material deficiencies and weaknesses identified in the Policy as well as in the practices, measures, procedures and controls that the Company applies for the prevention of Money Laundering and Terrorist Financing. In this regard, the report shall outline the materiality of the deficiencies and weaknesses, the risk implications and the actions taken and/or recommendations made for rectifying the situation;
c) The number of Internal Suspicion Reports submitted by employees of the Company to the AML and Compliance Officer;
d) The number of Reports submitted by the AML and Compliance Officer to MOKAS, with information/details on the main reasons for suspicion and highlights of any particular trends;

e) Information, details or observations regarding the communication with the employees on Money Laundering and Terrorist Financing preventive issues;
f) Summary figures, on an annual basis, of Clients' total cash deposits in Euro and other currencies in excess of the set limit of 10.000 Euro (together with comparative figures for the previous year) as reported in the Monthly Prevention Statement. Any comments on material changes observed compared with the previous year are also reported;
g) Information on the policy, measures, practices, procedures and controls applied by the Company in relation to high risk Clients, as well as the number and country of origin of high risk Clients with whom a business relationship is established or an occasional transaction has been executed;
h) Information on the systems and procedures applied by the Company for the ongoing monitoring of Clients' accounts and transactions;
i) Information on the measures taken for the compliance of branches and subsidiaries of the Company, that operate in countries outside the European Economic Area, with the requirements of the Directive in relation to Client identification, due diligence and record keeping procedures and comments/information on the level of their compliance with the said requirements;
j) Information on the training courses/seminars attended by the AML and Compliance Officer and any other educational material received;
k) Information on training/education and any educational material provided to staff during the year, reporting, the number of courses/seminars organised, their duration, the number and the position of the employees attending, the names and qualifications of the instructors, and specifying whether the courses/seminars were developed in-house or by an external organisation or consultants;
l) Results of the assessment of the adequacy and effectiveness of staff training;
m) Information on the recommended next year's training program;
n) Information on the structure and staffing of the department of the AML and Compliance Officer as well as recommendations and timeframe for their implementation, for any additional staff and technical resources which may be needed for reinforcing the measures and procedures against Money Laundering and Terrorist Financing.

3.4. *Monthly Prevention Statements*

The AML and Compliance Officer shall prepare and submit to CySEC, on a monthly basis, the CySEC Form 144-08-11 "Monthly prevention statement regarding the prevention of Money Laundering and Terrorist Financing", which includes:

- Details for the total cash deposits accepted by the Company;

- The Internal Suspicions Reports; and
- The AML and Compliance Officer's Reports to MOKAS.

The completion of the Monthly Prevention Statement is an opportunity for the Company to initially evaluate and subsequently, to reinforce its systems of control and monitoring of its operations, for the purpose of timely identification of cash transactions that may be unusual and/or which may entail a higher risk of Money Laundering or financing of terrorism activities.

The said Form must be completed and submitted to CySEC within fifteen (15) days from the end of each month.

The Internal Auditor shall be responsible to review, at least annually, the submission to CySEC of the relevant "Monthly prevention statement regarding the prevention of Money Laundering and Terrorist Financing".

3.5. *Responsibilities of the Alternate AML and Compliance Officer*

The Company shall appoint an Alternate AML and Compliance Officer, who will be replacing the AML and Compliance Officer, in the case of his/her absence from the office and will be responsible for the execution of his/her duties and responsibilities. The Company must immediately inform CySEC for the appointment of the AML and Compliance Officer, the Alternate AML and Compliance Officer, as well as any other member of the Regulatory Compliance & AML Department, submitting their name, their position and their contact details.

It is however noted that, the Alternate AML and Compliance Officer will not replace the latter in case of his/her resignation from the position, but he/she may act as a temporary replacement of the AML and Compliance Officer until a new candidate is hired. The Board will proceed with the appointment of a new AML and Compliance Officer.

3.6. *Responsibilities of the Company's employees*

All Company's employees have an individual and personal responsibility to comply with the AML/CFT activities legislation and regulations. The Company has zero-tolerance to violations and internal disciplinary actions will be implemented in case of non-adherence to the provisions of this AML Policy and the regulatory framework. In this respect, the Company expects from its employees to perform the following:

a) Conduct business in accordance with applicable AML laws, Company's policies and procedures, and the highest ethical standards;

b) Do not provide advice or other assistance to persons who attempt to violate or avoid AML laws or the Company's policies and procedures;
c) Consider the AML and Compliance Officer's approval or rejection of any disputable transaction as final and binding;
d) Fully execute their obligations against the Law to disclose any suspicions about a transaction that might be related to Money Laundering or Financing of Terrorism activities;
e) Adequately record and retain details of all transactions undertaken with or for third parties, including payments and receipts of funds, movements of custody securities and collateral, as well as all dealings in financial instruments.

4. Client Acceptance Policy

The Company has developed and implements client acceptance procedures, in accordance with the applicable legislative and regulatory framework, in order to prevent the initiation of a relationship with clients against whom restrictive measures apply or present an impermissible level of risk of Money Laundering or Terrorist Financing.

The Client Acceptance Policy shall clearly define the procedure and the specific criteria for accepting new Clients, as well as for the risk categorization of the accepted Clients. These procedures and criteria shall be in line with the provisions of the AML Law and as well as any directives and circulars issued from CySEC from time to time and shall be followed by the Company's employees who are involved in the Clients' onboarding procedure.

The Company takes into consideration the following principles for accepting new Clients:

- the Clients' background, examining the profession, the knowledge and experience of the Client along with the said financial instruments and/or type of investment services, academic qualifications etc.;
- the type and nature of Clients' business, obtaining a brief description of the Clients' work experience as well as the area of expertise;
- the country of origin, identifying whether the Client is located in a third country jurisdiction which may be considered suspicious for Money Laundering services. In such cases the Company will ask for additional information regarding the Client to ensure that such possibility is eliminated or managed accordingly;
- the services and financial instruments applied for and the anticipated level and nature of business transactions, in order to ensure that they correspond to the respective Client's profile;

- the expected source and origin of funds, in order to ascertain whether any of the funds of the Client may be resulted by any Money Laundering or criminal activities.

In the case the abovementioned principles are considered and followed, then the Clients are acceptable and are categorized as normal risk Clients. The category of low risk Clients includes the Clients that the Company has determined to categorize as such. The Company may accept Clients who are categorized as high risk Clients, as long as the abovementioned principles are followed. The Company shall apply the enhanced due diligence and identification measures for the high risk Clients and the relevant due diligence and identification procedures for the specific types of high risk Clients, as applicable.

4.1. Know Your Client (KYC)

Know Your Client principle ("KYC") forms the basis of all procedures for the prevention of Money Laundering and Terrorist Financing.
This principle provides for the collection and maintenance of sufficient information about the client, for the purposes of:

- recognition and certification (verification) of their identity and
- evaluation of their overall picture.

The Clients' identity details must be fully up-to-date throughout the business relationship, which is achieved by reviewing said details on a regular basis or ad hoc in the event of doubt regarding their validity.

The Company should obtain Annex I ("Know Your Client (KYC) Form") completed from the Client.

In this evaluation framework and in order to ascertain the identity and financial profile of the Client, Annex IV lists the key documents that must be collected.
The implementation of the principle is essentially achieved through the collection and verification of the Annex IV data as well as the receipt of all the necessary information that contributes to the formation of the knowledge of the expected transactional profile.

4.2. Performing electronic verification

The verification of Client's identification via electronic means is carried out either directly by the Company or through a third party. Both the Company and the said third parties should cumulatively satisfy the following conditions:

a) The electronic databases kept by the third party or to which the third party or the Obliged Entity, as defined under Section 2a of the AML Law, has access are registered to and/or approved by the Data Protection Commissioner in order to safeguard personal data (or the corresponding competent authority in the country the said databases are kept);

b) Electronic databases provide access to information referred to both present and past situations showing that the person really exists and providing both positive information (at least the Client's full name, address and date of birth) and negative information (e.g. committing of offences such as identity theft, inclusion in deceased persons records, inclusion in sanctions and restrictive measures' list by the Council of the European Union and the UN Security Council);

c) Electronic databases include a wide range of sources with information from different time periods with real-time update and trigger alerts when important data alter;

d) Transparent procedures have been established allowing the Financial Organization to know which information was searched, the result of such search and its significance in relation to the level of assurance as to the Client's identity verification;

e) Procedures have been established allowing the Financial Organization to record and save the information used and the result in relation to identity verification.

The Company shall evaluate the results of electronic verification in order with the conditions of Article 61(3) of the AML Law to be satisfied. The Company establishes mechanisms for the carrying out of quality controls in order to assess the quality of the information on which it intends to rely. The said information should come from two or more sources. The electronic verification procedure shall at least satisfy the following correlation standard:

a) Identification of the Client's full name and current address from one source, and
b) Identification of the Client's full name and either his current address or date of birth from a second source.

For purposes of carrying out the electronic verification, the Company shall establish procedures in order to satisfy the completeness, validity and reliability of the information to which it has access. It is provided that the verification procedure shall include a search of both positive and negative information.

The requirements of Article 64(1)(a) of the AML Law and of the AML Directive shall also apply to Companies or other legal persons requesting to establish a business relationship or an occasional transaction by mail, telephone or through the internet. The Company shall take additional measures to ensure that the

companies or other legal persons operate from the address of their main offices and carry out legitimate activities in all respects.

4.3. Derogation under Section 62(2) of the AML Law (L.188(I)/2007)

The Company does not apply the derogation provided under section 62(2) of the Prevention and Suppression of Money Laundering Activities Law (L.188(I)/2007) in its normal course of business, as client and beneficial owner identity verification is completed prior to the establishment of any business relationship.

However, in the rare event that the Company deems it necessary to proceed under the derogation in order not to interrupt the normal conduct of business — and where the risk of money laundering or terrorist financing is assessed as low — the Company shall ensure full compliance with the conditions and safeguards set out in CySEC Circular C721, including the 15-day verification timeframe, deposit thresholds, refund procedures, and client consent requirements.

Time of Application of Due Diligence Measures and Identification Procedures

1. The Company verifies the identity of the client and the beneficial owner before the establishment of a business relationship or the carrying out of an occasional transaction.

2. By way of derogation from paragraph (1), the verification of the identity of the client and the beneficial owner may be completed during the establishment of a business relationship if this is necessary not to interrupt the normal conduct of business and where there is little risk of money laundering or terrorist financing occurring. In such situations these procedures shall be completed as soon as practicable after the initial contact and before any transactions take place.

3. Without prejudice to what is stated in paragraph (2) and by way of derogation from paragraph (1), for cases that fall under the supervision of the Cyprus Securities and Exchange Commission (CIFs), the verification of the identity of the client and the beneficial owner may be completed during the establishment of a business relationship, provided that this is necessary not to interrupt the normal conduct of business and where the risk of money laundering or terrorist financing is low. In such cases, these procedures shall be completed as soon as practicable after the initial contact.

According to article 61(1)(a) and (b) of the Law, client identification and client due diligence procedures include “identifying the client/beneficial owner” and “verifying the identity of the client/beneficial owner”.

The identification of a client/beneficial owner occurs before the establishment of a business relationship with the said person. It is noted that the identification procedure includes the following (where appropriate):

a. Creation of an economic profile for the client/beneficial owner, and/or
b. Carrying out a suitability test in accordance to article 26(2) of the Law regarding the provision of investment services, the exercise of investment activities and the operation of regulated markets (the ‘L. 87(I)/2017’) and/or
c. Carrying out an appropriateness test in accordance to article 26(3) of L. 87(I)/2017.

As a general rule, in accordance to article 62(1) of the Law, the verification of identity of a client/beneficial owner, also takes place before the establishment of a business relationship with the said person.

By way of derogation to the general rule of article 62(1) of the Law, in accordance to the article 62(2) of the Law and CySEC’s Circular C721, the verification of identity of the client/beneficial owner of the Company may be completed during the establishment of a business relationship, provided that all the following conditions are met:

a) if this is necessary so as not to interrupt the normal conduct of business, and
b) where there is little (low) risk of money laundering or terrorist financing occurring, and
c) where the verification procedure is completed within 15 calendar days from initial contact.

In relation to paragraphs (2) and (3) above and pursuant to CySEC Law, when commencing the establishment of a business relationship with a client/beneficial owner whose identity has not been yet verified, the risk may be assessed as low when, as a minimum, the following, among others, are taken into consideration:

- If the verification of the customer/beneficial owner’s identity has not been completed, the cumulative amount of deposited funds of a client/beneficial owner should not exceed €2,000, irrespective of the number of accounts the client/beneficial owner holds with the regulated entity. The amount of €2,000 does not automatically categorise the client as a low risk client. It is noted that the Company should assess each business relationship’s risk in accordance with the appropriate procedure as

per the Law and the CySEC's Directive for the Prevention and Suppression of Money Laundering and Terrorist Financing ('CySEC's Directive').

- The Company accepts deposits only from a bank account (or through other means that are linked to a bank account e.g. credit card), that is in the name of the client with whom establishes a business relationship. Third-party payments must be prohibited.

- The cumulative time in which the verification of the identity of a customer/beneficial owner is completed, must not exceed 15 days from initial contact.

- It is noted that the initial contact takes place the moment that the client either accepts the terms and conditions or makes their first deposit, whichever comes first.

- Within the timeframe of 15 days from initial contact, the Company takes all reasonable measures to ensure that the percentage of clients that have not complied with the request to submit verification documents, is considerably low (e.g. the Company issues requests/reminders to the customer/beneficial owner informing them of their obligation to submit the requested documents for the verification of their identity).

- Where the verification of the client/beneficial owner's identity has not been completed during the designated timeframe of 15 days, the commencement of a business relationship must be terminated on the date of the deadline's expiry and all deposited funds must be returned to the client/beneficial owner, in the same bank account from which they originated. The procedure for returning the funds must occur immediately, regardless of whether the client has requested the return of their funds or not.

- The returned funds (deposits) include any profits the client has gained during their transactions and deducting any losses incurred.

- Within the timeframe of 15 days from initial contact, the client/beneficial owner must undergo at least one Enhanced Due Diligence measure as described in this manual.

- No funds are withheld and no accounts are frozen, save for those cases of suspicion of money laundering, where the regulated entity is under obligation to immediately report their suspicion to MOKAS and notify CySEC of the suspicious transaction incident in the designated procedure.

It is provided that the above paragraph shall be without prejudice to the factors of potentially lower money laundering and terrorist financing risk situations set out in Annex V that the Company shall take into account when assessing the risks relating to types of customers, geographic areas, and particular products, services, transactions or delivery channels.

It is noted that the Company is under obligation to include in their risk management/money laundering manual, the designated internal practice, the measures, procedures and controls undertaken for the proper and effective implementation and monitoring of compliance with article 62(2) of the Law.

No deposits should be accepted by the Company, where the client/beneficial owner has not provided information as to:

(i) the full identification of the client, and
(ii) the creation of an economic profile, and/or
(iii) the completion of the suitability test, where applicable, and/or
(iv) the completion of the appropriateness test, where applicable.

The Company shall appropriately, adequately, and in a timely manner warn the client of the above procedure, including, but not limited to, the policy for handling open positions, the process for refunding deposited funds, the 15-day deadline for completing verification and the conditions under which the business relationship may be terminated. The Company shall obtain the client's explicit consent to this procedure before establishing any business relationship.

5. Risk Classification

5.1. Risk Based approach

Clients are categorized according to the risk of money laundering and terrorist financing into at least four risk categories, as follows:

Unacceptable	Failure to start or stop synergy
High	Increased due diligence
Middle	Ordinary due diligence
Low	Simplified due diligence

Depending on the risk category of each Client and/or the degree of risk of each transaction, specific management measures are taken, i.e. the required due diligence is demonstrated, distinguished as normal, simplified or enhanced.

Unacceptable Risk Category

In the category of unacceptable risk, where the start of cooperation is not allowed or an existing cooperation is interrupted, the Clients who belong to the following cases are included:

- Persons for whom there is certainty or reasonable doubt as to involvement in criminal activities, or as to membership in criminal or terrorist organizations, or as to political or other support or funding of such organizations or organizations;
- Persons who either are or should be known to have already been convicted or prosecuted for criminal offences, such as drug trafficking, misuse of public funds, money laundering, terrorism or terrorist financing, or persons against whom restrictive measures are in force, based on decisions of the European Union, OFAC or the United Nations;
- Persons for whom the conditions of certification and verification of their identity have not been met. As an exception, the certification and verification of the identity can be carried out during the conclusion of the business relationship, as long as this is required in order not to interrupt the smooth conduct of transactions and as long as the risk of committing the offenses is small;
- Persons who provide financial or insurance services without a license or control from a Supervisory Authority.

The Company must have in place policies, controls and procedures to mitigate and manage effectively the risks identified and those shall be proportionate to the nature and size of the Company.

In order to effectively manage any kind of risk identified, the Company shall apply all the appropriate measures and procedures, on a risk-based approach, so as to focus its effort in those areas where the risk of Money Laundering and Terrorist Financing appears to be higher. The Company maintains a risk-based approach policy for accepting Clients and assigns to its Clients the following risk categories:

1. High risk Clients
2. Middle risk Clients
3. Low risk Clients

The Company takes into consideration, among others, the below risk factors:

Scale and complexity of the services

When identifying the risk associated with the Clients (including the beneficial owners), the Company should consider the risk related to:

1. The Client's (and Clients' beneficial owner's) business or professional activity;
2. The Client's reputation;
3. Nature and behavior.

Countries and geographical areas risk factor

When identifying the risk associated with the countries and geographical areas, the Company may consider the risk related to:

1. The jurisdiction in which the Client and the beneficial owner are based;
2. The jurisdiction that are the Client's and beneficial owner's main places of business;
3. The jurisdiction to which the Client and beneficial owner have relevant personal links; and
4. The jurisdiction from where funds are received from or sent to.

Products, services and transactions risk factor

When identifying the risk associated with their products, services and transactions, the Company should consider the risk related to:

1. The level of transparency, or opaqueness, the product service or transaction affords;
2. The complexity of the product, service or transaction; and
3. The value or size of the product, service or transaction.

Delivery channels

When identifying the risk associated with the way in which the Client obtains the products or services they require, the Company should consider the risk related to:

1. The extent to which the business relationship is conducted on a non-face-to-face basis;
2. Any introducers or intermediaries the Company might use and the nature of their relationship with the Company.

5.2. Dynamic risk management

Risk Management is a continuous process, carried out on a dynamic basis and not an isolated event of a limited duration. Client's activities change as well as the services and financial instruments provided by the Company change. The same happens to the financial instruments and the transactions used for Money Laundering or Terrorist Financing.

In this respect, the AML and Compliance Officer undertakes regular reviews of the characteristics of existing Clients, new Clients, services and financial instruments and the measures, procedures and controls designed to mitigate any resulting risks from the changes of such characteristics. These reviews shall be duly documented, as applicable, and form part of the Annual Money Laundering Report.

5.3. Relevant International Organizations

On implementing appropriate measures and procedures on a risk-based approach, and on implementing the Client identification and due diligence procedures, the AML and Compliance Officer consults data, information and reports that are published by the following relevant international organizations:

- FATF
- The Council of Europe Select Committee of Experts on the Evaluation of Anti-Money laundering Measures (MONEYVAL)
- The EU Common Foreign & Security Policy (CFSP)
- The UN Security Council Sanctions Committees
- The International Money Laundering Information Network (IMOLIN) -
- The International Monetary Fund (IMF)
- The Joint Committee European Supervisory Authorities
- The Ministry of Foreign Affairs with regards to the UN Security Council international sanctions EU Council's restrictive measures
- The EU Sanctions Map

6. Due Diligence Measures

Based on the riskiness of the Client and/or the transaction, specific management measures are taken and the required due diligence (ordinary, simplified or enhanced) is demonstrated.

6.1. Content of Due Diligence Measures

Client due diligence measures, both at the inception and throughout the business relationship, include:

- The verification and verification of the Client's identity, based on documents, data or information, from reliable and independent sources, including any secure, remote or electronic identification process that is defined by the regulatory framework and/or recognized, approved, or accepted by the competent Authority.
- Verifying the identity of the beneficial owner and taking reasonable steps to verify it, so that the Company can be certain that it knows the beneficial owner; with regard to legal entities, so that the Company can obtain knowledge of the Client's ownership and control structure.
- The collection of information about the purpose and nature of the business relationship or significant transactions or activities of the Client or the beneficial owner.
- The examination, with particular care, of any transaction or activity, which by its nature or the way in which it is carried out or by the data concerning the person or status of the person involved in the transaction, can be linked to Money Laundering or Terrorist Financing, especially if the transaction is complex or of unusually high value, or without an obvious financial or clear legal reason.
- The exercise of continuous supervision, with regard to the business relationship, with a thorough examination of the transactions and activities of the Clients and the beneficial owners, throughout the duration of this relationship, in order to ensure that the transactions carried out or the activities that exist are consistent with the existing information about Clients, their business activities, the characteristics of the assessed risk and the origin of funds.
- Ensuring up-to-date documents, data or information regarding the supervision of the Client (periodic updating of information).
    a. If there is a change in the Client's legal status and situation such as:
        i. Change of directors/secretary,
        ii. Change of registered shareholders and/or beneficial owners,
        iii. Change of registered office,
        iv. Change of trustees,
        v. Change of corporate name and/or trading name,
        vi. Change of entity type (if a legal person);

vii. Change of the principal trading partners and/or undertake new major business activities;

b. If there is a change in the way and the rules the Client's account operates, such as:
   i. Change in the persons that are authorised to operate the account,
   ii. Application for the opening of new account for the provision of new investment services and/or financial instrument.

- Taking any appropriate measure, including not completing the transaction and refusing to provide services or carry out activities, if the conditions of certification and verification of the Client's identity have not been met, or when the Company has not ensured the observance of due diligence measures, as well as in case of subsequent submission of reports to the Authority for the Client.

6.2. Transactions that favour anonymity

In the case of Clients' transactions via the phone or fax where the Client is not present so as to verify the authenticity of their signature or that they are the real owners of the account or that they have been properly authorised to operate the account, the Company shall apply reliable methods, procedures and control mechanisms over the access to the electronic means so as to ensure that it deals with the true owner of the authorised signatory to the account.

The Company's employees shall first verify the identity of the person placing the order as follows:

- If the order is given over the phone, the person receiving the order should ask for personal identification data (i.e. ID, home address, phone number, middle name, date of birth etc.); and
- If the order is given in writing, (through fax, mail or delivery by hand) then the person receiving the order should verify the Client's signature against the specimen found in the records (legal documentation signed by the Client) kept by the Company.

Due to unacceptably high Money Laundering and Terrorist Financing risks, maintaining anonymous account or account in obviously fictious named is prohibited.

6.3. Refusal of new Clients and termination of existing

Evidence of identity must be obtained as soon as reasonably practicable after first contact and before establishing the business relationship or the execution of an occasional transaction. In the case of failure to obtain satisfactory evidence of identity of the Client in a reasonable time or the Client refuses to give information in relation to their identity, then the Company reserves the right to refuse to provide the requested service or perform a particular transaction.

The failure by a Client to provide satisfactory evidence of identity may, in itself, lead to a suspicion that the potential Client may be engaging in Money Laundering, and in such a case the Company should seriously consider reporting the case to MOKAS. In the case where, during the business relationship, the Client fail or refuse to provide updated information in a timely manner, the Company may freeze the Client accounts, return the assets where applicable and terminate the business relationship, while at the same time may examine whether it is justified, under the circumstances, to submit a report to MOKAS.

6.4. Enhanced Due Diligence

The Company applies increased due diligence measures in cases where it considers there is a high risk of Money Laundering or Terrorist Financing.
This is an indicative list of factors and types of evidence of potentially higher risk clients:

1. Client risk factors:
   a) The business relationship is conducted in unusual circumstances;
   b) Clients that are resident in geographical areas of higher risk or high-risk thord countries;
   c) Legal persons or arrangements that are personal asset-holding vehicles;
   d) Companies that have nominee shareholders or shares in bearer form;
   e) Businesses that are cash-intensive;
   f) The ownership structure of the company appears unusual or excessively complex given the nature of the company's business.
2. Product, service, transaction or delivery channel risk factors:
   a) Private banking;
   b) Products or transactions that might favour anonymity;
   c) Non-face-to-face business relationships or transactions, without certain safeguards, such as electronic signatures;
   d) Payment received from unknown or unassociated third parties;
   e) New products and new business practices, including new delivery mechanism, and the use of new or developing technologies for both new and pre-existing products.
3. Geographical risk factors:
   a) Countries identified by credible sources, such as mutual evaluations, detailed assessment reports or published follow-up reports, as not having effective AML/CFT systems;

b) Countries identified by credible sources as having significant levels of corruption or other criminal activity;

c) Countries subject to sanctions, embargos or similar measures issued by, for example, the Union or the United Nations;

d) Countries providing funding or support for terrorist activities, or that have designated terrorist organisations operating within their country.

The Company is also responsible to identify client specific issues and apply measures accordingly. Indicative are some of the following cases:

- When it is transacting with a natural person or legal entity with an establishment in a high-risk third country. (It is provided that, enhanced Client due diligence measures need not be automatically invoked with respect to branches or majority owned subsidiaries of the Company established in the European Union which are located in high-risk third countries, where those branches or majority owned subsidiaries fully comply with the group-wide policies and procedures in which case, the Company shall use the risk-based approach.)
- When the transactions are carried out with **the non-physical presence of the Client** , the Company applies one or more of the following measures to verify their identity:
  a) ensures that the Client's identity is verified with additional supporting documents, data or information;
  b) takes additional measures to check or certify the submitted documents or requires confirmatory certification from a credit institution or financial institution established in the European Union.
- When entering into business relationships with clients who are **PEPs.** The Company:
  a) Gathers sufficient information to identify whether a potential Client is or may become a PEP and has in place risk management systems and procedures that will enhance the process.
  b) Gets approval from the Senior Management before starting the relationship.
  c) It examines the origin of funds and source of wealth of the Client in question.
  d) Provided that, where a PEP is no longer entrusted with a prominent public function by the Republic or a member state or a third country, or with a prominent public function by an international organisation, a Company shall, for at least 12 months, be required to take into account the continuing risk posed by that person and apply risk sensitive measures until the risk is totally mitigated.

In addition, the Company applies increased due diligence measures to the "**Persons known to be close associates" of PEPs.**

Enhanced due diligence measured to be followed by the Company where applicable, in addition to the measures under the simplified due diligence procedure, may include:

*Increasing the **quantity** of information obtained for Client due diligence purposes:*

This may include obtaining and assessing information about the Client's or beneficial owner's reputation and assessing any negative allegations against them. Examples include:

- Information about their family members and close business partners;
- Information about their past and present business activities; and
- Adverse media searches,

Information about the intended nature of the business relationship. This may include information on:

- Number, size and frequency of transactions that are likely to pass through the account;
- Why the Client is looking for a specific product or service, in particular where it is unclear why the Client's needs cannot be met better in another way or in another jurisdiction;
- Destination of funds;
- The nature of the Client's or beneficial owner's business.

Information about the intended nature of the business relationship to ascertain that the nature and purpose of the business relationship is legitimate and to help the Company obtain a more complete Client risk profile. This may include obtaining information on:

- The number, size and frequency of transactions that are likely to pass through the account, to enable the Company to spot deviations that might give rise to suspicion (in some cases, requesting evidence may be appropriate);
- Why the Client is looking for a specific product or service, in particular where it is unclear why the Client's needs cannot be met better in another way, or in a different jurisdiction;
- The destination of funds;
- The nature of the Client's or beneficial owner's business, to enable the firm to better understand the likely nature of the business relationship.

*Increasing the **quality** of information obtained for CDD purposes to confirm the Client's or beneficial owner's identity including by:*

- Requiring the first payment to be carried out through an account verifiably in the Client's name with a bank subject to Client due diligence standards that are not less robust than those set out in Chapter II of Directive (EU) 2015/849;

- Establishing that the Client's wealth and the funds that are used in the business relationship are not the proceeds of criminal activity and that the source of wealth and source of funds are consistent with the Company's knowledge of the Client and the nature of the business relationship. The source of funds or wealth can be verified, inter alia, by reference to VAT and income tax returns, copies of audited accounts, pay slips, public deeds or independent media reports. The Company should have regard to the fact that funds from legitimate business activity may still constitute Money Laundering or Terrorist Financing.

Increasing the frequency of reviews

- Increasing the frequency of reviews of the business relationship to ascertain whether the Client's risk profile has changed and whether the risk remains manageable;
- Obtaining the approval of Senior Management to commence or continue the business relationship to ensure that Senior Management are aware of the risk their firm is exposed to and can take an informed decision about the extent to which they are equipped to manage that risk;
- Reviewing the business relationship on a more regular basis to ensure any changes to the Client's risk profile are identified, assessed and, where necessary, acted upon; or,
- Conducting more frequent or in-depth transaction monitoring to identify any unusual or unexpected transactions that might give rise to suspicion of Money Laundering and/or Terrorist Financing.

The Company is not required to apply all the EDD measures listed above in all cases. For example, in certain high-risk situations it may be appropriate to focus on enhanced ongoing monitoring during the course of the business relationship. The Company determines the frequency and intensity of monitoring on a risk-sensitive basis, taking into account the nature, size and complexity of its business and the level of risk to which it is exposed. The Company's transaction monitoring system relies on up-to-date Client information and enables the firm reliably to identify unusual and suspicious transactions and transaction patterns by setting red flags that are checked by the Compliance team without undue delay.

6.5. Simplified Due Diligence

According to the law, the Company may apply simplified client due diligence measures if the business relationship or the transaction presents a lower degree of risk. The Company needs to make sure that it collects sufficient information in order to assess and ascertain whether a business relationship or transaction presents a lower degree of risk. The Company when assessing the abovementioned needs to pay special attention to any activity of those clients or to the type of transactions which by nature may be used or abused for Money Laundering or Terrorist Financing purposes.

When assessing the risks of Money Laundering or Terrorist Financing which relate to types of clients, geographical areas and particular products, services, transactions or delivery channels, the Company needs to takes into account at least the factors listed below of potentially lower risk situations.

Non- exclusive factors and types of pptentially lower risk:

1. Client risk factors:
    a) Public companies listed on a stock exchange and subject to disclosure requirements, either by stock exchange rules or through law or enforceable means, which impose requirements to ensure adequate transparency of beneficial ownership;
    b) Public administrations or enterprises;
    c) Clients that are resident in geographical areas of lower risk
2. Product, service, transaction or delivery channel risk factors:
    a) Life insurance policies for which the premium is low;
    b) Insurance policies for pension schemes if there is no early surrender option and the policy cannot be used as collateral;
    c) A pension or similar scheme that provides retirement benefits to employees, where contributions are made by way of deduction from wages and the scheme rules do not permit the assignment of a member's interest under the scheme;
    d) Financial products or services that provide appropriately defined and limited services to certain types of Clients, so as to increase access for financial inclusion purposes;
    e) Products where the risks of Money Laundering and Terrorist Financing are managed by other factors such as purse limits or transparency of ownership such as certain types of electronic money;
3. Geographical risk factors — registration, establishment, residence in:
    a) Member States;
    b) Third countries having effective AML/CFT systems;
    c) Third countries identified by credible sources as having a low level of corruption or other criminal activity;
    d) Third countries which, on the basis of credible sources such as mutual evaluations, detailed assessment reports or published follow-up reports, have requirements to combat money laundering and terrorist financing consistent with the revised FATF Recommendations and effectively implement those requirements.

6.6. Reliance on third parties for Client identification and due diligence purposes

The Company may rely on third parties for the implementation of Client identification and due diligence procedures, provided that the third person makes immediately available all data and information, which

must be certified true copies of the originals, that were collected in the course of applying Client identification and due diligence procedures. It is provided that, the ultimate responsibility for meeting these requirements shall remain with the Company who relies on the third party.

The Company shall obtain data and information so as to verify that the third person is subject to professional registration in accordance with the competent law of its country of incorporation and/or operation as well as supervision for the purposes of compliance with the measures for the prevention of Money Laundering and Terrorist Financing.

The Company shall not rely on a third party only at the outset of establishing a business relationship or the execution of an occasional transaction for the purpose of verifying the identity of their Clients. According to the degree of risk any additional data and information for the purpose of updating the Client's economic profile or for the purpose of examining unusual transactions executed through the account, is obtained from the natural persons (directors, beneficial owners) who control and manage the activities of the Client and have the ultimate responsibility of decision making as regards to the management of funds and assets.

In the case the Company relies on a third party, shall apply the following additional measures/procedures:

- Before the establishment of the business relationship or the carrying out of the occasional transaction shall apply due diligence measures to the third party;
- Shall sign an agreement with the third party specifying the obligations of each party;
- Shall maintain a separate file for every third party of the present paragraph, where it stores the relevant information;
- The commencement of the cooperation with the third party and the acceptance of Client identification data verified by the third party is subject to approval by the AML and Compliance Officer.

The Company shall not rely on third parties established in high -risk third countries for the implementation of Client identification and due diligence procedures (branches or majority owned subsidiaries of the third parties established in the European Union, which are located in high-risk third countries shall be excluded, assuming they fully comply with their group-wide policies regarding data protection and sharing information for AML/CFT purposes).

The third parties shall forward immediately to the Company the copies of the documents obtained, as well as any relevant data and information on the identity of Client or the beneficial owner which the third party has collected when applying the above procedures and measures.

The Company shall perform a due diligence procedure on all future associates by taking into consideration factors such as member of a professional body, country of establishment or regulated entity and keep such records and any subsequent updates on file.

The Company shall examine, as far as reasonably possible, the background and purpose of all complex and unusually large transactions, and all unusual patterns of transactions, which have no apparent economic or lawful purpose and in particular, the Company shall increase the degree and nature of monitoring of the business relationship, in order to determine whether those transactions or activities appear suspicious.

6.7. Ongoing monitoring of client accounts

The Company examines and checks, on a regular basis, the validity and adequacy of the Client identification data and information it maintains, in all cases but with a special focus on high risk Clients, to ensure that existing Client information is kept updated. The AML and Compliance Officer and the whole Regulatory Compliance & AML Department will ensure that regular review and update of Clients' identification data is conducted and will take steps to obtain sufficient Client information to comply with suspicious activity reporting requirements. This will provide assurance that the Company is able to capture any material change in the Client's profile or any potential suspicious activity.

Transactions executed for the Clients are compared and evaluated against the anticipated account's turnover, the usual turnover of the activities/operations of the Client and the data and information kept for the Client's economic profile. Significant deviations are investigated, and the findings are recorded in the respective Client's file. Transactions that are not justified by the available information on the Client, are thoroughly examined so as to determine whether suspicions over Money Laundering or Terrorist Financing arise for the purposes of submitting an internal report to the AML and Compliance Officer, and then by the latter to MOKAS. In order for the investigation of the Clients' transactions to be performed, full understanding of the Clients' normal and reasonable account activity according to their economic profile shall be granted. In addition, the Company shall maintain and implement the relevant means of identifying transactions which fall outside the regular pattern of an account's activity or complex or unusual transactions or transactions without obvious economic purpose or clear legitimate reason. Without such knowledge, the Company is not able to discharge its legal obligation to identify and report suspicious transactions to MOKAS.

The procedures and intensity of monitoring accounts and examining transactions are determined on a risk-based approach as the review dates will be triggered depending on the Client's risk category. The reviews are planned as below:

Risk category	Monitoring intensity
High Risk	every year
Middle Risk	every 2 years
Low Risk	every 2 years

The outcome of the said review is recorded in a separate note/form, which is kept in the respective Client's file. The monitoring procedure shall achieve, as a minimum, the following:

a) Identifying all high risk Clients. Therefore, the systems or the measures and procedures of the Company are able to produce detailed lists of high-risk Clients so as to facilitate enhanced monitoring of accounts and transactions;

b) Detecting of unusual or suspicious transactions that are inconsistent with the economic profile of the Client for the purposes of further investigation;

c) The investigation of unusual or suspicious transactions and the preparation of a separate memo where the results of the investigation will be recorded;

d) All necessary measures and actions must be taken, based on the investigation's findings, including any internal reporting of suspicious transactions/activities to the Compliance ofifcer;

e) Ascertaining the source and origin of the funds credited to accounts.

The Company shall introduce and implement, where appropriate and proportionate, in view of the nature, scale and complexity of its business and the nature and range of the investment services and activities undertaken in the course of that business, adequate automated electronic management information systems which will be used in the investigation of Clients' transactions and be capable of supplying the Board and the AML and Compliance Officer, on a timely basis, all the valid and necessary information for the identification, analysis and effective monitoring of Client accounts and transactions based on the assessed risk for Money Laundering or Terrorist Financing purposes.

The relevant electronic management information systems shall be capable to extract a list of data and information that is missing regarding the Client identification and the construction of a Client's economic

profile. In addition, the system may allow automated reminders as regard the expiration of certain identification documents like passports and utility bills as well as reminders for the KYC review of the Clients' accounts, by sending automated emails. The monitoring of accounts and transactions are carried out in relation to specific types of transactions and economic profile, as well as by comparing periodically the actual movement of the account with the expected turnover as declared at the establishment of the business relationship.

For all the Clients' accounts, automated electronic management information systems shall be able to add up the movement of all related accounts on a consolidated basis and detect unusual or suspicious activities and types of transactions. This can be done by setting limits for a particular type, or category of accounts (e.g. high-risk accounts) or transactions (e.g. deposits and withdrawals in cash, transactions that do not seem reasonable based on usual business or commercial terms, significant movement of the account incompatible with the size of the account balance), taking into account the economic profile of the Client, the country of his origin, the source of the funds, the type of transaction or other risk factors. The Company shall give particular attention to transactions exceeding the abovementioned limits, which may indicate that a Client might be involved in unusual or suspicious activities.

7. Reporting to MOKAS

At a first step, the AML and Compliance Officer receives information from the Company's employees in relation to knowledge or suspicious of Money Laundering or Terrorist Financing activities and then, prepares a written report, known as the Internal Suspicion Report (Annex II), with all the information provided by the relevant member of staff. The information included in the report will be evaluated in detail by the AML and Compliance Officer, in the light of all other relevant information, for the purpose of determining whether or not the information or other matter contained in the report proves this fact or creates such a suspicion and so a report shall be submitted to MOKAS. In order for the AML and Compliance Officer to effectively review the incident, he/she shall have direct and timely access to any information, data and documents that are available to the Company. The results of the evaluation and review performed by AML and Compliance Officer and the decision made will be documented and explained in written form (Annex III).

If, following the evaluation, there are reasonable suspicions that monetary sums constitute proceeds of illegal activities or relate to Terrorist Financing and the AML and Compliance Officer decides that MOKAS should be notified, a report is submitted to MOKAS through the electronic portal goAML

http://www.law.gov.cy/Law/MOKAS/MOKAS.nsf/All/8D5B6DF6DC5D5815C2257BE1002A2848?OpenDocument

It is noted that, in the case the AML and Compliance Officer knows or has reasonable suspicion that monetary sums, irrespective of their exact amount, constitute proceeds of illegal activities or relate to Terrorist Financing, the Company needs to ensure that MOKAS is immediately notified, by submitting the relevant report and providing complimentary information if requested. The AML and Compliance Officer is obliged to report to MOKAS any attempt to carry out such suspicious transactions as well.

After submitting the report to MOKAS, the Company shall adhere to any instructions given by MOKAS, as to whether or not to continue or suspend a particular transaction or to maintain the particular account active, in an effort to avoid any frustration to the investigations conducted. On the other hand, MOKAS may not give such instructions to the Company, but the Company itself may subsequently wish to terminate its relationship with the Client concerned for risk avoidance reasons. In such a case, the Company exercises particular caution not to alert the Client concerned that a suspicion report has been submitted to MOKAS.

Furthermore, after the submission of a suspicion report, the Clients' accounts concerned, as well as any other connected accounts, are placed under the close monitoring of the AML and Compliance Officer.The Company, its employees and directors are prohibited from disclosing to the involved Client or third parties that information has been duly transmitted or requested, or that an investigation into money laundering or terrorist financing is being or may be or will be conducted.

The disclosure of information in good faith by the Company or by an employee or director of the Company, shall not constitute a breach of any restriction on disclosure of information imposed by contract or by any legislative, regulatory or administrative provision, and shall not involve the Company or its employees and directors in liability of any kind even in circumstances where they were not precisely aware of the underlying criminal activity and regardless of whether the illegal activity actually occurred. Finally, a person who submits an Internal Suspicion Report (Annex III), or a Report to MOKAS for suspicious transactions pursuant to the provisions of the AML Law and AML Directive, is protected from being exposed to threats or hostile action, and in particular from adverse or discriminatory employment actions.

The report will be prepared manually online on the web application of goAML system at http://www.law.gov.cy/Law/MOKAS/MOKAS.nsf/All/8D5B6DF6DC5D5815C2257BE1002A2848?OpenDocument. The system will allow saving of draft reports and other features that will assist the AML and Compliance Officer to prepare the report. The system will allow attaching to the report relevant documents. This option is more time consuming since all relevant fields should be filled-in in the system.

The AML and Compliance Officer must ensure that in the case of a suspicious transaction investigation by MOKAS, he/she will be able to provide without delay the following information:

a) The identity of the account holders;
b) The identity of the beneficial owners of the account;
c) The identity of the persons authorised to manage the account;
d) Data of the volume of funds or level of transactions flowing through the account;
e) Connected accounts;
f) In relation to specific transactions:

- The origin of the funds
- The type and amount of the currency involved in the transaction
- The form in which the funds were placed or withdrawn, for example cash, cheques, wire transfers
- The identity of the person that gave the order for the transaction
- The destination of the funds
- The form of instructions and authorization that have been given
- The type and identifying number of any account involved in the transaction

8. Trainings

The effectiveness of this Policy is based on the existence of comprehensive and modern educational programs that respond to changing conditions, according to the AML Law and AML Directive, by introducing a complete education and training program.

The timing and content of the training provided to the employees of the various departments is adjusted according to the needs of the Company. The frequency and timing can vary depending on to the amendments of legal and/or regulatory requirements and employees' duties. In such cases, the AML and Compliance Officer takes all the reasonable measures, after obtaining the approval by the Board, customizing the training program of the Company's employees in order to ensure that they are updated accordingly.

As a consequence of this, the Company establishes training programs (in person or by sending electronic material) which are repeated at regular intervals, in order to ensure that the staff has full knowledge of their duties and obligations, while being kept informed of any new developments.

The training program aims at educating employees on the latest developments in the prevention of Money Laundering and Terrorist Financing, including the practical methods and trends used for this purpose. The training program shall have a different structure for new and existing employees, as well as for different

departments of the Company, according to the services that they provide. This means that each department of the Company shall have its own training scheme.

The Company's annual training program should be submitted to the Board for approval.

9. Record keeping

All data and information collected by the Company are kept in paper or electronic form for a period of five (5) years after the end of the business relationship with the Client or the date of the occasional transaction. Upon expiration of the period of five (5) years, the Company may delete personal data, unless the documents are used to any ongoing investigations, in which case are kept until MOKAS confirms that the investigation has been completed and the case has been closed.

The Company keeps the following documents and information to be used in any investigation or investigation of a potential attempt or commission of AML/CFT carried out by the Authority, the Company's Internal Audit, or any other competent public authority:

a) The documents and information required to comply with its due diligence obligations are set out above, including information obtained through any secure, remote or electronic identification process, as defined by the regulatory framework and/or recognized, approved or is accepted by the competent Authority.

b) The supporting evidence and records of all business relations and transactions which are necessary for the determination of the transactions and their recording;

c) The relevant documents regarding the correspondence with Clients and other persons with whom the Company maintains a business relationship;

d) In the case of Client due diligence performed by a third party, evidence of the evaluation of the systems and procedures used by the third party that the Company relies on for the Client identification and due diligence;

e) The records of any reports related to suspicious transactions submitted to the Compliance officer and/or MOKAS.

The above documents shall be made available without delay to MOKAS and the CySEC, for the purpose of discharging the duties imposed on them by the AML Law, as the information may be used as evidence in any subsequent investigation by the authorities. The records kept by the Regulatory Compliance & AML

Department provide audit trail evidence during any subsequent investigation. In practice, the business units of the Company will be routinely making records of work carried out for Clients in the course of normal business and these records should be archived.

The documents/data obtained, for compliance with the AML Directive, must be in their original form or certified true copy form. In the case that the documents are certified as true copies by a different person than the Company itself or by the third person that the Company relied for the KYC procedures, the documents/data must be apostilled or notarized.

A true translation is attached in the case that the documents/data are in a language other than Greek or English.

Client identification documents obtained prior to conducting a business relationship or during the Client file review stage should always be recent (one year from the issue date where applicable) and always up to date. Documents relating to the verification of the Client's resident address and/or bank references are considered recent when submitted to the Company within six (6) months form the issue date.

The responsibility for the acceptability or otherwise of any unduly certified copies submitted to the Company lies with the AML and Compliance Officer. However, the Company shall not be liable for any forged documents, except where it was aware or should have been aware of the forgery. The Company and the approved persons shall be entitled to rely on the truth of duly certified documents submitted by the Client in original form or in duly certified copies, except where the Company and the approved persons are in any way aware or should have been aware that the documents submitted by the Client are not accurate or provide misleading information.

10. Processing of personal data

The processing of any kind of personal data shall be carried out for the purposes of the prevention of the Money Laundering and Terrorist Financing and shall not be further processed in a way that is incompatible with these purposes, as this is prohibited.

The Company shall provide new Clients with the following:

a) Information required pursuant to Article 11(1) of the Processing of Personal Data and for the Free Movement of such Data Law of 2018 before the establishment of the business relationship or the carrying out of an occasional transaction; and

b) Information, prior to the commencement of a business relationship or the execution of an occasional transaction, on the processing to which the personal data is subjected pursuant to the provisions of the Law for purposes of prevention of Money Laundering and Terrorist Financing.

The access rights to the data subject, may be lifted in whole or in part in accordance with the provisions of the processing of personal data (Protection of the Individual) Law, for purposes of proper fulfilment of the duties of Companies and supervisory authorities or to avoid obstruction of official or legal inquiries, analyses, investigations or procedures for the purposes of the present Law and to ensure that prevention, investigation and detection of Money Laundering and Terrorist Financing is not jeopardized.

11. Update of the Policy

This Policy is created, owned and maintained by the Regulatory Compliance & AML Department, which is responsible for maintaining version series, original requests, and supporting documentation with all relevant approvals of this Policy.

The Policy is reviewed at frequent intervals and will be updated whenever such a need arises and clients are notified in writing.

Some of the circumstances that can trigger the review process are the identification of situations that are not adequately captured in the Policy and updates in the applicable legislative and regulatory framework.

Annexes

Annex I – Know Your Client (KYC) Form

Date:

Name/Name of Client:

Client Type:

Individual / Legal Entity

I. GENERAL CLIENT DETAILS

Individual

LAST NAME : _____

NAME : _____

FATHER'S NAME : _____

MATRONNAME: _____

DATE OF BIRTH : _____

PLACE OF BIRTH: _____ NATIONALITY: _____

ID number: _____ DATE: _____ PUBLICATION START: _____

TRANSIT NO. : _____ DATE: _____ EDIT. START : _____

VAT number: _____ D.O. Y _____

ADDRESS : _____

P.C. : _____ CITY : _____ TEL :_____ _____

PROFESSION : _____

PROFESSIONAL ADDRESS: _____

P.C. : _____ CITY : _____ TEL :_____

Legal Entity

CORPORATE NAME / TRADE TITLE :

_____

_____

LEGAL FORM _____

NO. OF RECOMMENDATION_____ DATE_____

AUTHORITY OF APPROVAL OF RECOMMENDATION

_____

A.M.A.E. _____ HEADQUARTERS _____

DEED OF REGISTRATION. COMPANY OF CONTRACT (for LLC)

_____

ADDRESS _____ P.O. _____

TAX DOMICILE _____

VAT NUMBER. _____ D.O.Y. _____

TELEPHONE _____

PURPOSE / TYPE OF ACTIVITY _____

Identity Details of Legal Representatives of a Legal Entity

LAST NAME : _____

NAME :_____

FATHER'S NAME : _____

MATRONNAME: _____

DATE OF BIRTH : _____

PLACE OF BIRTH: _____ NATIONALITY: _____

ID number: _____ DATE: _____ PUBLICATION START: _____

TRANSIT NO. : _____ DATE: _____ EDIT. START: _____

VAT number: _____ D.O. Y _____

ADDRESS : _____

P.C. : _____ CITY : _____ TEL : _____

PROFESSION : _____

PROFESSIONAL ADDRESS: _____

P.C. : _____ CITY : _____ TEL : _____

Beneficial Beneficiary Identification Details

LAST NAME : _____

NAME : _____

FATHER'S NAME : _____

MATRONNAME: _____

DATE OF BIRTH: _____ PLACE OF BIRTH: _____

ID: _____ DATE: _____ EDIT. START: _____

TRANSIT NO. : _____ DATE: _____ EDIT. START: _____

VAT number: _____ D.O. Y _____

ADDRESS : _____

P.C. : _____ CITY : _____ TEL : _____

PROFESSION : _____

BUSINESS ADDRESS: _____

P.C. : _____ CITY : _____ TEL : _____

II. CLIENT FINANCIAL/TRADING PROFILE DETAILS

1. Client's source of income

Wages/Pensions/Income from Professional activity

Corporate profits

Income from real estate

Income from money

Loan from PI

Donations

Other

Describe in detail: _____

2. Purpose for which a business relationship is entered into

Describe in detail: _____

3. Estimated movement of the account on an annual basis

☐	< €49,999
☐	€50,000 - €99,999
☐	€100,000 - €499,999
☐	€500,000 - €999,999
☐	€1,000,000 - €1,499,999
☐	€1,500,000 - €4,999,999
☐	€5,000,000 - €9,999,999
☐	>10,000,000

4. Country origin / destination of funds

Most common countries of origin/destination _____

_____

_____

Name and Signature of Client/Legal Representative

Annex II – Internal Suspicion report

INTERNAL SUSPICION REPORT FOR MONEY LAUNDERING AND TERRORIST FINANCING

INFORMER'S DETAILS

Name: ..... Tel: .....

Department: ..... Fax: .....

Position: .....

CUSTOMER'S DETAILS

Name: ....

Address: ....

..... Date of Birth: .....

Tel: ..... Occupation:.....

Fax: ..... Details of Employer: .....

.....

Passport No.: ..... Nationality: .....

ID Card No.: ..... Other ID Details: .....

INFORMATION/SUSPICION

Brief description of activities/transaction: ....

....

Reason(s) for suspicion: ....

....

Informer's Signature Date

....

FOR COMPLIANCE OFFICER'S USE

Date Received: ..... Time Received: ..... Ref. .....

Reported to MOKAS: Yes/No ... Date Reported: ..... Ref .....

Annex III – Internal Evaluation Report

INTERNAL EVALUATION REPORT FOR MONEY LAUNDERING AND TERRORIST FINANCING

Reference: ..... Customer's Details: .....

Informer: ..... Department: .....

INQUIRIES UNDERTAKEN (Brief Description)

.....
.....
.....

ATTACHED DOCUMENTS

.....
.....
.....
.....

COMPLIANCE OFFICER'S DECISION

.....
.....
.....

FILE NUMBER .....

COMPLIANCE OFFICER'S SIGNATURE DATE

....

Annex IV – Specific client identification cases

A. Natural persons residing in the Republic

a) The Company ascertain the true identity of natural persons who are residents of the Republic Cyprus by obtaining the following information:

   i. True name and/or names used as these are sated on the official identity card or passport, ii. full permanent address in the Republic, including postal code,
   ii. Telephone (home and mobile) and fax numbers,
   iii. E-mail address, if any,
   iv. Date and place of birth,
   v. Nationality and
   vi. Details of the profession and other occupations of the Client including the name of employer/business organisation.

b) The acceptable method for the verification of the identification of a Client's identity is the reference to an original document which is issued by an independent and reliable source that carries the Client's photo. After the Company is satisfied for the Client's identity from the original identification documents presented, it keeps copies of the pages containing all relevant information which are certified, by the Company, as true copies of the original documents.

c) In addition to the name verification, it is important that the Client's permanent address is also verified by using one of the following ways:

   i. Visit at the place of residence (in such a case, the Company's officer who carries out the visit prepares a memo which is retained in the Client's file), and
   ii. The production of a recent (up to 6 months) utility bill, local authority tax bill or a bank statement or any other document same with the aforesaid (to protect against forged or counterfeit documents, the prospective Clients are required to produce original documents).

d) In addition to the above, the procedure for the verification of a Client's identity is reinforced if the said Client is introduced by a reliable staff member of the Company, or by another existing reliable Client who is personally known to a member of the Board of Directors. Details of such introductions are kept in the Client's file.

B. Natural persons not residing in the Republic

a) For Clients who are not normally residing in the Republic, in addition to the information collected according to point 1 above, the Company, without prejudice to the application on a risk-sensitive basis, shall require and receive information on public positions which the prospective Client holds or held in the last twelve months as well as whether he is a close relative or associate of such individual, in order to verify if the Client is a PEP, according to point 9 of this Annex.

b) For those Clients not residing in the Republic, passports shall always be requested and, if available, official national identity cards issued by competent authorities of their country of origin shall be obtained and certified true copies of the pages containing the relevant information from the said documents are obtained and kept in the Client's files. In addition, it is advised, if in doubt for the genuineness of any document (passport, national identity card or documentary evidence of address), to seek verification of identity with an Embassy or the Consulate of the issuing country or a reputable credit or financial institution situated in the Client's country of residence.

c) In addition to the aim of preventing Money Laundering and Terrorist Financing, the abovementioned information is also essential for implementing the financial sanctions imposed against various persons by the United Nations and the European Union. In this regard, passport's number, issuing date and country as well as the Client's date of birth always appear on the copies of documents obtained, so that the Company would be in a position to verify precisely whether a Client is included in the relevant list of persons subject to financial sanctions which are issued by the United Nations or the European Union based on a United Nations Security Council's Resolution and Regulation or a Common Position of the European Union's Council respectively.

C. Joint accounts

In the cases of joint accounts of two or more persons, the identity of all individuals that hold or have the right to manage the account, shall be verified according to the procedures set in points 1 and 2 above.

D. Accounts of unions, societies, clubs, provident funds and charities

In the case of accounts in the name of unions, societies, provident funds and charities, the Company shall ascertain their purpose of operation and verifies their legitimacy by requesting the production of the articles and memorandum of association/procedure rules and registration documents with the competent governmental authorities (in case the law requires such registration). Furthermore, the Company shall obtain a list of the members of Board of Directors/management committee of the abovementioned

organisations and verify the identity of all individuals that have been authorised to manage the account, according to the procedures set in points 1 and 2 above.

E. Accounts of unincorporated businesses, partnerships and other persons with no legal substance

a) In the case of unincorporated businesses, partnerships and other persons with no legal substance, the identity of the directors, partners, beneficial owners and other individuals who are authorised to manage the account shall be verified according to the procedures set in points 1 and 2 above. In addition, in the case of partnerships, the original or a certified true copy of the partnership's registration certificate shall be obtained.

b) The Company shall obtain documentary evidence of the head office address of the business, ascertain the nature and size of its activities and receive all the information required for the construction of the economic profile of the business.

c) The Company shall request, in cases where exists, the formal partnership agreement and also obtain mandate from the partnership authorising the opening of the account and confirming authority to a specific person who will be responsible for its operation.

F. Accounts of legal persons

a) The Company shall take all necessary measures for the full ascertainment of the legal person's control and ownership structure as well as the verification of the identity of the natural persons who are the beneficial owners and exercise control over the legal person.

b) The verification of the identification of a legal person that requests the establishment of a business relationship or the execution of an occasional transaction, comprises the ascertainment of the following:

i. the registered number,

ii. the registered corporate name and trading name used,

iii. the full addresses of the registered office and the head offices,

iv. the telephone numbers, fax numbers and e-mail address,

v. the members of the board of directors,

vi. the individuals that are duly authorised to operate the account and to act on behalf of the legal person,

vii. the beneficial owners of private companies and public companies that are not listed in a regulated market of a European Economic Area country or a third country which is categorised by the Company as lower risk,

viii. the registered shareholders that act as nominees of the beneficial owners,

ix. the economic profile of the legal person.

c) For the verification of the identity of the legal person, the Company requests and obtains, inter alias, original or certified true copies of the following documents:

i. certificate of incorporation and certificate of good standing of the legal person,

ii. certificate of registered office,

iii. certificate of directors and secretary,

iv. certificate of registered shareholders in the case of private companies and public companies that are not listed in a regulated market of a European Economic Area country or a third country, which is categorised by the Company as lower risk,

v. memorandum and articles of association of the legal person,

vi. a resolution of the Board of Directors of the legal person for the opening of the account and granting authority to those who will operate it,

vii. in the cases where the registered shareholders act as nominees of the beneficial owners, a copy of the trust deed/agreement concluded between the nominee shareholder and the beneficial owner, by virtue of which the registration of the shares on the nominee shareholder's name on behalf of the beneficial owner has been agreed,

viii. documents and data for the verification, according to the provisions of the present Directive, the identity of the persons that are authorised by the legal person to operate the account, as well as the registered shareholders and beneficial owners of the legal person.

d) Where deemed necessary for a better understanding of the activities, sources and uses of funds/assets of a legal person, the Company obtains copies of its latest audited financial statements (if available), and/or copies of its latest management accounts.

e) For legal persons incorporated outside the Republic, the Company requests and obtains documents similar to the above.

f) As an additional due diligence measure, on a risk-sensitive basis, the Company may carry out a search and obtain information from the records of the Registrar of Companies and Official Receiver of the Republic (for domestic companies) or from a corresponding authority in the company's (legal person's) country of incorporation (for foreign companies) and/or request information from other sources in order to establish that the applicant company (legal person) is not, nor is in the process of being dissolved or liquidated or struck off from the registry of the Registrar of Companies and Official Receiver and that it continues to be registered as an operating company in the records of the Registrar of Companies and Official Receiver of the Republic or by an appropriate authority outside the Republic.

It is stressed that, if at any later stage any changes occur in the structure or the ownership status or to any details of the legal person, or any suspicions arise emanating from changes in the nature of the transactions performed by the legal person via its account, then it is imperative that further enquiries should be made for ascertaining the consequences of these changes on the documentation and information held by the Company for the legal person and all additional documentation and information for updating the economic profile of the legal person is collected.

g) In the case of a Client-legal person that requests the establishment of a business relationship or the execution of an occasional transaction and whose direct/immediate and principal shareholder is another legal person, registered in the Republic or abroad, the Company, before establishes a business relationship or executes an occasional transaction, verifies the ownership structure and the identity of the natural persons who are the beneficial owners and/or control the other legal person.

h) Apart from verifying the identity of the beneficial owners, the Law requires that the persons who have the ultimate control over the legal person's business and assets are identified. In the cases that the ultimate control rests with the persons who have the power to manage the funds, accounts or investments of the legal person without requiring authorisation and who would be in a position to override the internal procedures of the legal person, the Company verifies the identity of the natural persons who exercise ultimate control as described above even if those persons have no direct or indirect interest or an interest of less than twenty fine per cent (25%) plus one (1) in the legal person's ordinary share capital or voting rights.

i) In cases where the beneficial owner of a legal person, requesting the establishment of a business relationship or the execution of an occasional transaction, is a trust set up in the Republic or abroad, the Company implements the procedure mentioned in this Policy.

G. Investment funds, mutual funds and firms providing financial or investment services

a) The Company may establish and maintain business relationships or execute occasional transactions with persons who carry out the above services and activities which are incorporated and/or operating in countries of the European Economic Area or a third country which, provided that, is categorised by the Company as lower risk:

   i. the said persons possess the necessary license or authorisation from a competent supervisory/regulatory authority of the country of their incorporation and operation to provide the said services, and

   ii. are subject to supervision for the prevention of Money Laundering and Terrorist Financing purposes.

b) In the case of the establishment of a business relationship or the execution of an occasional transaction with persons who carry out the above services and activities and which are incorporated and/or operating in a third country other than those mentioned in point (a) above, the Company requests and obtains, in addition to the abovementioned, in previous points, documentation and the information required for the identification and verification of persons, including the beneficial owners, the following:

   i. a copy of the license or authorisation granted to the said person from a competent supervisory/regulatory authority of its country of incorporation and operation, whose authenticity should be verified either directly with the relevant supervisory/regulatory authority or from other independent and reliable sources, and

   ii. adequate documentation and sufficient information in order to fully understand the control structure and management of the business activities as well as the nature of the services and activities provided by the Client.

c) In the case of investment funds and mutual funds the Company, apart from identifying beneficial owners, obtains information regarding their objectives and control structure, including documentation and information for the verification of the identity of investment managers, investment advisors, administrators and custodians.

H. Nominees or agents of third persons

a) The Company takes reasonable measures to obtain adequate documents, data or information for the purpose of establishing and verifying the identity, according to the procedures set in the abovementioned points:

   i. The nominee or the agent of the third person, and

   ii. Any third person on whose behalf the nominee or the agent is acting.

b) In addition, the Company obtains a copy of the authorisation agreement that has been concluded between the interested parties.

I. PEP's accounts

a) When the Company establishes a business relationship or carries out an occasional transaction with PEPs, the Company should apply enhanced due diligence measures. Without prejudice of the relevant provisions of the Law, in this case the Company should apply the below additional enhanced due diligence measures:

   i. Puts in place appropriate risk management procedures to enable it to determine whether a prospective Client is a PEP. Such procedures may include, depending on the degree of risk,

the acquisition and installation of a reliable commercial electronic database for PEPs, seeking and obtaining information from the Client himself or from publicly available information. In the case of legal entities and arrangements, the procedures aim at verifying whether the beneficial owners, authorised signatories and persons authorised to act on behalf of the legal entities and arrangements constitute PEPs. In case of identifying one of the above as a PE, then automatically the account of the legal entity or arrangement should be subject to the relevant procedures specified in the Law and the Directives.

ii. The decision for establishing a business relationship or the execution of an occasional transaction with a PEP is taken by a senior management person of the Company and the decision is then forwarded to the AML and Compliance Officer. When establishing a business relationship with a Client (natural or legal person) and subsequently it is ascertained that the persons involved are or have become PEPs, then an approval is given for continuing the operation of the business relationship by a senior management person of the Company which is then forwarded to the AML and Compliance Officer.

iii. Creates the economic profile of the Client; the details of the expected business and nature of activities of the Client forms the basis for the future monitoring of the account. The profile should be regularly reviewed and updated with new data and information. The Company is particularly cautious and most vigilant where its Clients are involved in businesses which appear to be most vulnerable to corruption such as trading in oil, arms, cigarettes and alcoholic drinks.

iv. The account is subject to annual review in order to determine whether to allow its continuance of operation. A short report is prepared summarizing the results of the review by the person who is in charge of monitoring the account. The report is submitted for consideration and approval to the board of directors and filed in the Client's personal file.

J. Trust accounts

When the Company establishes a business relationship or carries out an occasional transaction with trusts:

- Must ascertain the legal substance, the name and the date of establishment of the trust and verify the identity of the trustor, trustee and beneficial owners, according to the Client identification procedures prescribed in the Law and the Directive.
- Ascertains the nature of activities and the purpose of establishment of the trust as well as the source and origin of funds requesting the relevant extracts from the trust deed and any other

relevant information from the trustees. All relevant data and information should be recorded and kept in the Client's file.

K. 'Client Accounts' in the name of third persons

a) The Company may open "Client accounts" (e.g. omnibus accounts) in the name of Companies ('third persons') from European Economic Area countries or a third country, which is categorised by the Company as lower risk.

b) In these cases, the Company:

   i. applies Client identification procedures and due diligence measures to the third person prescribed in the Law and the Directive.

   ii. ascertains that the third person is subject to mandatory professional registration in accordance with the relevant laws of the country of operation and

   iii. ascertains that the third person is subject to regulation and supervision by an appropriate competent authority in the country of operation for anti-Money Laundering and Terrorist Financing purposes.

Annex V – List of Factors of Potentially Lower Risk

Indicative list of factors and types of evidence of potentially lower risk referred to in Section 4.3. of this Policy.

(1) Client risk factors:

a. public companies listed on a stock exchange and subject to disclosure requirements (either by stock exchange rules or through law or enforceable means), which impose requirements to ensure adequate transparency of beneficial ownership;
b. public administrations or enterprises;
c. clients that are resident in geographical areas of lower risk as set out in point (3);

(2) Product, service, transaction or delivery channel risk factors:

a. life insurance policies for which the premium is low;
b. insurance policies for pension schemes if there is no early surrender option and the policy cannot be used as collateral;
c. a pension, superannuation or similar scheme that provides retirement benefits to employees, where contributions are made by way of deduction from wages, and the scheme rules do not permit the assignment of a member's interest under the scheme;
d. financial products or services that provide appropriately defined and limited services to certain types of customers, so as to increase access for financial inclusion purposes;
e. products where the risks of money laundering and terrorist financing are managed by other factors such as purse limits or transparency of ownership (e.g. certain types of electronic money);

(3) Geographical risk factors:

a. Member States;
b. third countries having effective AML/CFT systems;
c. third countries identified by credible sources as having a low level of corruption or other criminal activity;
d. third countries which, on the basis of credible sources such as mutual evaluations, detailed assessment reports or published follow-up reports, have requirements to combat money laundering and terrorist financing consistent with the revised FATF Recommendations and effectively implement those requirements or included in the EU Commission list of high risk third countries.