REPUBLIC  OF CYPRUS

INSURANCE COMPANIES CONTROL SERVICE

Orders for Life-Insurance Undertakings and Life-Insurance Intermediaries in accordance with Article 59(4) of the PREVENTION AND SUPPRESSION OF MONEY LAUNDERING ACTIVITIES LAW OF 2007-2019

(Fifth Edition)

December 2019

TABLE OF CONTENTS

Introduction

(i) In 1992, the Republic of Cyprus enacted the first Law by which money laundering deriving from drug trafficking was criminalized. Few years later, in 1996 the Republic of Cyprus enacted "The Prevention and Suppression of Money Laundering Activities Law" defining and criminalizing money laundering deriving from all serious criminal offences. The said law was subsequently amended to adopt new international initiatives and standards in the area of money laundering, including the 2nd European Union Directive for the prevention of the use of the financial system for the purpose of money laundering (Directive 91/308/EEC).

(ii) On 13/12/2007 the House of Representatives enacted "The Prevention and Suppression of Money Laundering Activities Law" (hereinafter to be referred to as "the Law") by which the former Laws on the prevention and suppression of money laundering activities of 1996-2004 were consolidated, revised and repealed. Under the Law, which came into force on 1 January 2008, the Cyprus legislation was harmonized with the 3rd European Union Directive on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing (Directive 2005/60/EC). The Law was amended in the following years in order to adopt international standards and best practices enhancing the mechanisms to prevent money laundering and terrorist financing.

(iii) On the 3 April 2018 the amending law came into force for harmonizing purposes with the 'Directive (EU) 2015/849 of the European Parliament regarding the prevention of the use of the financial system for the legalization of funds from illegal activities or for terrorist financing, the amendment of the EU Regulation 648/2012 of the European Parliament and Council, and the abolition of the Directive 2005/60/EC of the European Parliament and Council and of the Directive 2006/70/EC of the Commission'[1] hereinafter to be referred to as 'EU Directive'. The Law in these Orders is considered to be the basic Law and all its subsequent amendments. Furthermore, the Law has been revised once more with very minor changes, on 31 May, 2019, based on the 4th Money Laundering Directive, as referred to above.

(iv) The present Orders (hereinafter to be referred to as "the Orders") issued by the Superintendent of Insurance are for Life-Insurance Undertakings and Life-Insurance Intermediaries (hereinafter to be referred to as "Obliged Entities") in accordance with Article

[1] https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32015L0849&from=EN

59(4) of the Prevention and Suppression of Money Laundering Activities Laws of 2007 to 2019 ("The Law"). Regarding insurance intermediaries, special consideration should be provided to the characteristics of insurance intermediaries who are under a contractual obligation to conduct insurance distribution business exclusively with one or more insurance undertakings (tied insurance intermediaries) and should apply appropriate and proportionate measures and controls.

(v) The present orders aim to provide guidance to obliged entities for defining policy, procedures and control systems for compliance with the Law provisions and with ultimate aim the effective prevention of money laundering and terrorist financing. It is emphasized that the Law explicitly states that Orders are directly binding and compulsory as regards their implementation by all persons to whom they are addressed. Furthermore, the Law assigns to the supervisory authorities, including the Superintendent of Insurance, the duty of monitoring, evaluating and supervising the implementation of the requirements of the Law and of the Orders issued to the supervised entities.

(vi) From 1999 up to 2019, the Superintendent of Insurance issued several Orders and circulars to obliged entities operating in Cyprus, recommending the introduction of specific measures against the use of the financial system for the purpose of anti-money laundering and combat terrorist financing. As from 1999, the Superintendent of Insurance, exercising its powers emanating from the Law enacted in 1996, proceeded with the issue of a series of Orders to all obliged entities operating in Cyprus prescribing the practices and procedures that they should adopt so as to comply with the requirements of the relevant legislation in force.

(vii) The Superintendent of Insurance may issue circulars and guidelines for the implementation of the Legal and Regulatory framework aiming to the compliance of the obliged entities which should be considered and implemented by obliged entities.

1. INTERNAL CONTROL PROCEDURES AND RISK MANAGEMENT

1.1. Obligation to establish procedures

1.1.1. ***The Law Article 58*** requires from obliged entities to implement adequate and appropriate policies, controls and procedures, which are proportionate to their nature and size, so as to mitigate and manage effectively the risks of money laundering and terrorist financing, in relation to the following:

(i) Customer identification and customer due diligence.

(ii) Record keeping

(iii) Internal reporting and reporting to the Unit for Combating Money Laundering (MOKAS)

(iv) Internal control, risk assessment and risk management in order to prevent money laundering and terrorist financing

(v) Detailed examination of each transaction which by its nature may be considered to be particularly vulnerable to be associated with money laundering offences or terrorist financing, and in particular complex or unusually large transactions and all other unusual patterns of transactions which have no apparent economic or visible lawful purpose

(vi) Briefing and regular training of staff

(vii) Risk assessment practices

(viii) Compliance management, and

(ix) Recruitment and assessment of employees' integrity.

1.1.2. The Board of Directors, the Senior Management and, of supervised entities in Cyprus (including European Branches which operate in Cyprus under the Freedom of Establishment – FOE), holds the final responsibility for ensuring that the obliged entity applies an effective system to prevent money laundering and terrorist financing. Therefore, they have the ultimate responsibility to ensure that appropriate and effective systems and procedures for internal control have been introduced and applied, which reduce the risk of the products and services of the company to be used for money laundering or terrorist

financing. The commitment of Senior Management for the implementation of the above measures is a key element for the design and implementation of a risk-based approach.

1.1.3. According to ***Article 58C of the Law***, the Senior Management of the obliged entity approves the policies, procedures and controls applied by the obliged entity in relation to money laundering and terrorist financing, as well as monitor, and where appropriate, enhance the measures adopted.

1.1.4. According to ***Article 2 of the Law*** 'senior management' means an officer or employee with sufficient knowledge of the obliged entity's money laundering and terrorist financing risk exposure and sufficient seniority to take decisions affecting its risk exposure, and need not, in all cases, be a member of the Board of Directors.

1.1.5. The policies and procedures of the obliged entities should clarify how the Senior Management intends to establish an appropriate system of internal control for the prevention of money laundering and terrorist financing. This includes the definition of a framework, which will specify the duties and responsibilities of the persons responsible for the implementation of specific aspects of the policy. Additionally, effective procedures should include appropriate management supervision, systems and controls, segregation of duties, training and other relevant practices.

1.1.6. ***Article 58D of the Law*** requires from obliged entities to designate a member of the Board of Directors, provided there is a board of directors, which shall be responsible for the implementation of the Law, Orders and circulars and/or regulations issued by the Superintendent of Insurance based on the Law, and any other relevant acts of the European Union.

1.1.7. The Insurance Undertaking appoints a member of the Board of Directors who will be responsible for the implementation of the Law, the Orders, circulars and/or regulations issued by the Superintendent of Insurance based on the Law, and any other relevant acts of the European Union and communicates immediately to the Superintendent of Insurance the name of this person and any other subsequent changes as provided by ***Article 58D of the Law***. Reports prepared by the AMLCO must be communicated directly to the Board of Directors through senior management.

1.1.8. ***Article 58B of the Law*** requires, when appropriate, due to the size and nature of the activities of the obliged entity the establishment of an independent internal audit function which will be responsible to verify the established internal policies, controls and procedures as referred in Article 58.

Provided, that the competent Supervisory Authority maintains the right to impose the obligation for the establishment of an independent audit service upon the obliged entity.

For Insurance Undertakings the establishment of an internal audit function is compulsory.

1.1.9. The Anti-Money Laundering Compliance Officer (hereinafter to be referred as "AMLCO") is appointed by the Board of Directors of the obliged entity. The AMLCO of a branch of an obliged entity from a Member State or a third country that is operating in Cyprus, is appointed by the Board of Directors of the obliged entity and reports directly to the Manager of the Branch and the Head AMLCO of the Group.

1.1.10. According to ***Article 59(6)(a)(iv) and (v) of the Law*** the Superintendent of Insurance may, among others, forbid temporarily, to persons that exercise managerial duties in an obliged entity, or any other natural person is considered responsible for any breach of the Law or Orders, the exercise of managerial duties. Also, it may impose an administrative fine, as defined in ***Article 59(6)(a)(ii) of the Law***, to persons that exercise managerial duties in an obliged entity, or to any other person, in case where it is determined that the breach was a result of their fault, deliberate omission or negligence. The Superintendent of Insurance may, upon its judgment, publish the name of the natural person who committed the breach and the type of the breach.

1.1.11. The Superintendent of Insurance requires from obliged entities to establish the following measures and procedures:

(i) The Board of Directors approves the general principles of the obliged entity's policy for anti-money laundering and combat terrorist financing, which it communicates to Senior Management, the AMLCO and staff. This will provide a clear message from the institution's management as regards the underlying values of corporate compliance culture and the risk appetite, which will determine the expectations, parameters and limits of operation of the organization and especially the commitment against money laundering and terrorist financing.

(ii) In case an obliged entity maintains branches or subsidiaries outside Cyprus, it should implement policies and procedures at Group level (refer to Section 9 of these Orders)

(iii) The Board of Directors and Senior Management should have a good understanding and knowledge of the level of risk for money laundering and terrorist financing that the obliged entity is exposed to so as to decide whether all necessary measures have been taken for its management and mitigation, according to the risk appetite of the obliged entity. Therefore, the AMLCO is responsible to prepare and submit for approval to the Board of Directors through the Senior Management, a report recording and assessing the potential risks for money laundering and terrorist financing considering the areas where the obliged entity is operating, the provision of new products and services, acceptance of new customers, the expansion to new markets/countries, the complex shareholding structure of legal persons, the method of attracting customers, the measures taken for their management and mitigation and also the mechanisms for monitoring the right and effective operation of internal regulations, procedures and controls.

(iv) The AMLCO is responsible for designing the internal policies, procedures and controls and the description and clear definition of responsibilities and limits of responsibility of each department that is dealing with matters related to the prevention of money laundering and terrorist financing. Therefore, an appropriate manual of procedures and risk management is prepared, which, after approval of the Senior Management, it is communicated to the officers, staff and Insurance Intermediaries that are responsible to implement the policy, procedures and controls adopted by the obliged entity and Insurance Intermediaries. The procedures manual covers, among other things, the customer acceptance policy of the obliged entity, the procedures for establishing a business relationship, customer identification and due diligence measures including the documents and information required for the establishment of a business relationship and for the execution of transactions, record keeping and the procedures for on-going monitoring of insurance policies and transactions, the procedures and controls for the detection of unusual and suspicious transactions and their reporting to the AMLCO. Also, it should include the policies and procedures of compliance with the processing of personal data and the exchange of information within the Group.

(v) The manual is periodically assessed and updated for a more effective management of the risks from money laundering and terrorist financing. The updated manual should be approved by Senior Management.

(vi) Policies, procedures and measures are applied so as the risk of money laundering and terrorist financing is identified, assessed and managed during the day-to-day operations of the obliged entity in relation to:

(a) the development of new products, services, new business practices, including new delivery channels;

(b) the use of new or developing technologies for both new and existing products; and

(c) possible changes in the business profile of the obliged entity (e.g. penetration to new markets by opening branches/subsidiaries in new countries/areas). This risk assessment should take place prior to the launch of the new products, business practices or the use of new or developing technologies.

(vii) Considering that the monitoring of customers and their transactions is of high importance for the identification of unusual or suspicious transactions it is essential for obliged entities to ensure an adequate level of data quality maintained in the customers' files and the information systems.

(viii) The Board of Directors and the Senior Management receive regular, adequate and objective information from the AMLCO and the Internal Auditor regarding the implementation and the efficiency of the measures and controls against money laundering and terrorist financing.

(ix) The Internal Audit inspects and evaluates, at least on an annual basis, the effectiveness and adequacy of the policy, procedures and controls applied by the Insurance Undertaking for preventing money laundering and terrorist financing and periodically and according to the risk through regular or specialized audits, verifies the level of compliance of the institution with the Law and the Superintendent of Insurance's Orders. The audit program should be appropriate to the size, nature of operations and risk profile of the Insurance Undertaking. The findings and observations of the Internal Audit are submitted to the Board of Directors and are notified to the Senior Management and the AMLCO of the Insurance Undertaking who take the necessary measures to ensure the correction of any weaknesses and omissions which have been

identified. The Internal Auditor monitors, on an ongoing basis, through progress reports or other means the implementation of his/her recommendations.

(x) The obliged entity applies explicit procedures and standards of recruitment and evaluation of the employees' integrity (existing and new recruits).

1.2. Customer Acceptance Policy

1.2.1. Obliged entities should develop and establish a clear policy as well as procedures for accepting new customers, fully in line with the provisions of the Law and the requirements of these Orders. The relevant policy should be prepared after detailed assessment of the risks encountered by each obliged entity from its customers and/or their transactions and/or their countries of origin or operations (See Section 3 of these Orders). The AMLCO prepares the customer acceptance policy and submits it through the obliged entity's Senior Management to the Board of Directors for consideration and approval. Once approved, the said policy is communicated to the competent staff of the obliged entity.

1.2.2. The said policy should set in an explicit manner the criteria for accepting new customers, the types of customers that will not be acceptable for a business relationship and should prescribe the categories of customers regarded as high risk. The said policy should also determine the conditions and relevant procedures under which a customer relationship should be terminated. The description of the types of customers that are not acceptable for a business relationship and the categories of high-risk customers should take into account factors such as the content and nature of their business activities, their country of origin and/or residence, the anticipated level and nature of business transactions of the customer as well as the expected source and origin of funds. The customer acceptance policy and related procedures should provide for enhanced due diligence for high risk customers as they are prescribed in the Law, these Orders and also those customers that the obliged entity itself has classified as high risk on the basis of its developed policy.

2. THE ROLE OF THE ANTI-MONEY LAUNDERING COMPLIANCE OFFICER ("AMLCO")

2.1. AMLCO Appointment

2.1.1. ***Article 69 of the Law*** requires from obliged entities to apply the following internal reporting procedures and reporting to MOKAS:

(i) Appoint a senior staff member who has the skills, knowledge and expertise as the AMLCO to whom a report will be submitted for any information or other matter which comes to the attention of a member of the staff and which, in the opinion of that person, proves or creates suspicions that another person is engaged in money laundering or terrorist financing,

(ii) require that any such report be considered in the light of all other relevant information by the AMLCO to determine whether the information or other matter set out in the report indeed proves this fact or creates such suspicion,

(iii) allow the AMLCO to have direct and prompt access to other information, data and documents which may be of assistance to him/her and which are available at the obliged entity, and

(iv) ensure that MOKAS is immediately informed, on their own initiative, by submitting a relevant report and providing additional information at the request of MOKAS, when they know or have reasonable suspicion that funds, irrespective of the amount, constitute revenue from money laundering and terrorist financing.

Further, the law explicitly states that the obligation to report to MOKAS includes the attempt to conduct such suspicious transactions.

2.1.2. The AMLCO is appointed by the Board of Directors of the obliged entity. The person appointed as the AMLCO should belong to the Management of the obliged entity so as to command the necessary authority. The obliged entity should inform immediately the Superintendent of Insurance for the appointment of the AMLCO, submitting his/her position/hierarchy and reporting lines of the AMLCO within the organizational structure of the obliged entity, his/her curriculum vitae and communication details.

2.1.3. The AMLCO should be established in Cyprus and act independently and autonomously in order to fulfil his/her obligations. If for any reason the obliged entity wants to have the AMLCO established abroad, then the Undertaking should request and receive the approval of the Superintendent of Insurance in writing, explaining the reasons for requesting the exception and also describing how the AMLCO duties will be fulfilled, in order to proceed with such an arrangement.

2.1.4. In case of termination/resignation of the AMLCO the obliged entity should immediately inform the Superintendent of Insurance.

2.1.5. The staff of the obliged entity should be made aware of the person appointed as AMLCO to whom they should report any information concerning transactions and activities for which they have knowledge or suspicion that might be related to money laundering and terrorist financing activities.

2.1.6. Additionally, the obliged entity should appoint an Alternate AMLCO who substitutes the AMLCO in case of his/her absence. Where it is deemed necessary, due to the volume and/or the geographic spread of the obliged entity operations, obliged entities may appoint "Assistant AMLCOs" by division, district or otherwise for the purpose of assisting the AMLCO. The staff of the obliged entity is informed of the person that has been appointed as Alternate AMLCO. The obliged entities should immediately communicate the appointment of the Alternate AMLCO to the Superintendent of Insurance, providing his/her name, position and contact details.

2.1.7. The Senior Management of the obliged entity ensures that the AMLCO has sufficient resources, including competent staff and technological infrastructures, for the effective discharge of his/her duties.

2.1.8. The AMLCO, the Alternate AMLCO and other members of staff who have been assigned with the duty of implementing the procedures for the prevention of money laundering and terrorist financing, have complete and timely access to all information concerning customers' identity, transactions' records and other relevant files and information maintained by the obliged entity so as to be fully facilitated in the effective discharge of their duties.

2.1.9. Obliged entities that keep branches or subsidiaries in another member state or a third country appoint the AMLCO as a coordinator, for ensuring the implementation by all branches and companies of the group, which are engaged in financial activities, of the group policy and the adequate and appropriate systems and procedures for the effective prevention of money laundering and terrorist financing. Hence, the AMLCO should monitor on a continuous basis the compliance with the obligations through on-site or off-site audits.

2.2. AMLCO Duties

2.2.1. The AMLCO should maintain a procedures manual for all his/her tasks/responsibilities. The role and responsibilities of the AMLCO, the Alternate AMLCO and also the Assistants AMLCOs (if applicable) should be clearly defined and recorded in the said manual.

As a minimum, the duties of the AMLCO should include the following:

(i) The AMLCO has the primary responsibility, together with the obliged entity's Senior Management, for establishing appropriate procedures and systems for the prompt implementation of the Law and the Orders of the Superintendent of Insurance as well as for adherence to all other circulars/recommendations which are issued by the Superintendent of Insurance, from time to time, for the prevention of the use of the obliged entity for money laundering and terrorist financing. In this regard, the AMLCO has the primary responsibility for the preparation of the obliged entity's risk management and procedures manual for the prevention of money laundering and terrorist financing which is submitted to Senior Management for approval. The manual should be assessed and updated periodically to adapt the procedures for the effective management of the risks emanating from money laundering and terrorist financing. The updated manual should be approved by Senior Management.

(ii) The AMLCO prepares the Customer Acceptance Policy which is submitted, through Senior Management, to the Board of Directors for approval. The AMLCO updates the Customer Acceptance Policy according to changes to the Laws and Regulations and due to other factors (internal and external) as required. The updated policy should be approved by the Board of Directors.

(iii) The AMLCO monitors and assesses whether the policy, procedures and controls that have been introduced for the prevention of money laundering and terrorist financing are correctly and effectively applied. In this regard, the AMLCO should apply appropriate monitoring mechanisms (e.g. on-site visits to units/branches) which will provide him/her with all necessary information for assessing the level of compliance of the units /branches of the obliged entity with the procedures and controls which are in force. If the AMLCO identifies shortcomings and/or weaknesses in the application of the policies, procedures and controls, he/she should give appropriate guidance for the implementation of corrective action.

(iv) The AMLCO ensures that all branches and subsidiaries of the obliged entity in Cyprus or abroad have taken all necessary measures for achieving full compliance with the provisions of these Orders.

(v) The AMLCO is responsible for the evaluation, on an annual basis, of all risks arising from existing and new customers, new products and services and the implementation of measures and controls for the effective management and mitigation of the aforesaid risks. The relevant report should be submitted, through Senior Management, to the Board of Directors for approval. A copy of the approved report should be retained by the obliged entity.

(vi) The AMLCO ensures that he/she, the Alternate AMLCO and the Assistant AMLCOs (if applicable) acquire the requisite knowledge and skills for the implementation of appropriate internal procedures for preventing, recognising and reporting transactions/activities suspected to be associated with money laundering or terrorist financing.

(vii) The AMLCO provides advice and guidance to the management and staff of the obliged entity on the correct implementation of policies, procedures and controls against money laundering and terrorist financing.

(viii) The AMLCO determines the Insurance obliged entity's units/branches staff that need further training and education for the purpose of preventing money laundering and terrorist financing and organises appropriate training seminars/workshops. In this regard, the AMLCO prepares and applies, in co-operation with other departments of the obliged entity, an annual staff training program.

(ix) The AMLCO ensures that the obliged entity maintains full records of the seminars and other training offered to the obliged entity's staff, as described under section "Education and Training" in these Orders and assesses the adequacy of the education/training provided.

(x) The AMLCO verifies that the third party to whom the obliged entity intends to assign the customer identification and due diligence measures is an obliged entity as set out in the Law and gives his/her written consent for the cooperation. The AMLCO evaluates the quality of the customers recommended by third parties.

(xi) The AMLCO audits the correct and effective implementation of the policy, procedures and controls that have been introduced by the obliged entityfor the prevention of money laundering and terrorist financing, and at Group level, where applicable. In this regard, the AMLCO should apply appropriate monitoring mechanisms (including off-site and on-site visits to units/branches/departments) which will provide him/her with the necessary information for the level of compliance of the obliged entity with what is currently in force. In case the AMLCO identifies deficiencies and/or weaknesses he/she should give appropriate instructions and guidance for corrective actions which the AMLCO monitors. The AMLCO should occasionally, and depending on the risk, inform the Board of Directors and the Senior Management of the findings of these audits and the level of compliance of the obliged entity. The AMLCO of branches should inform the manager of the branch and the Group AMLCO.

(xii) The AMLCO shall take or suggest, where appropriate, corrective measures, in matters of prevention of money laundering and terrorist financing in accordance with the findings of the audit conclusions of the Superintendent of Insurance.

(xiii) The AMLCO considers the findings of the Internal Audit and takes corrective action for issues regarding the prevention of money laundering and terrorist financing.

(xiv) The AMLCO takes or recommends, where appropriate, measures to prevent money laundering and terrorist financing taking into account the National and Supranational Risk Assessment reports.

(xv) The AMLCO ensures that the obliged entity can produce reports of customers in printed form according to the customer risk category.

(xvi) The AMLCO maintains a register for a period of five years of all cases of persons (prospective customers) with whom the establishment of a business relationship was not allowed.

(xvii) The AMLCO responds to requests from MOKAS and provides all the information requested and fully co-operates with MOKAS.

(xviii) The AMLCO responds to all requests and queries from the Superintendent of Insurance and provides all relevant requested information and fully co-operates with the Superintendent of Insurance.

(xix) The AMLCO ensures that the obliged entity considers the public announcements of the Financial Action Task Force ("FATF") in respect of countries which do not implement or apply inadequately the FATF recommendations and ensures that enhanced due diligence measures and monitoring of business relations/transactions are applied. Additionally, he/she ensures that enhanced due diligence measures are applied to high-risk third countries identified by the European Commission and by the obliged entity itself.

2.3. AMLCO Annual Report

2.3.1. The AMLCO prepares the Annual Report which is a significant tool for assessing the obliged entity's level of compliance with its obligations laid down in the Law and the Superintendent of Insurance Orders for the prevention of money laundering and terrorist financing.

2.3.2. The Annual Report should be prepared within two months of the end of each calendar year (the latest by end of February) and submitted to the Board of Directors of the obliged entity through the Senior Management. In the case of an obliged entity operating in Cyprus in the form of a branch, the Annual Report should be submitted to the Board of Directors through the Senior Management and the Group AMLCO at the headquarters of their country of origin.

2.3.3. The Board of Directors reviews and assesses the Annual Report. The Senior Management of the obliged entity will take all appropriate action, as deemed necessary under the circumstances, to remedy any weaknesses and/or deficiencies identified in the Annual

Report. Copies of the minutes of approval of the Board of Directors must be submitted to the Superintendent of Insurance immediately after approval.

2.3.4. A copy of the Annual Report which is submitted to the Board of Directors must also be submitted, simultaneously, to Superintendent of Insurance.

2.3.5. The AMLCO's Annual Report should deal with money laundering and terrorist financing preventive issues pertaining to the year under review and, as a minimum, should contain the following:

(i) Information about any changes in the business operation of the obliged entityduring the last year, with reference to products and services offered, countries of operation, and any technological developments affecting the procedures and controls for anti-money laundering and combat terrorist financing.

(ii) Information on changes in the Law and the Superintendent of Insurance Orders which took place during the year and measures taken and/or procedures introduced for securing compliance with the above changes.

(iii) Information on the number of inspections and reviews performed by the AMLCO and the Insurance Undertaking's Internal Audit Unit and the material deficiencies and weaknesses identified in the anti-money laundering and terrorist financing policies, procedures and controls. In this regard, the report should outline the seriousness of the deficiencies, the risk implications and the recommendations made as well as the action taken for rectifying the situation.

(iv) Information on the audits carried out by the Superintendent of Insurance, highlighting deficiencies and weaknesses identified, the risks involved as well as the corrective measures and actions taken or undertaken to improve the situation.

(v) The number of internal money laundering suspicious reports submitted by the obliged entity's employees to the AMLCO with possible comments/observations about the content of the suspicions and of any particular trends.

(vi) The number of internal suspicious reports which have been evaluated by the AMLCO and were not submitted to MOKAS.

(vii) The number of suspicious reports submitted by the AMLCO to MOKAS with information of the main reasons for suspicion and highlights of any particular trends.

(viii) Summary data as follows:

(a) No of customers by country of origin, No of PEPs, No of non-face-to-face customers

(b) No of new customers

(c) No of customers per risk category

(d) No of prospective customers with whom the establishment of business relationship was not allowed for compliance reasons

(e) No of customers with whom the business relationship was terminated for compliance reasons

(f) Level of Cash Transactions – No of cash transactions, Total Amount of cash received, Total No of cash transactions above € 10,000

(g) No of policies with surrender value between € 100.000 and € 250.000, and above € 250.000, in-force and surrendered during the year

(h) No of policies with related beneficiaries, No of policies with at least one non-related beneficiary

(i) No of insurance intermediaries broken down as tied and non-tied

(ix) Information on the policy, procedures and controls applied by the obliged entity in relation to high risk customers.

(x) Information on the training seminars attended by the AMLCO, the Alternate AMLCO and the Assistant AMLCOs and on any other educational material received.

(xi) Information on training/education provided to the Board of Directors, Senior Management, Insurance Intermediaries and staff during the year, reporting:

- No of seminars performed
- Their duration
- Persons attended (specifying their role)
- Name(s) and qualifications of the instructor(s)
- Information whether the seminar was developed internally by the obliged entity or by an external organization

- Summary information of the timetable and content of the seminar.

(xii) Results of the assessment of the adequacy and effectiveness of staff training.

(xiii) List of third parties with whom the obliged entity has established cooperation for the purpose of customer identification and due diligence measures and a list of third parties that the AMLCO has rejected.

(xiv) Information on the structure and staffing of the AMLCO's Unit as well as recommendations for any additional staff and technical resources which may be needed for reinforcing the measures and procedures against money laundering and terrorist financing.

(xv) An overall assessment of the effectiveness of the systems and controls, adequacy of resources and also deficiencies and weaknesses identified together with the action plan of how the obliged entity is intending to apply corrective action including the expected deadline for completion of the corrective actions.

(xvi) Information about the branches/subsidiaries of the obliged entity that operate in other countries and also the information on the measures taken for their compliance with the provisions of these Orders and the framework of the obliged entity.

3. RISK BASED APPROACH

3.1. Introduction

3.1.1. For the purposes of article 58(d), ***Article 58A(1) and (2) of the Law*** requires obliged entities to take appropriate measures to identify, and assess the risks of money laundering and terrorist financing which they face, taking into account risk factors, including factors which relate to their customers, countries and geographical areas, products, services, transactions or delivery channels for the provision of services . These measures should be proportionate to the size and nature of their operations. The risk assessment is documented, updated and made available to the Superintendent of Insurance through the Risk Assessment Report referred to in section 3.6.

3.1.2. The Risk Based Approach ("RBA") is central to an appropriate implementation of an effective AML and CTF framework. It means that obliged entities identify, assess and understand the money laundering and terrorist financing (ML/TF) risks to which they are exposed, and implement the most appropriate mitigation measures. This approach enables them to focus their resources where the risks are higher.

3.1.3. The RBA should be commensurate with the nature, size and complexity of the business. This means that a simple risk assessment might be enough for smaller or less complex obliged entities, and that where obliged entities are part of a Group, risk assessments should take into account group-wide risk appetite and framework.

3.1.4. There are several discrete steps in assessing the most cost effective and proportionate way to manage and mitigate the money laundering and terrorist financing risks faced by the company. These steps are:

- *Identification*: Identify the money laundering and terrorist financing risks that are relevant to the company considering the size and nature of its operations/activities.
- *Assessment*: Assess the risks presented by the company's particular customers and any underlying beneficial owners, products or services, transactions, delivery channels, geographical areas of operation.
- *Management*: Design and implement controls to manage and mitigate these assessed risks, in the context of the company's risk appetite.
- *Monitoring*: Continuously monitor and improve the effective operation of these controls.
- *Reporting*: Record appropriately what has been done, and why.

3.1.5. The European Commission on 26 June 2017 published its first ***Supranational Risk Assessment*** ("SRA") with the aim of assisting member states to identify, analyze and address the risks related to money laundering activities and terrorist financing. Obliged entities should consider the findings of this Report, including its updates, to the extent that they may affect their individual risk assessment.

3.1.6. The ***National Risk Assessment*** ("NRA") of Cyprus published in November 2018 provides information of the Cyprus risks of money laundering and terrorist financing inherent in its business. Obliged entities should be aware of the findings of this Report, including its updates, to the extent that they may affect their individual risk assessment.

3.1.7. To assist the overall objective to prevent money laundering and terrorist financing, a RBA:

- recognizes that the money laundering/terrorist financing threat to companies varies across customers, jurisdictions, products and delivery channels;
- allows management to differentiate between their customers in a way that matches the risk in their particular business;
- allows the Board of Directors and Senior Management to apply its own approach to the company's procedures, systems and controls, and arrangements in particular circumstances; and
- helps to produce a more cost-effective system.

3.1.8. ***Article 61(2) of the Law*** requires obliged entities to apply identification procedures and customer due diligence measures but allows the extent of such measures to be determined according to the degree of risk considering at least the variables listed in Appendix I of the Law. Obliged entities should be able to demonstrate to the competent Supervisory Authorities that the extent of the measures is commensurate with the risks of money laundering and terrorist financing that they face.

3.1.9. The RBA should set out factors obliged entities should consider when assessing the money laundering and terrorist financing (ML/TF) risk associated with a business relationship. They also set out how firms should adjust the extent of their customer due diligence ("CDD") measures in a way that is commensurate to the ML/TF risk they have identified.

The firm's decisions on the CDD measures to be applied must take account of the Risk Factor Guidelines issued jointly by the European Supervisory Authorities[2].

3.1.10. No system of controls will detect and prevent all money laundering and terrorist financing. The RBA will, however, serve to balance the cost imposed on individual companies and their customers with a realistic assessment of the threat of the firm being used in connection with money laundering or terrorist financing. It allows the company to focus the effort where it is needed and will have the biggest impact.

3.1.11. The AMLCO is responsible for the identification, recording and assessment of all possible risks. However, the successful implementation of systems and controls on a RBA requires the full commitment of Senior Management and the active cooperation of the other units of the obliged entity. It is also necessary to clearly communicate the agreed policies and procedures to all the relevant staff of the obliged entity together with the introduction of robust mechanisms for their effective implementation, the early identification of weaknesses and the implementation of corrective action.

3.1.12. The obligation to report suspicious transactions is not risk based but applies regardless of the risk involved. The information obtained during the customer identification and due diligence measures must be sufficient to provide adequate insight about the nature of the business relationship allowing the identification of any unusual or suspicious transactions.

3.2. Identification

3.2.1. A risk-based approach starts with the identification and recording of the risks. During the identification of the risks obliged entities should examine the relevant risk factors, including the identity and occupation of their customer, the countries or the geographical areas in which the customer operates, the specific products and specific services and transactions requested by the customer, as well as the channels used by the obliged entity for the provision of such products, services and transactions. In the cases where the

[2] Joint Guidelines under Articles 17 and 18(4) of Directive (EU) 2015/849 on simplified and enhanced customer due diligence and the factors credit and financial institutions should consider when assessing the money laundering and terrorist financing risk associated with individual business relationships and occasional transactions ("The Risk Factors Guidelines").
https://eba.europa.eu/documents/10180/1890686/Final+Guidelines+on+Risk+Factors+%28JC+2017+37%29.pdf

business, products and customer base of an obliged entity are relatively simple, involving relatively few products and customers, or customers with similar characteristics, a simple, standard approach is more appropriate for most customers, with emphasis on those customers who fall outside the 'norm'.

3.2.2. Obliged entities shall consider the risk factors referred to in the "Risk Factors Guidelines" published jointly by the European supervisory authorities in accordance with articles 17 and 18(4) of the European Union Directive. It should be noted that the risk factors included in these guidelines are not exhaustive and obliged entities are not expected to consider all risk factors for all cases.

3.2.3. The information about these risk factors for money laundering and terrorist financing should originate from a wide range of sources in which access is obtained either individually or through commercially available tools or databases that gather information from various sources. Obliged entities should define the type and number of sources according to the degree of risk.

3.2.4. Obliged entities should always consider the following sources of information:

(i) The Supranational Risk Assessment of the European Commission;

(ii) Information from the Government, such as the National Risk Assessment of Cyprus, the policy statements and warning indications;

(iii) The information from the Superintendent of Insurance, such as circulars, guidelines and the justification derived from the imposition of regulatory fines;

(iv) Information from MOKAS, the Police such as threat reports, warnings and typologies;

(v) Information received from customers at the beginning of the business relationship.

3.2.5. Other sources of information obliged entities may consider in this context are:

(i) Information from international standard-setting bodies, such as mutual evaluation reports or legally non-binding "blacklists";

(ii) Typologies and information on emerging risks of the industry;

(iii) Information from civil society, such as corruption indices and country reports;

(iv) Information from credible and reliable open sources such as reports in reputable newspapers;

(v) Information from credible and reliable commercial organizations such as risk and intelligence reports; and

(vi) Information from statistical organizations and academia.

3.3. Assessment

3.3.1. Obliged entities need to assess and evaluate the risks they are facing through the potential use of their services by criminals for the purpose of money laundering or terrorist financing. During this assessment, obliged entities should consider the various factors affecting the risk considering their relative importance.

3.3.2. When considering the various risk factors and allocating weights on each factor the obliged entities should make an informed judgment about the relevance of each risk factor in the context of the business relationship. This often results in obliged entities allocating different weights/scores to different factors.

3.3.3. The weight given to each of these factors is likely to vary from product to product and customer to customer (or categories of customers) and between obliged entities. When weighting risk factors and scoring customer risk, obliged entities should ensure that:

- weighting and scoring are not unduly influenced by just one factor
- the risk rating should not consider any business aspects/factors e.g. profit considerations
- weighting and scoring do not lead to a situation where no business relationship is classified as high risk;
- the provisions of the Law and the Orders regarding situations that always present a high money laundering risk cannot be over-ruled by the firm's weighting and scoring; and

- any automatically generated risk scores could be overridden. The rationale for the decision to over-ride such scores should be documented appropriately, especially of the change is from a higher to a lower risk.

3.3.4. The RBA should allow the obliged entity to assess individual customers and categorize them to a specific level of risk, which in turn will drive the level and extent of identification and due diligence measures appropriate to that customer. It is noted that, unless specified in the Law or the Orders of the Superintendent of Insurance, the existence of individual risk factors does not necessarily imply the categorization of a customer relationship at high or low risk. Although obliged entities often categorize the risk as high, medium and low, it is possible to classify it in other categories.

3.3.5. As part of the assessment process obliged entities should consider the inherent likelihood of a risk materializing as well as the impact it will have on the company.

3.4. Management

3.4.1. Once the risks are identified and assessed the obliged entity should design and implement the appropriate procedures, systems, measures and controls to manage and mitigate them in accordance with the procedures provided for in these Orders.

3.4.2. The intensity and depth of risk mitigation measures including customer due diligence (CDD) checks depend on the money laundering and terrorist financing risks. In particular, it should be emphasized that the identity and status of parties to life insurance contracts, including the beneficiary and where relevant the beneficial owner(s), will determine the extent of the controls to be performed, in particular if a Politically Exposed Person (PEP) is involved. The importance of the entities' internal controls should also be highlighted, whose structure and organization depend on the money laundering and terrorist financing risks identified and for which, in any case, the "tone from the top" i.e. the involvement of Senior Management, plays a central role.

3.4.3. The particular circumstances of each obliged entity will determine the suitable procedures, systems, measures and controls that need to be applied to counter and manage risk. In the cases where the business, products and customer base of an obliged entity are relatively simple, involving relatively few products and customers, or customers with similar

characteristics, a simple, standard approach is more appropriate for most customers, with emphasis on those customers who fall outside the 'norm'.

3.4.4. The identification, assessment and management of the risks is more effective if the quality of the data held by the obliged entities and Insurance Intermediaries is of high standard. Insufficient data quality and missing information will lead to incorrect alert messages, management supervision reports and inappropriate management.

3.4.5. As part of the management process and the mitigation measures and controls implemented, the obliged entities should assess the residual likelihood of a risk materializing as well as the impact it will have on the company.

3.5. Monitoring

3.5.1. Obliged entities should assess, on a regular basis, the correct implementation but also the effective functioning of the RBA and the internal policies, procedures and controls at the level of business, AMLCO and Internal Audit. In this context, obliged entities should:

(a) Revise the systems and controls regularly so as to achieve the continuous and effective management of risks arising from changes in the characteristics of existing customers, new customers, products and services and geographical dispersion.

(b) Ensure that they have methodologies and controls to identify emerging risks of money laundering and terrorist financing and that they are able to assess the risks and, where appropriate, incorporate them in a timely manner both in the institution overall risk assessment and in the individual risk assessments they carry out.

(c) Implement procedures for the examination and control of new products, services of new business practices, including new channels for the provision of services and the use of new or developing technologies for new or existing products and any methods used by criminals for money laundering or terrorist financing.

(d) Appropriate procedures for the timely identification of changes in the economic and risk profile of their customers.

3.6. Reporting

3.6.1. Obliged entities should document and report their Risk Based Approach in a "Risk Assessment Report" including the risks identified, the assessment and management of these risks, as well as the monitoring of the process, the measures and controls. The obliged entity should be able to demonstrate to the Superintendent of Insurance the adequacy of these risk assessments and related risk management measures. Therefore, the detailed recording of the measures taken by the obliged entity will help it to demonstrate:

(a) the ways they have used to identify and assess the risks of possible use of their products and services for money laundering and terrorist financing;

(b) how they concluded to the introduction and implementation of the specific policies, procedures and controls for the management and mitigation of risks;

(c) the methods of monitoring and improvement where this is deemed necessary, of the specific policies, procedures and controls, and

(d) the setup for reporting to senior managers on the operation of the control procedures.

3.6.2. This report should be submitted on an annual basis to the Board of Directors of the obliged entity, through Senior Management, in order to recognize the residual risks that reflect to the risk appetite of the obliged entity and also for their approval. A copy of the approved Risk Assessment Report, together with the minutes of the Board of Directors where the views are recorded, and the approval of the Board of Directors should be retained by the obliged entity.

3.6.3. ***Article 58A(2) of the Law*** requires that the Risk Assessment Report must be kept fully updated. It is therefore necessary to re-evaluate the risks, on an annual basis even where obliged entities consider that there is no need for revising the relevant report.

3.6.4. Obliged entities are obliged, under the responsibility of the AMLCO, to be able to create customer reports, at any time, indicating the customer risk category and including the names of the customers and the ultimate beneficial owners, insurance policy number, the branch in which the insurance policy is held, Insurance Intermediary, date of commencement of the business relationship, date of last update.

4. CUSTOMER IDENTIFICATION AND DUE DILIGENCE PROCEDURES

4.1. Introduction

4.1.1. According to ***Article 61(2) of the Law*** obliged entities must determine the extent of their CDD measures and ongoing monitoring on a risk-sensitive basis, depending on the type of customer, business relationship, product or transaction. However, the persons engaged in financial and other business must be able to demonstrate to the competent supervisory authorities that the extent of the measures is appropriate in view of the risks of money laundering and terrorist financing.

4.1.2. Obliged entities should collect and maintain adequate information about a customer allowing them to identify the customer and define their financial and risk profiles. This information will allow the obliged entity to detect unusual transactions and activity, not relating to the profile of the customer, and hence identify suspicious activity.

4.2. When to apply customer identification and due diligence procedures

4.2.1. ***Article 60 of the Law*** requires persons carrying financial or other business to apply customer identification and due diligence procedures in the following cases:

(a) when establishing a business relationship;

(b) when carrying out occasional transactions amounting to EUR 15 000 or more, whether the transaction is carried out in a single operation or in several operations which appear to be linked;

(c) when there is a suspicion of money laundering or terrorist financing, regardless of the amount of transaction;

(d) when there are doubts about the veracity or adequacy of previously obtained customer identification documents, data or information previously collected for the customer identification.

4.3. Identification and due diligence procedures

4.3.1. ***Article 61(1) of the Law*** provides that the customer identification procedures and due diligence measures, include the following:

(i) Identifying the customer and verifying the customer's identity on the basis of documents, data or information obtained from a reliable and independent source;

(ii) Identifying the beneficial owner's identity and taking reasonable measures to verify that person's identity based on documents, data or information issued or obtained from an independent, reliable source so that the person carrying on financial or other business is satisfied that he/she knows who the beneficial owner is, including, as regards legal persons, trusts and similar legal arrangements, taking risk-based and adequate measures to understand the ownership and control structure of the customer;

(iii) Assessing and, depending on the case, obtaining information on the purpose and intended nature of the business relationship;

(iv) Conducting ongoing monitoring of the business relationship including scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the information and data in the possession of the obliged entity in relation to the customer, the business and risk profile of the customer, including, where necessary, the source of funds and ensuring that the documents, data or information held are kept up-to-date.

It is understood that in applying the measures in paragraphs (i), and (ii) above, obliged entities shall also verify that any third person purporting to act on behalf of the customer is duly authorized by the customer for this purpose and identifies and verifies the identity of the third person.

4.3.2. According to ***Article 2 of the Law***, "beneficial owner" means the natural person who ultimately owns or controls the customer and/or the natural person on whose behalf a transaction or activity is being conducted and includes at least

(a) in the case of corporate entities

(i) the natural person who ultimately owns or controls a corporate entity through direct or indirect ownership of a sufficient percentage of the shares or voting rights or ownership interest in that corporate 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

European Union law or subject to equivalent international standards which ensure adequate transparency of ownership information.

Provided that-

(a) an indication of direct shareholding shall be a shareholding of 25% plus one share or an ownership interest of more than 25% in the customer held by a natural person; and

(b) an indication of indirect ownership shall be a shareholding of 25% plus one share or an ownership interest of more than 25% in the customer held by a corporate entity, which is under the control of a natural person, or by multiple corporate entities, which are under the control of the same natural person or persons.

It is further provided that control by other means can be verified, inter alia, based on the criteria provided for in section 142(1)(b) and section 148 of the Companies Law. Provided further that the control by other means can be verified, inter alia, based on the criteria provided for in section 142 (1) (b) and section 148 of the Companies Law.

(ii) the natural person who holds the position of a senior manager if, after having exhausted all possible means and provided there are no grounds for suspicion, no person under subparagraph (i) of the present paragraph is identified, or if there is any doubt that the person identified is the beneficial owner.

It is provided that the obliged entity shall keep record of the actions taken in order to identify the beneficial ownership under sub paragraphs (i) and (ii);

(b) in the case of trusts:

(i) the settlor;

(ii) the trustee or commissioner;

(iii) the protector, if any;

(iv) the beneficiary, or where the individual benefiting from the legal arrangement or legal entity have yet to be determined, the class of persons in whose main interest the legal arrangement or entity is set up or operates;

(v) any other natural person exercising ultimate control over the trust by means of direct or indirect ownership or by other means; and

(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 in paragraph (b);

4.3.3. ***Article 61(3) of the Law*** provides that for the purposes of the provisions relating to identification procedures and customer due diligence requirements, proof of identity is satisfactory if -

(a) It is reasonably possible to establish that the customer is the person he/she claims to be, and

(b) the person who examines the evidence is satisfied, in accordance with the procedures followed under the Law, that the customer is actually the person who he/she claims to be.

4.3.4. ***Article 61(4) of the Law*** requires for life insurance or other investment-related insurance business, in addition to the customer due diligence measures required for the customer and the beneficial owner, financial institutions shall take the following customer due diligence measures on the beneficiaries of life insurance and other investment-related insurance policies, as soon as the beneficiaries are identified or designated:

(a) In the case of beneficiaries identified as specifically named persons or legal arrangements, taking the name of the person;

4.3.5. In the case of beneficiaries that are designated by characteristics or by class or by other means, obtaining sufficient information concerning those beneficiaries to satisfy the financial institution that it will be able to establish the identity of the beneficiary, the latest at the time of the payout. It is noted that obliged entities should establish to their satisfaction that they are dealing with a real person (natural or legal) and obtain sufficient evidence of identity to establish that a prospective policy holder is who he/she claims to be. The verification procedures necessary to establish the identity of the prospective policyholder should be based on reliable data, documents and information issued or obtained from independent reliable sources, i.e. those data, documents and information that are the most difficult to amend or obtain illicitly. Certified true copies of the identification evidence should always be retained by the obliged entities and kept in customers' files. However, it must be appreciated that no single form of identification can be fully guaranteed as genuine or representing correct identity and, consequently, the identification process will generally need to be cumulative.

4.4. Timing of customer identification and due diligence procedures

4.4.1. ***Article 62(1) of the Law*** requires that the verification of the identity of the customer and the beneficial owner is performed before the establishment of a business relationship or the carrying out of the transaction.

4.4.2. By derogation of Article 62(1) of the Law, ***Article 62(2) and (3) of the Law*** allows the verification of the identity of the customer and the beneficial owner to be completed during the establishment of a business relationship if this is necessary so as not to interrupt the normal conduct of business and where there is little risk of money laundering or terrorist financing. Provided that in in such a case the customer and beneficial owner identity verification procedures shall be completed as soon as possible after the initial contact.

4.4.3. By derogation of Article 62(1) of the Law, with respect to Article 61(4) of the Law, ***Article 62(5A)*** verification of the identity of beneficial owners is carried out the latest at the time of payout pursuant to the insurance policy: Provided that, in the case of assignment to a third person, in whole or in part, of the life insurance or other investment-related insurance to a third party, credit institutions and financial institutions are aware of the assignment shall identify the beneficial owner at the time of the assignment to the natural or legal person or legal arrangement receiving for its own benefit the value of the insurance policy assigned.

4.4.4. As a rule, obliged entities are expected to seek and obtain satisfactory evidence of identity of their prospective customers prior to the conclusion of a relationship. The identification and verification of the identity of the beneficial owners and the beneficiary under the policy may exceptionally take place after the business relationship with the policyholder is established, but in all such cases, identification and verification should occur at the latest before the time of payout or the time when the beneficiary intends to exercise vested rights under the policy.

4.4.5. ***Article 62(4) of the Law*** clearly requires that in cases where an obliged entity cannot comply with customer due diligence requirements as defined in Article 61(1)(a)(b)(c), it does not establish a business relationship or does not carry out the transaction, as the case may be, terminates that business relationship and examines the possibility of submitting a

suspicious transaction report in relation to the customer to MOKAS, in accordance with the provisions of Article 69 of the Law.

4.5. Update of identification data of existing customers

4.5.1. ***Article 60(d) of the Law*** requires obliged entities to apply the identification procedures and customer due diligence measures when there are doubts about the accuracy or adequacy of the documents, data or information previously collected for the identification of an existing customer. Furthermore, ***Article 62(6) of the Law*** requires the application of identification procedures and customer due diligence measures not only to new customers but also to existing customers at the appropriate times, on a risk-sensitive basis, among others, at times when the relevant circumstances of the customer change.

4.5.2. Obliged entities must ensure that customer identification records remain up-to-date and relevant throughout the business relationship. In this respect, an obliged entity must undertake, on a regular basis, or whenever there are doubts about the veracity of the identification data, reviews of existing records, especially for high-risk customers. The policy and the procedures for the prevention of money laundering and terrorist financing should determine the timeframe during which the regular review, examination and update of the customer's identification data and other data and information should be conducted, depending on the risk categorization of each customer. If, as a result of these reviews, at any time throughout the business relationship, the obliged entity becomes aware that it lacks sufficient information about an existing customer, it should take all necessary action to obtain the missing information and identification data as quickly as possible.

4.5.3. In addition to the requirement for the update of the customer identification data and information on a regular basis or when it is observed that unreliable or inadequate data and information are being held, obliged entities should check the adequacy of the data and information held with regard to the customer's identity and business/economic profile, whenever one of the following events or incidents occurs:

(a) An individual transaction takes place which appears to be unusual and/or significant compared to the normal pattern of transactions and the business/economic profile of the customer.

(b) There is a significant change in the customer's legal status and/or situation,

such as:

(i) Change of director(s)/ secretary;

(ii) Change of registered shareholder(s) and/or beneficial owner(s);

(iii) Change of registered office;

(iv) Change of trustee(s), settlor(s), protector(s), beneficiary(ies);

(v) Change of corporate name and/or trading name used; and

(vi) Change of the principal trading partners and/or taking-up of new major business activities and/or expansion of activities to other countries.

(c) Significant change of the policy or in the relationship, such as:

(i) Change of the beneficiary(ies) of the policy

(ii) application for the purchase of a new insurance product.

(d) Change of the risk level of the customer (e.g. customer from lower to higher risk).

(e) Change in the customer's business activities.

(f) Discovery of negative information about the customer in the press or the internet or commercial information databases or information submitted by a competent supervisory authority or MOKAS or due to an investigation which indicate the need for the update of the customer and/or possible change to the risk profile of the customer.

4.5.4. If a customer fails or neglects to submit, the required data and identification information for the updating of his/her identity and business/economic profile the obliged entity shall take all necessary action and shall employ any means it deems necessary to obtain the missing information and identification data. If the obliged entity after having exhausted all available and/or appropriate means is unable to collect the required information within a reasonable timeframe and/or if the customer persistently refuses to submit the required information and as a result the obliged entity is unable to comply with the customer identification requirements set out in the Law and these Orders, then the obliged entity should terminate the business relationship and close all the insurance policies of the customer concerned while at the same time it should examine whether is warranted under the circumstances to submit a report of suspicious transactions/activities to MOKAS',

4.6. Simplified identification and due diligence measures ("SDD")

4.6.1. ***Article 63(1) of the Law*** states that obliged entities may apply simplified customer due diligence measures, if they have been satisfied, in advance, that the business relationship or transaction presents a low degree of risk. It is provided that the obliged entity monitors the transaction and the business relationship sufficiently to enable the detection of unusual or suspicious transactions.

4.6.2. ***Article 63(2) of the Law*** states that, when assessing the risks of money laundering or terrorist financing which relate to types of customers, geographical areas and particular products, services, transactions or delivery channels, the obliged entity takes into account at least the factors of potentially lower risk situations set out in Appendix II of the Law.

4.6.3. The application of simplified due diligence measures does not imply an exception to any due diligence measure, however obliged entities may adjust the extent, time or type of each or all due diligence measures in a manner to be proportionate to the low risk they have identified. Scenarios of lower risk and where SDD might be applied include:

(a) Products that only pay out at death and/or in the event of disability;

(b) customers that are publicly listed companies on exchanges with adequate disclosure requirements for transparency of beneficial ownership;

(c) transactions involving de minimis amounts, such as life insurance policies where the annual premium is no more than EUR 1 000 or a single premium of no more than EUR 2 500;

(d) insurance policies for pension schemes if there is no surrender clause and the policy cannot be used as collateral;

(e) 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 (e.g., small insurance premiums);

4.6.4. In those situations, SDD may include:

(a) Verifying the identity of the customer and the beneficial owner after the establishment of the business relationship;

(b) reducing the frequency of customer identification updates e.g. an update and review only in case of activation events, such as when the customer seeks the provision of a new product or new service or when the limit of a specific transaction has been reached;

(c) reducing the degree of on-going monitoring and scrutinizing transactions, based on a reasonable monetary threshold;

(d) not collecting specific information or carrying out specific measures to understand the purpose and intended nature of the business relationship, but inferring the purpose and nature from the type of transactions or business relationship established; and

4.6.5. In case of indications that the risk may not be low or if there are suspicions of attempted money laundering or terrorist financing or where the obliged entity has doubts as to the accuracy of the information received, simplified due diligence measures should not be applied. Also, simplified measures should not be applied where it is possible that specific high-risk scenarios may apply and an obligation to implement enhanced due diligence measures is provided.

4.6.6. The application of simplified due diligence measures does not exempt an institution from applying adequate procedures for monitoring transactions and the business relationship so as to identify suspicious or unusual transactions in a timely manner and submit a report to MOKAS.

4.7. Construction of a customer's business profile

4.7.1. ***Article 61(1) of the Law*** requires, inter alia, that customer identification procedures and customer due diligence measures, include the following:

(i) the identification and verification of the customer's identity on the basis of documents, data or information issued or obtained from a reliable and independent source;

(ii) the verification of the identity of the beneficial owner and taking reasonable measures to verify his/her identity so as to ensure that the obliged entity is satisfied that it knows who the beneficial owner is, including as regards legal persons, trusts, companies, foundations and similar legal arrangements, taking reasonable measures to understand the ownership and control structure of the customer; and

(iii) assessing and, depending on the case, , obtaining information on the purpose and the intended nature of the business relationship.

4.7.2. The obliged entity must be satisfied that it's dealing with a real person (natural or legal) and, for this reason, should obtain sufficient evidence of identity to verify that the person is who he claims to be. The verification of the customer's identification is based on reliable data and information issued or obtained from independent and reliable sources. Certified true copies, as per section 6.2, of the identification evidence should be archived in the policy holder's file.

4.7.3. It is noted that as an additional measure of verification of the identity of the customer and the beneficial owner, obliged entities may also use the information stored in the records referred to in ***Article 61A of the Law***. It should be emphasized that the obliged entity cannot rely solely on the information from the central register for the fulfilment of the requirements of the customer identification and due diligence measures.

4.7.4. It is clarified that a person's residential address is considered an integral part of the identity of the person and, thus, there needs to be a separate procedure for the verification of the customer's address. The customer's address can also be verified by an on-site visit of an officer and/or by a 'tied' insurance intermediary of the obliged entity. Details of the visit should be recorded on a form that is kept with the customer's file.

4.7.5. The data and information that are collected before the establishment of the business relationship, with the aim of constructing the customer's business/economic profile should, as a minimum, include the following:

(a) the purpose and the reason for requesting the establishment of a business relationship;
(b) the customer's size of wealth and annual income and the clear description of the main business/professional activities/operations;
(c) the expected origin of funds.

4.8.5. ***Article 67(4) of the Law*** provides that in the case of a group, the competent supervisory authority of the home Member State and the competent supervisory authority of the host Member State (for branches and subsidiaries) may consider that an obliged entity applies the measures referred to in Sections 4.8.1-4.8.4 above, if the following conditions are met:

(a) the obliged entity relies on information provided by a third party that is part of the same group.

(b) the said group applies customer due diligence measures, record-keeping rules and programs against money laundering and terrorist financing in accordance with the requirements of the European Union Directive or equivalent rules.

(c) the effective implementation of the requirements referred to in point (b) is supervised at group level by a competent authority of the home Member State or the third country.

4.8.6. All copies of the identification documents, data and information obtained by an obliged entity from a third party should be duly certified as described in Section 6.2.

4.8.7. Obliged entities may rely on third parties only at the outset of establishing a business relationship for the purpose of ascertaining and verifying the identity of their customers. Any data and information for the purpose of updating the customer's business profile during the relationship, should be obtained directly from the natural person in the name of whom the insurance policy is maintained, or in the case of legal persons, from the natural persons who are the ultimate beneficial owner of the shares capital of the legal persons or who exercise the ultimate control of the legal persons or who have the responsibility of decision making and who manage the operations of the customer. It is provided that the documents certification, for the update, may be performed by the third party.

4.8.8. The policy and the procedures should specify the measures taken by the obliged entity to comply with the requirements of the Law and the present Orders, including, as a minimum, the following:

(i) The AMLCO shall verify that the third party is an obliged entity as defined in paragraphs (a), (b), (c) and (d) of section (1) of Article 2A or another equivalent institution or person located in a Member State or a third country which;

4.8. Reliance on third parties for customer identification and due diligence

4.8.1. ***Article 67(1) of the Law*** permits obliged entities to rely on third parties for the application of the customer identification procedures and customer due diligence measures, as these are prescribed in Article 61(1)(a), (b) and (c) of the Law. It explicitly provides that the ultimate responsibility for performing the above-mentioned measures and procedures remains with the obliged entity which relies on the third party.

4.8.2. The Law considers as third parties the obliged entities specified in Article 2A(1)(a)(b)(c) and (d) of the Law or other similar institutions or persons located in the Member States or in a third country which:

(i) apply customer due diligence measures and record-keeping measures consistent with those laid down in the directive of the European Union and

(ii) are subject to supervision consistent with the relevant requirements of the European Union Directive.

4.8.3. According to ***Article 67(2)(b) of the Law*** obliged entities cannot rely on third parties established in high-risk third countries, unless the Superintendent of Insurance has exempted from this prohibition branches and subsidiaries of majority participation of obliged entities established in the European Union, where such branches and subsidiaries fully comply with the policies and procedures applied at group level in accordance with Article 68A of the Law.

4.8.4. ***Article 67(3) of the Law*** provides that obliged entities should require from the third party to:

(i) make immediately available to them the data, information and documents of identity obtained as a result of the application of the procedures for customer identification and due diligence measures in accordance with the requirements of the Law; and

(ii) immediately forwards to them certified copies of these documents and the relevant data and information on the identity of the customer and the beneficial owner which the third person collected while applying the above-mentioned procedures and measures.

(a) Applies customer due diligence measures and record-keeping measures consistent with those laid down in the European Union Directive; and

(b) is subject to supervision consistent with the relevant requirements of the European Union Directive.

(ii) The obliged entity shall sign an agreement with the third party specifying the obligations of each party, including the financial conditions, the names and signatures of the persons designated by the third party, and who have the right to certify the documents.

(iii) For each third party mentioned above and before the business relationship commences, identification procedures and due diligence measures are applied.

(iv) The AMLCO evaluates the quality of the customers recommended by third parties. The evaluation must include at least the number of customers recommended by the third party, number of customers with whom the relationship was terminated for non-compliance reasons, number of internal suspicion reports and suspicion reports to MOKAS. If the quality is deemed unsatisfactory then the relationship with the third party is terminated.

(v) The AMLCO maintains a separate file in which the identity data is recorded, evidence certifying that the third party is subject to supervision under the Law and an assessment of the quality of the customers recommended by the third party. This information should be updated on an annual basis.

(vi) The AMLCO maintains a register with the following data/information on the third parties with which the obliged entity has or had a business cooperation:

1. Name
2. Business address
3. Professional activities sector
4. Supervisory Authority
5. Commencement date of cooperation
6. Date of last evaluation
7. Date of next evaluation
8. Results of evaluation of customers recommended

9. Yearly number of customers recommended to the obliged entity in the last three years, by year
10. Number of customers reported to MOKAS
11. Date and reason for the termination of the business cooperation, if applicable

(vii) The AMLCO maintains a register with the following data/information on the third parties with which a business cooperation was rejected:

1. Name
2. Business address
3. Professional activities sector
4. Supervisory Authority
5. Date of rejection
6. Reasons for rejection

(viii) The commencement of the cooperation with the third party and the acceptance of the verification of identity of customers by the third party must bear the written and duly justified approval of the obliged entity's senior management, after taking into consideration any written comments/proposal made by AMLCO, which is kept in the individual record file of the third party maintained by the obliged entity.

4.8.9. ***Article 67(5) of the Law*** provides that Article 67 does not apply to outsourcing or agency relationships, where, on the basis of a contractual arrangement, the outsourcing service provider or the agent is to be regarded as part of the obliged entity.

4.9. Specific customer identification issues

4.9.1. Natural Persons

Obliged entities shall verify the identity of natural persons residing in Cyprus or abroad by obtaining the following information:

1. Customer name on the basis of the official national identity card or passport in force
2. Full permanent residence address
3. Telephone numbers
4. Email address

5. Date and place of birth
6. Profession or occupation of the customer including the name of employer/business organization
7. Annual Income

4.9.2. The name used should be verified by reference to a document obtained from a reliable and reputable source which bears a photograph. A current valid full passport, or a national identity card should be requested, and the relevant number should be registered. Having been satisfied that the original identification document/s has been presented, obliged entities should obtain a copy which is duly certified as described in Section 6.2.

4.9.3. In addition to the name verification, the customer's permanent residence address should be verified in one of the following ways:

(i) the presentation of a recent (up to 6 months) utility bill (e.g. water, electricity), or housing insurance document, or municipal taxes and/or bank account statement,

(ii) visit to the place of residence by a member of staff of the obliged entity.

4.9.4. For customers not permanently residing in Cyprus, in addition to the above, obliged entities are advised, if in any doubt, to seek to verify identity with a reputable financial institution in the client's country of residence.

4.9.5. The above information is also necessary, further to the objective of preventing money laundering and terrorist financing, for the purposes of implementing financial sanctions, trade embargoes or measures related to terrorism, terrorist financing or the proliferation of weapons of mass destruction, as imposed against different persons by the United Nations and the European Union or other organizations with whom the financial institution complies on the basis of its internal framework, as well as the lists of the United Nations and the European Union concerning individuals designated as terrorists or linked to terrorism. Therefore, the number, date and country of issue of the passport and the date of birth of the customer must always be indicated on the copies of the data obtained, so that the obliged entity can accurately ascertain whether the customer is included on a list of persons subject to sanctions issued by the United Nations or the European Union on the basis of the relevant UN Security Council Resolution and Regulation or Common Position of the Council of the European Union, respectively.

4.9.6. According to article 4(1) of the Implementation of the Provisions of the United Nations Security Council Resolutions or Decisions (Sanctions) and the Decisions and Regulations of the Council of the European Union (Restrictive Measures) Law of 2016 (58(I)/2016), any person who contravenes any of the provisions of the Security Council Resolutions or Decisions (sanctions) and/or the Decisions and Regulations of the Council of the European Union (restrictive measures) is guilty of an offence and without prejudice to any other provision of a law providing for a longer sentence, in the case of conviction, shall be subject to imprisonment not exceeding two years or to a penalty payment not exceeding one hundred thousand euros or to both sentences in the case of a natural person, and in the case of a legal person in a penalty payment not exceeding three hundred thousand euro.

4.9.7. According to Article 3(2) of Law 58(I)/2016, the supervisory authorities as defined in section 59 of the Law may take measures under the provisions of section (6) of article 59 of the Law where a person subject to their supervision fails to comply with the provisions of Law 58(I)/2016. Moreover, in accordance with Article 6 of Law 58(I)/2016 if a competent authority determines that a person undertakes any act in breach of any of the provisions of the Security Council Resolutions or Decisions (Sanctions) and/or Decisions and Regulations of the Council of the European Union (Restrictive Measures), reports the infringement to the Police for a relevant investigation.

4.9.8. Article 16B(1) of the Anti-Terrorism Law of 2010 (110(I)/2010) requires that obliged entities as defined in article 2 of the Law freeze all funds, financial assets and financial resources belonging to or controlled by a designated person or entity, owned or controlled in whole or in part, directly or indirectly, by a designated person or entity, derive or stem from funds or other assets owned or controlled, directly or indirectly, by a designated person or entity, owned or controlled by a person or entity, acting on behalf of, or following instructions by a designated person or entity.

4.9.9. According to article 16C(1) and (2) of Law 110(I)/2010, obliged entities report to their supervisory authorities who they, in turn, report to the Ministry of Foreign Affairs any assets that have been frozen or any action taken in relation to compliance with the restrictive measures of the European Union and the sanctions of the Security Council of the United Nations, as referred to in article 17 of Law 110(I)/2010. If an obliged entity fails to comply with the provisions of article 16C(1), then the supervisory authority may take the measures as provided for in section 59(6) of the Law.

4.10. Legal persons (companies)

4.10.1. Because of the difficulties of identifying beneficial ownership, transactions on behalf of legal persons (e.g. group policies), before a business relationship is established, when the legal person is not known, measures should be taken by way of a company search and/or other commercial enquires to ensure that the applicant company has not been, or is not in the process of being dissolved, struck off, wound-up, terminated. In addition, if changes to the company structure of ownership occur subsequently, or suspicions are aroused by a change in the profile of the business carried out by the company, further checks should be made. obliged entities should take all appropriate measures to fully establish the control structure and ownership of legal persons and verify the identity of the beneficial owners (natural persons) and the natural persons exercising the actual control of the company.

4.10.2. In the cases customers that are legal persons incorporated locally or abroad the obliged entity should ascertain the following:

1. Registration Number and date of incorporation.
2. Registered name and trading name used.
3. Registered office address.
4. Full addresses of the Head office/principal trading offices.
5. Telephone numbers, fax numbers and e-mail address.
6. Members of the board of directors.
7. The persons that are duly authorised to represent and act on behalf of the company.
8. The beneficial owners of private companies and public companies that are not listed in a recognised Stock Exchange of the European Union or a third country with equivalent disclosure and transparency requirements.
9. The registered shareholders acting as proxies (nominees) of the beneficial owners.
10. The business profile of the company in accordance with the provisions of Section 4.7 above.

4.10.3. The obliged entity should verify the identity of the person(s) authorized to represent the company, the registered shareholder(s) and the beneficial owner(s) and, in addition, obtain the original or certified copies of the following documents and data:

1. Certificate of incorporation.
2. Certificate of registered office.
3. Certificate of directors and secretary.
4. Certificate of registered shareholders.
5. Memorandum and Articles of Association.
6. A resolution of the Board of Directors of the company, certified by the company's Secretary, conferring authority to the persons who will represent the company and make transactions.
7. In the cases where the registered shareholders act as nominee(s) of the beneficial owner(s), a copy of the trust deed/agreement concluded between the nominee(s) and the true beneficiary(ies), by virtue of which the registration of the shares on the nominee(s) name on behalf of the beneficiary has been agreed.
8. Documents and data for the verification of the identity of the authorized signatories, the registered shareholders and ultimate beneficial owners in accordance with the provisions of these Orders.

4.10.4. For companies incorporated abroad, obliged entity should request and obtain documents similar to the above.

4.11. Enhanced due diligence measures

4.11.1. ***Article 64(3) of the Law*** requires obliged entities to apply enhanced customer due diligence measures, in addition to the measures as referred to in Articles 60, 61 and 62 of the Law and in other cases which by their nature, present a high risk of money laundering or terrorist financing. It is provided that when assessing the said risks the obliged entity takes into account at least the factors of potentially higher risk situations, as set out in Appendix III of the Law.

4.11.2. ***Article 64(1) and (4) of the Law*** requires obliged entities to apply enhanced due diligence measures in the following cases:

(i) When transacting with a natural person or legal entity with an establishment in a high risk third country.

(ii) In cross-border correspondent relationships with a third-country respondent institution, a credit institution and financial institution

(iii) In transactions or business relationships with a Politically Exposed Person,

(iv) When the transactions are complex and unusually large, and all unusual patterns of transactions, which have no apparent economic or lawful purpose

4.11.3. The customer acceptance policy of each obliged entity must determine the categories of customers considered to be of potentially high risk, as defined in the Law, in these Orders as well as for those customers the obliged entity has classified as of high risk on the basis of its risk assessment.

4.11.4. The criterion for obtaining satisfactory data evidence of a customer's identity should consider the risk of money laundering and terrorist financing deriving from each customer, and in each case obliged entities should make informed decisions about the appropriate measures to be applied. The extent and number of measures and controls to be effected for customer identification may vary depending on the risk deriving from the customer's characteristics such as country of origin, type of service or product requested by the customer, background and business or professional activities of the customer, the expected origin and size of funds etc. Data on the expected source of money, namely how payments will be effected, from where and by whom, should always be recorded in order to facilitate the subsequent control of transactions.

4.11.5. For customers classified as high risk, obliged entities must take, in addition to the usual due diligence measures, enhanced and additional measures to manage and mitigate appropriately the risks. As a minimum, the enhanced due diligence measures must include obtaining approval from a senior manager for the commencement or the continuation of a business relationship, the taking of adequate measures to ascertain the source of wealth to be transacted with the obliged entity and the systematic monitoring of the transactional behavior of the customer. Furthermore, the business relationship should be updated at least once a year or at a shorter interval if deemed necessary.

4.11.6. The AMLCO must be informed of the new high-risk customers that the obliged entity intends to accept, as well as the existing customers who fall into the high-risk category and exercise an advisory role before the final decision is taken. It is stressed that changing the risk category of high-risk customers to a lower level requires the approval of the AMLCO.

4.12. High Risk Customers

4.12.1. **Complex and unusually large transactions or unusual types of transactions**

Article 64(4) of the Law requires from an obliged entity to 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 obliged entity shall increase the degree and nature of the monitoring of the business relationship in order to determine whether these transactions or activities appear suspicious.

The obliged entity must apply adequate measures to identify complex and unusually large transactions or unusual types of transactions. Where an obliged entity detects such transactions because:

(i) are greater than expected on the basis of the institution's knowledge of the customer, the business relationship or the category to which the customer belongs;

(ii) they constitute an unusual or unexpected kind of transaction compared to the normal activity of the customer or the type of transactions associated with similar customers, products or services; or

(iii) are particularly complex compared to other similar transactions related to similar items, products or customer services.

and the obliged entity was not informed of the relevant economic rationale or the legitimate purpose or has doubts as to the accuracy of the information received, it must apply enhanced due diligence measures. These measures should allow the obliged entity to understand the background and purpose of these transactions, e.g. by locating the source and destination of the funds or by finding more information about the customer's business activity in order to determine the likelihood of the customer executing the specific transactions, and monitoring of the business relationship and the implied transactions more frequently and with greater attention to the details.

4.12.2. **Politically Exposed Persons ("PEPs")**

4.12.2.1 ***Article 2 of the Law*** (article 2) defines that Politically Exposed Person means a natural person who is or has been entrusted with prominent public functions in the Republic or in

a another country, an immediate close relative of such person as well as a person known to be a close associate of such persons:

(a) Provided that, for the purpose of the present definition, "prominent public function" means any of the following public functions:

(i) Heads of state, heads of government, ministers and deputy or assistant minister and assistant minister;

(ii) members of parliament or of similar legislative bodies;

(iii) members of the governing bodies of political parties;

(iv) members supreme courts, of constitutional courts or of other high-level judicial bodies, the decisions of which are not subject to further appeal, except in exceptional circumstances;

(v) members of courts of auditors or of the boards of central banks;

(vi) ambassadors, chargés d'affaires and high-ranking officers in the armed and security forces;

(vii) members of the administrative, management or supervisory bodies of State-owned enterprises;

(viii) directors, deputy directors and members of the board or equivalent function of an international organization;

(ix) mayor.

It is provided that the above-mentioned public functions do not cover middle-ranking or more junior officials.

(b) "Close relatives of a Politically Exposed Person" includes the following persons:

(i) Spouse or a person considered to be equivalent to a spouse of a Politically Exposed Person.

(ii) Children and their spouses, or persons considered to be equivalent to a spouse, of a Politically Exposed Person.

(iii) Parents of a Politically Exposed Person;

(c) "Person known to be a close associate of a Politically Exposed Person" means a natural person: -

(i) known to be jointly a beneficial owner of a legal entity or legal arrangement or is associated with any other close business relationship with a Politically Exposed Person,

(ii) who is the sole beneficial owner of a legal entity or legal arrangement which is known to have been set up for de facto benefit of a Politically Exposed Person.

4.12.2.2 ***Article 64(1)(c) of the Law*** requires, for transactions or business relationships with Politically Exposed Persons, from obliged entities to:

(a) have in place appropriate risk management systems, including risk-based procedures, to determine whether the customer or the beneficial owner is a Politically Exposed Person.

(b) apply the following measures in cases of business relationships with a Politically Exposed Person:

i. receive approval from senior management for establishing or continuing a business relationship with such a person;

ii. takes adequate measures to establish the source of wealth and source of funds that are involved in business relationships or transactions with such a person;

iii. conducts enhanced ongoing monitoring of that business relationship.

(c) apply the measures referred to in subparagraphs (i) and (ii) to close relatives or persons known as close associates of a politically exposed person.

4.12.2.3 Article 64(2) of the Law requires that:

(a) An obliged entity takes reasonable measures in order to determine whether the beneficiaries of a life insurance or other investment-related insurance policy and/or, where required, the beneficial owner of the beneficiary are politically exposed persons;

(b) The measures referred to in paragraph (a) shall be taken the latest at the time of the payout or at the time of the assignment, in whole or in part, of the insurance policy;

(c) When –

i. The beneficiary of a life insurance or other investment-related insurance policy and/or, where required, the beneficial owner of the beneficiary are politically exposed persons at the time of the payout or at the time of the assignment of the insurance policy; and/or

ii. higher risks are detected in transactions or in business relationships with a politically exposed person, in addition to the application of customer due diligence measures referred to in sections 60, 61 and 62, an obliged entity-

iii. informs senior management prior to payout of insurance policy proceeds; and

iv. conducts enhanced scrutiny of the entire business relationship with the policyholder.

4.12.2.4 Without prejudice to the application, on a risk sensitive basis, of enhanced customer due diligence measures, where a Politically Exposed Person has ceased to be entrusted with a prominent public function within the meaning described above, for a period of at least one year, obliged entities shall not be obliged to consider such a person as politically exposed.

4.12.2.5 Business relationships with Politically Exposed Persons may expose an obliged entity to increased risks, obliged entities should be more diligent when the said persons originate from a country which is widely known to face problems of bribery, corruption and financial irregularity and whose anti-money laundering statutes and regulations are not equivalent with international standards. In order to manage effectively such risks, obliged entities should assess the countries of origin of their customers so as to identify those countries that are more vulnerable to corruption or maintain laws and regulations that do not adequately meet the recommendations of the Financial Action Task Force ("FATF"). Regarding the issue of corruption, a useful source of information is the "Transparency International Corruption Perceptions Index" which can be found on the web-site of Transparency International at www.transparency.org. Regarding the issue of adequacy of application of the recommendations of the FATF, obliged entities may retrieve information from the country assessment reports prepared by FATF or other regional bodies operating

in accordance with FATF's principles (e.g. Moneyval Committee of the Council of Europe) the International Monetary Fund and the World Bank.

4.12.2.6 Obliged entities should adopt, further to the above legal requirements, the following additional 'due diligence' measures, when they have a new policy and/or establish a business relationship with a PEP:

(i) Establish appropriate risk management procedures to enable them to determine whether a prospective customer is a PEP. Such procedures should include, depending on the degree of risk each obliged entity faces, the acquisition and installation of a reliable commercial electronic database for PEPs which is available on the market, seeking and obtaining information from the customer himself or from publicly available information which, inter-alia, can be retrieved from the internet. In the case of companies, legal entities and arrangements, the procedures should aim at verifying whether the beneficial owners, authorized signatories and persons authorized to act on behalf of the company constitute PEPs. In case of identifying one of the above as a "Politically Exposed Person", then automatically the insurance policy of the company, legal entity or arrangement should be subject to the procedures stipulated in the Law and these Orders.

(ii) The decision for establishing a business relationship with a PEP should be taken by the obliged entity's Senior Management. When establishing a business relationship with a customer (natural or legal) and subsequently it is ascertained that the person(s) involved are or have become PEPs, then the approval of the obliged entity's Senior Management should be given for continuing the operation of the business relationship and/or insurance policy. In this respect, the obliged entity's systems should, at regular intervals and at least once a month, check their customers (and their associated natural persons) to identify such cases.

(iii) The AMLCO should provide comments as regards the relationship with a PEP and Senior Management should consider these comments and the level of risk of money laundering and terrorist financing to which the obliged entity may be exposed and to the extent to which the obliged entity has appropriate means for the effective management of that risk prior to the approval of the relationship.

(iv) Before establishing a business relationship with a PEP, the obliged entity should obtain adequate documentation to ascertain not only his/her identity but also to

assess his/her business reputation (e.g. references and letters of recommendation from third parties).

(v) Obliged entities should establish the business profile of the policyholder by obtaining the information prescribed in Section 4.7 above. The profile of the expected business activity should form the basis for the future monitoring of the insurance policy. The profile should be regularly reviewed and updated with new data and information. Obliged entities should be particularly cautious and most vigilant where their customers are involved in businesses which appear to be most vulnerable to corruption such as trading in oil, arms, cigarettes and alcoholic drinks;

(vi) The obliged entities apply appropriate measures to determine the source of the wealth and origin of the funds to be used in the context of the business relationship so that it can be assured that the undertaking is not managing revenue originating from corruption or other criminal activity. The measures that obliged entities should take to determine the source of the wealth and the origin of funds of the Politically Exposed Person depend on the degree of risk associated with the business relationship. Where the risk is particularly high, obliged entities should verify the source of the wealth and the origin of the funds on the basis of reliable and independent data, documents or information.

(vii) The obliged entity should perform enhanced and on-going monitoring of the customer transactions. If unusual transactions are identified and or new information is made available, then the risk profile should be re-evaluated. Furthermore, the insurance policy should be subject to annual review in order to determine whether the specific life insurance policy will continue to be in force. A memo should be prepared summarizing the results of the review by the insurance officer. The memo should be submitted for consideration and approval to the obliged entity's Senior Management and archived in the customer's personal file.

4.12.3. **Transactions with a natural person or legal entity established in a third country of high risk**

4.12.3.1 According to ***Article 64(1) of the Law***, obliged entities should apply enhanced customer due diligence measures, in addition to the measures referred to in Articles 60, 61 and 62 of

the Law, when dealing with a natural person or legal entity established in a high risk third country.

4.12.3.2 High risk third country means a third country, indicated by the European Commission[3] under the provisions of paragraph (2) of Article 9 of the European Union Directive through the publication of delegated acts, which presents strategic deficiencies in its national system for combating money laundering and terrorist financing, which are seen as major threats to the financial system of the European Union, and a third country, which is classified by the obliged entities as high risk, in accordance with the risk assessment provided for in Article 58A of the Law, risk assessment.

4.12.3.3 It is provided that, automatic application of enhanced customer due diligence measures is not required in the case of a branch or a subsidiary of majority participation in a high risk third country and the ownership status belongs to an obliged entity established in the European Union, where this branch or a majority-holding subsidiary complies fully with the policies and procedures applied at group level in accordance with the provisions of Article 68A and, in that case, the obliged entity implements a risk-based approach.

4.12.3.4 Additionally, ***Article 64(3) of the Law*** requires obliged entities to apply enhanced customer due diligence measures, in addition to the measures referred to in sections 60, 61 and 62 and in other cases which by their nature, present a high risk of money laundering or terrorist financing. It is provided that when assessing the said risks the obliged entity takes into account at least the factors of potentially higher risk situations, as set out in Appendix III.

4.12.3.5 The above risk factors include announcements published by the Financial Action Task Force (FATF), for countries that do not apply requirements for anti-money laundering and terrorist financing in line with the recommendations of the FATF. Specifically, in order to protect the international financial system from risks of money laundering and terrorist financing and to encourage countries to comply fast with international standards, FATF publishes after each meeting of its members, two documents with the names of countries

[3] COMMISSION DELEGATED REGULATION (EU) 2016/1675 of 14 July 2016, supplementing Directive (EU) 2015/849 of the European Parliament and of the Council by identifying high-risk third countries with strategic deficiencies https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R1675&from=EN. This Regulation was subsequently amended by the delegated acts 2018/105 and 2018/1467.

having strategic weaknesses/shortcomings in the field of money laundering and terrorist financing and working with them to address these shortcomings.

4.12.3.6 According to the recommendation number 19 of the FATF, financial institutions are required to apply enhanced due diligence and monitoring measures with business relationships or transactions with natural or legal persons or financial institutions that originate from countries that do not or inadequately apply the FATF recommendations.

4.12.3.7 Obliged entities may increase the information received for customer identification and due diligence measures as well as the intended nature of the business relationship. Furthermore, additional diligence should be exercised as regards the beneficial owners and the origin of the funds to be received and also frequent and thorough monitoring of transactions in order to identify any unusual or unexpected transactions which may raise suspicions of money laundering and terrorist financing.

4.13. On-going monitoring of the business relationship, insurance policies and transactions

4.13.1. ***Article 61(1)(d) of the Law*** requires that identification procedures and customer due diligence measures include the exercise of ongoing monitoring of the business relationship including scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the information and data in the possession of the obliged entity in relation to the customer, the business and risk profile of the customer, including where necessary, relating to the source of funds and ensuring that the documents, data or information held are kept up-to-date.

4.13.2. ***Article 58(e) of the law*** requires, inter alia, obliged entities to examine in detail any transaction which by its nature maybe considered to be particularly vulnerable to be associated with money laundering offences or terrorist financing and in particular complex or unusually large transactions and all other unusual patterns of transactions which have no apparent economic or visible lawful purpose.

4.13.3. Ongoing monitoring of customer insurance policies and transactions is an essential element of any effective system of anti-money laundering and terrorist financing procedures. obliged entities must have a full understanding of the normal and justified movement of their customers' insurance policies and of their overall economic profile so

that they can identify transactions outside the ordinary or constitute complex or unusual transactions or are carried out without any apparent financial purpose or clear legal reason.

4.13.4.The procedures, the frequency and depth of the examination of transactions and the monitoring of insurance policies should consider the level of risk and achieve, as a minimum, the following:

(i) Creation of reports and/or warning messages/alert rules for suspicious or unusual transactions, according to specific parameters and scenarios defined.

(ii) The investigation of unusual or suspicious transactions by competent employees appointed for this purpose. The results of the investigations should be recorded and be readily available for inspection.

(iii) Taking all necessary measures and actions on the basis of the findings of the investigation including the internal reporting of suspicious transactions/activities to the AMLCO.

4.13.5. The filtering of the financial institution's customer base on the basis of the lists of persons or entities subject to restrictive measures, issued on the basis of relevant European Union Regulations and Decisions of the Security Council of United Nations. The filtering is carried out at the beginning of the business relationship. With the introduction of new persons in existing lists or new lists, the information system filters the customer base of the obliged entity, in order to ascertain whether it maintains or maintained a business relationship with the specific persons or entities.

4.13.6. The monitoring of the insurance policies and transactions must be carried out in relation to certain types of transactions, the economic profile of the customer, the usual turnover/activities of the customer and comparing at regular intervals the movement of the insurance policy with the expected movement of the insurance policy. Significant deviations should be further investigated, and the findings should be recorded in a separate memo which is archived in the customer's file.

4.13.7. The obliged entity will create thorough policies and procedures outlining the way transaction monitoring is conducted and the parameters/scenarios that are taken into consideration. Monitoring will be conducted by the aggregation of premiums and

movement of all linked insurance policies on a consolidated basis and the production of budge alerts and exception reports where deviations from the specified parameters, scenarios and thresholds will be detected and will be investigated by the AMLCO and/or competent employees assigned with this type of responsibility and sufficiently trained to carry out their duties effectively'.

4.13.8. The needs of each obliged entity will be different, and each system will vary depending on the relative risk assessment and its capabilities according to the size, nature and complexity of the institution. These should be updated periodically so as to consider and reflect changes in laws and directives, as well as any other information the obliged entity determines as relevant.

5. CASH DEPOSITS AND WITHDRAWALS

5.1. Cash Deposits

5.1.1. Cash is an important tool and one of the preferred methods for money laundering and terrorist financing. Hence to enhance the system for anti-money laundering and combating terrorist financing it is essential to have effective methods of detecting illegal funds at the initial stage and when criminals attempt to place cash from illegal activities in the financial system.

5.1.2. Obliged entities and Insurance Intermediaries should apply appropriate procedures for accepting and checking cash deposits on a Risk Based Approach. Obliged entities are required, depending on the estimated risk, to exercise control in order to ascertain the source and origin of the cash and also to determine whether the amount and nature of the transaction is consistent with the activities/operations and economic profile of the customer. Additionally, and depending on the limits and controls to be set by each obliged entity, appropriate documentary evidence and data on the financial, commercial or other purpose of the cash deposit should be obtained, which should be performed after approval is received from a higher authority. Similar checks should also be carried out for cash deposits when it is suspected that the transaction is likely to be linked to money laundering or financing of terrorism.

5.1.3. Obliged entities are prohibited from accepting cash in foreign currency.

5.2. Deposits of cash imported from abroad

5.2.1. Obliged entities are prohibited from accepting cash deposits in euro of a value equal to or greater than 10,000 euro imported from abroad where:

(i) these are not accompanied by the relevant import declaration to the Customs Department ("Cash Declarations") under Regulation (EC) 1889/2005 of the European Parliament and of the Council on cash checks entering or leaving the Community[4] and the control of cash entering or leaving the community and the Exercise of Intra-Community Controls Law (N. 53 (I) of 2009)[5] or

(ii) the import declaration contains incomplete, false or untrue evidence.

5.2.2. In that regard, it is clarified that under Regulation (EC) 1889/2005 of the European Parliament and of the Council on cash checks entering or leaving the Community and the control of cash entering or leaving the community and the Exercise of Intra-Community Controls Law (N. 53 (I) of 2009) , any natural person entering Cyprus from a third country or another Member State of the European Union and carries cash of a value equal to or more than 10,000 euro is required to declare the amount in question to a competent officer of the Customs department.

5.3. Definitions of group of connected persons and linked cash deposits

5.3.1. "Group of connected persons" consists of:

(i) family members (i.e. spouse and children),

(ii) a natural person and a business entity in which the natural person and any member of his family is a partner or a member or director or beneficial owner or has in any way the control,

(iii) a natural person and a company in which the natural person is a director or possesses substantial interest either on his own or with other members of his family or together with other partners,

(iv) legal person and parent company, subsidiaries, affiliates, connected companies or other entities which have a substantial interest in the legal entity,

[4] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32005R1889&from=EN
[5] http://www.cylaw.org/nomoi/enop/non-ind/2009_1_53/full.html

(v) two or more persons, natural or legal, who have economic dependency or are associated in such a way that they may be considered to represent a single risk.

5.3.2. For the purposes of the above, "substantial interest" in a company means the interest in any class of shares of the company's capital, with a rate of 25% or more in the class of such shares or interest which gives in any way the ability to someone to decide the election of the majority of the company's Directors or to exert significant influence.

6. RECORD KEEPING PROCEDURES

6.1. Introduction

6.1.1. ***Article 68(1) of the Law*** requires obliged entities to maintain the following documents and information, for a period of five (5) years after the end of the business relationship with the customer or after the date of an occasional transaction:

(a) Copies of documents and information required for compliance with the customer due diligence requirements as determined by the Law;

(b) relevant evidence and records of transactions which are necessary for the identification of transactions;

(c) relevant correspondence documents with customers and other persons with whom a business relationship is maintained.

6.1.2. ***Article 68(2) of the Law*** requires an obliged entity to ensure that all documents referred to in subsection Article 68(1) of the Law are promptly and without delay made available to MOKAS and the Superintendent of Insurance for the purpose of execution of the duties assigned to them pursuant to the provisions of the Law

6.2. Certification

6.2.1. The copies of the customer identification evidence must be certified by the obliged entity employee or the Insurance Intermediary who verifies the identity of the customer or the third party to whom the obliged entity relies for the purpose of verifying the identity of the customer. The certification should bear the name and signature of the person certifying the document and the date of certification. In the case of a third party it should bear the

stamp of the third party to whom the obliged entity relies for the purpose of verifying the identity of the customer.

6.2.2. For non- Cypriots in case of natural persons and/or legal persons or entities that have not been incorporated in Cyprus, obliged entities may obtain documents bearing the stamp Apostille, in accordance with the Hague Convention, and which are translated into Greek or English for the proper understanding of their content. These documents, which bear the Apostille stamp, must be the original and carry the distinctive serial number which has been designated by the Central Authority in the country of issue. The obliged entity, after having seen the original documents, may maintain true copies of the said documents in the customer file. The said copies must be certified by an employee of the obliged entity, bear the name of the employee, the signature of the employee who certifies the documents as well as the date of the certification.

6.2.3. Other methods of certification

(a) A Notary Public – (not Certifying Officer)

(b) The Embassy or Consulate of the Cyprus Republic

6.3. Data Protection

6.3.1. ***Article 70B of the Law*** provides that the processing of personal data carried out under the provisions of the Law is subject to the provisions of the Law providing for the Protection of Natural Persons with regard to the Processing of Personal Data and for the Free Movement of such Data Law. Also, personal data are processed by obliged entities only for the purposes of the provisions of the Law and are not subject to any other incompatible processing. The processing of personal data for purposes other than those provided for by Law, such as commercial purposes, is prohibited.

6.3.2. Obliged entities must provide their new customers with the information required under Article 11(1) of the Law providing for the Protection of Natural Persons with regard to the Processing of Personal Data and for the Free Movement of such Data Law, prior to the commencement of a business relationship or the execution of an occasional transaction. Obliged entities should provide information to their new customers before commencing the business relationship or executing an occasional transaction about the processing of

personal data under the provisions of the Law for the purpose of preventing money laundering and terrorist financing.

6.3.3. The right of access by the data subject to the data relating to it may be partially or wholly waived in accordance with the provisions relating to the Law providing for the Protection of Natural Persons with regard to the Processing of Personal Data and for the Free Movement of such Data of 2018 (Law 125(I)/2018) -

(a) For the purpose of the proper fulfilment of the duties of obliged entities and supervisory authorities, as they derive from the Law,

(b) in order not to obstruct the conduct of official or legal investigations, analysis or procedures for the purposes of the Law and to ensure that the prevention, investigation and detection of money laundering and terrorist financing are not jeopardized.

6.4. Record Keeping

6.4.1. The processing of personal data under the provisions of the Law in order to prevent money laundering and terrorist financing is considered a matter of public interest in accordance with the provisions of Directive 95/46/EC.

6.4.2. Obliged entities must ensure that all the above documents are promptly and without any delay made available to MOKAS and the competent Supervisory Authorities for the purpose of discharging their legal duties.

6.4.3. Moreover, obliged entities must apply appropriate systems which will enable them to promptly identify and inform Superintendent of Insurance and MOKAS as to whether they maintain or have maintained, during the previous five years, a business relationship with specified natural or legal persons and on the nature of that business relationship.

6.4.4. MOKAS needs to be able to compile a satisfactory audit trail and destination of illicit money and be able to establish the business profile of any insurance policy and customer under investigation. To satisfy this requirement, obliged entities must ensure that they will be able to promptly provide the following information in the case of a money laundering investigation by MOKAS:

(c) The identity of the policy holder(s).

(d) The identity of the beneficial owner(s).

(e) The value and volume of premiums or number of policies.

(f) The value and volume of premiums of related persons policies

(g) For selected policy(ies):

(i) The origin of the funds;

(ii) The type and amount of the currency involved;

(iii) The form in which the funds were deposited or withdrawn i.e. cash, cheques, wire transfers etc.;

(iv) The identity of the person undertaking the transaction;

(v) The form of instructions and authority.

6.5. Format of Records

6.5.1. It is recognized that copies of all documents cannot be retained indefinitely. Prioritization is, therefore, a necessity. Although the Law prescribes a period of retention, where the records relate to on-going investigations, they should be retained until it is confirmed by the competent authority, that is conducting the investigation, that the case has been closed.

6.5.2. Keeping the data and the documents for the identity, transactions, business correspondence and other details comprising the customer's business profile creates a large volume of records that need to be stored. Therefore, retention may be in other formats, except for the original documents, such as electronic or other form. The main objective is to allow obliged entities to promptly and without delay retrieve relevant information.

6.5.3. In defining their document retention policy, obliged entities should consider both the statutory requirements and the potential needs of MOKAS and the competent supervisory authorities.

6.5.4. ***Article 47 of the Law*** provides that in the cases that the relevant information is stored in a computer, it must be possible to present them in a visible and legible form, so that they can be transmitted to MOKAS.

7. EDUCATION AND TRAINING

7.1.1. ***Article 58(f) and (g) of the Law*** requires that an obliged entity applies adequate and appropriate policies, controls and procedures, which are proportionate to its nature and size, to mitigate and manage the risks of money laundering and terrorist financing effectively, in relation to the following:

58(f) informing its employees in relation to:

(i) the systems and procedures in accordance with Article 58 paragraphs of (a) to (e)

(ii) the Law

(iii) the Directives and Orders issued by the competent Supervisory Authority according to Article 59(4) of the Law

(iv) the European Union's Directives on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing and

(v) the relevant requirements for personal data protection.

58(g) ongoing training of their staff to recognize and handle transactions and activities suspected to be related with money laundering or terrorist financing activities.

7.1.2. The effectiveness of the procedures and recommendations contained in these Orders and other relevant circulars of the Superintendent of Insurance in relation to the prevention of money laundering and terrorist financing depends on the extent to which obliged entity's staff appreciate the seriousness of subject matter and the risks it imposes on the obliged entity and the financial system of the and the level of their education with regard to their duties and statutory obligations for countering this serious problem. It is reminded that staff is personally liable for failure to report information, regarding money laundering and terrorist financing, in accordance with the internal reporting procedures. Consequently, staff of obliged entities must be encouraged to cooperate and report, without delay, anything that comes to their attention in relation to transactions for which there is a slight suspicion that they are related to money laundering or terrorist financing. In this regard, it is crucial that obliged entities establish adequate measures to ensure that their staff is fully aware of their duties and responsibilities. In this regard, the AMLCO has the responsibility, in cooperation with other competent units of the obliged entity (i.e. Human Resources

department), to prepare and implement, on an annual basis, an education and training programme for the staff as required by the Law and these Orders.

7.1.3. The Board of Directors and the Senior Management must be informed of their responsibilities under the Law and these Orders as well as the changes and new developments in the legal and regulatory framework. Although the education of the Board of Directors and Senior Management of the obliged entity is not expected to be the same as the training offered to the rest of the staff, however they must understand the importance of the requirements of the Law and the relevant Directives and Orders, the consequences of non-compliance and the risks for the institution. Without a general understanding of the aforementioned requirements, the Board of Directors and the Senior Management will not be able to provide adequate management supervision, approve policies, procedures or provide sufficient resources for the effective prevention of money laundering and terrorist financing.

7.1.4. The AMLCO ensures that the obliged entity maintains information in relation to the training seminars and other education provided to the staff/Insurance Intermediary on the prevention of money laundering and terrorist financing and assesses the adequacy of the training and education provided. The following information shall be kept, as a minimum:

(a) Employee name by department and by position or Insurance Intermediary name.

(b) Date, title, timetable and duration of the seminar and the names and qualifications of the instructors.

(c) Whether the lecture/seminar was prepared internally or offered by an external organization.

(d) Summary information for the content of the seminar.

7.1.5. The timing and content of the training provided to the staff of the obliged entity should consider the size and nature of the activities of each obliged entity. Furthermore, the frequency of training can vary depending on the amendments to the legal and/or regulatory requirements, staff duties, new recruits as well as any other changes in the country's overall financial system.

7.1.6. The training programme should aim at educating staff on the latest developments and typologies in anti-money laundering and terrorist financing including the practical methods

and trends used by criminals for this purpose. The training programme should have a different structure for new staff, customer service staff, compliance staff, staff moving from one department to another or staff dealing with the attraction of new customers. New recruits should be educated in understanding the importance of preventive policies against money laundering and terrorist financing and the procedures, measures and controls that the obliged entity has in place for that purpose. Customers service staff dealing directly with the public should be trained on the verification of new customers' identity, the exercise of due diligence on an on-going basis, the monitoring of insurance policies of existing customers and the detection of patterns of unusual and suspicious activity. On-going training should be given at regular intervals to ensure that staff is reminded of its duties and responsibilities, changes in the legal and regulatory framework, changes in the policies, procedures and controls of the obliged entity and kept informed of any new developments.

7.1.7. It is crucial that all members of staff directly involved in the anti-money laundering and terrorist financing preventive system fully understand the need to implement consistently policies and procedures for that purpose. In this regard, obliged entities should promote a culture and understanding among their staff with regard to the importance of the prevention and its key role to the successful implementation of the related policy and procedures.

8. RECOGNITION, INTERNAL REPORTING AND REPORTING TO MOKAS OF SUSPICIOUS TRANSACTIONS/ACTIVITIES

8.1. Internal Report of suspicious transactions/activities

8.1.1. ***Article 27 of the Law*** specifies that it is an offence for any person who, in the course of his trade, profession, business or employment, acquires knowledge or reasonable suspicion that another person is engaged in money laundering or terrorist financing not to report this knowledge or suspicion as soon as it is reasonably practical, after the information came to his/her attention, to MOKAS. Failure to report in these circumstances is punishable on conviction by a maximum of two (2) years imprisonment or a fine not exceeding 5.000 euro or both penalties. The staff should report to the AMLCO their knowledge or suspicion of money laundering or terrorist financing on an "Internal Suspicion Report for money laundering and terrorist financing" as listed in Appendix 1.

8.1.2. In the case of personnel of obliged entities, ***Article 26 of the Law*** provides that the internal suspicious report to the AMLCO constitutes fulfilment of the legal obligation to disclose information deriving from Article 27. Therefore, obliged entities should ensure that all staff are aware of their legal obligations and the person (i.e. the AMLCO) to whom they will report their knowledge or suspicions of money laundering or terrorist financing.

8.1.3. ***Article 70 of the Law*** requires persons engaged in financial or other business to refrain carrying out transactions which they know or suspect to be related with money laundering or terrorist financing before they inform MOKAS of their suspicion in accordance with Articles 27 and 69 of the Law. As already mentioned above, the obligation to report to MOKAS includes also the attempt to carry such suspicious transactions. It is provided that if it is impossible to refrain from carrying out the transaction or is likely to frustrate efforts to pursue the persons of a suspected money laundering or terrorist financing operation, the obliged entities must inform MOKAS immediately afterwards.

8.1.4. In accordance with ***Article 69A of the Law***, disclosure of information in "good faith" by an obliged entity or by an employee or by a director of such an obliged entity, in accordance with the provisions of Article 69 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 obliged entity or its directors or

employees 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.

8.1.5. In accordance with ***Article 69B of the Law***, a person who submits an internal report or a report to MOKAS for suspicious transactions pursuant to the provisions of section 69, is protected from being exposed to threats or hostile action, and in particular from adverse or discriminatory employment actions.

8.1.6. Considering that obliged entities and Insurance Intermediaries ensure that they always hold sufficient information, that they have built a substantial economic profile and that they are aware of the activities of their customers so that they are able to promptly recognize that a transaction does not fall within the scope of the size and the activities of the customer and is unusual or suspicious.

8.1.7. Additional to the identification of suspicious transactions relating to money laundering, obliged entities and Insurance Intermediaries must ensure that they have appropriate tools in place for identifying suspicious transactions involved in terrorist financing. The funding of terrorist organizations is done from revenue originating from both legal and illegal sources.

8.1.8. All "Internal Suspicious Reports" must be archived by the AMLCO.

8.2. AMLCO Evaluation of Internal Suspicion Report and report to MOKAS

8.2.1. The AMLCO evaluates and examines the Internal Suspicion Report received citing other available sources of information and discusses the events in relation to the specific case with the reporting employee and, where deemed necessary, with the senior officers of the reporting employee. The evaluation of the information included in the suspicion report submitted to the AMLCO should be made on a separate form which should also be archived in the relevant file. The said report, which is referred as "Evaluation of Internal Suspicion Report for money laundering and terrorist financing", is attached, as Appendix 2, to these Orders. As part of the review, other linked insurance policies or relationships of the customer that was reported should be considered.

8.2.2. If as a result of the evaluation described above, the AMLCO decides not to disclose the relevant information to MOKAS, then he/she should fully explain the reasons for the decision in the "Evaluation of Internal Suspicion Report for money laundering and terrorist financing" which, as already mentioned, should be archived in the relevant file.

8.2.3. If, as a result of the evaluation described above, the AMLCO decides to reveal the information to MOKAS then his/her report should be submitted to MOKAS via the secure communication channels as defined by MOKAS, the sooner possible. Obliged entities should have the submitted reports in a printed form for audit purposes.

8.2.4. The AMLCO must include in the Suspicion Report all relevant information concerning the customer, transactions or activities, according to the information in his/her possession.

8.2.5. After the submission of a suspicion report to MOKAS the transactions of all customers included in the report should be duly monitored by the AMLCO.

8.2.6. If, as a result of the evaluation described above, the AMLCO decides not to reveal the relevant information to MOKAS then he/she should fully explain the reasons for such a decision on the "Evaluation of Internal Suspicion Report for money laundering and terrorist financing" which should, as already stated, be archived in the relevant file.

8.2.7. The AMLCO acts as a first point of contact with MOKAS, upon commencement of, and during the investigation of the case examined after the submission of the suspicion report to MOKAS.

8.2.8. After submitting the suspicion report, the obliged entity may wish to discontinue the relationship with the customer to avoid the risk involved in continuing the operation of that insurance policy. In such a case, the obliged entity should be particularly attentive so that, in accordance with Article 48 of the Law, they do not disclose to the customer that a suspicion report has been submitted to MOKAS. Therefore, there must be close contact with MOKAS to avoid creating any obstacles or difficulties in conducting the investigations.

8.2.9. After submitting the suspicion report, obliged entities must follow any instructions given by MOKAS, in particular whether they will complete a particular transaction or keep the specific insurance policy in service. It is noted that Article 26(2)(c) of the Law provides the authority to MOKAS to instruct obliged entities, such as, not to execute or delay the

execution of a customer instruction without such action being considered as a violation of any contractual or other obligation of the obliged entities and its employees.

8.2.10. ***Article 71 of the Law*** provides that the non-execution or the delay in execution of any transaction for the account of a customer, by an obliged entity shall not constitute breach of any contractual or other obligation of the said person towards its customer if it is due to-

(a) the non-provision of sufficient details or information for-

(i) the nature and the economic or commercial purpose of the transaction, and/or

(ii) the parties involved, as required by the Regulation (EC) no. 1781/2006 of the European Parliament and of the Council of 15 November 2006 on information on the payer accompanying transfers of funds, or

(b) the knowledge that the money held to the credit of the account or the transaction, may be connected with money laundering or terrorist financing offences or with the commission of other criminal offence.

8.2.11.***Article 26(2)(c) of the Law*** provides that where a person discloses to MOKAS his/her suspicion or belief that any funds or investments are derived from or used in connection with a predicate offence or any matter on which such a suspicion or belief is based - The non-execution or the delay in the execution of an order by the said persons upon instructions of MOKAS, with regard to sums or investments referred to above, shall not constitute violation of any contractual or other obligation on the said persons or/and his/his employers.

8.3. Examples of suspicious transactions/activities

8.3.1. A criminal seeking to legalize income from illegal activities or to finance terrorism will try to use any product or service offered by the obliged entities as a means of making illegal money look legal. This process can vary from a simple cash transaction to more pretentious and complex transactions. A list containing examples of suspected transactions/activities related to money laundering and terrorist financing is attached in Appendix 3 of these Orders.

8.3.2. The list attached in Appendix 3 is only a sample list aiding obliged entities, Insurance Intermediaries and their staff in identifying the main ways in which illegal revenues are legalized and terrorism is financed as well as understand the methodologies used. The identification by obliged entities and Insurance Intermediaries of any of the transactions listed in Appendix 3 should be the subject of further investigation and a reason for seeking additional information and/or explanations concerning the source and origin of the funds, the nature and the economic/commercial purpose of the transaction as well as the events associated with the specific activity.

9. IMPLEMENTATION OF THESE ORDERS BY THE BRANCHES AND SUBSIDIARIES OF INSURANCE UNDERTAKINGS

9.1.1. ***Article 68A(1) and (2) of the Law*** requires that Insurance Undertakings belonging to a Group to implement group-wide policies and procedures, including data protection policies, as well as policies and procedures for sharing information within the Group, for the purpose of preventing money laundering and terrorist financing. In addition, they shall ensure that these policies and procedures are effectively implemented at the level of branches and majority-owned in Member States and third countries.

9.1.2. According to ***Article 2 of the Law***, a Group shall mean a group of Insurance Undertakings consisting of a parent undertaking, its subsidiaries and the entities in which the parent undertaking or its subsidiaries hold a participation, as well as undertakings linked to each other by a relationship within the meaning of Article 22 of Directive 2013/34/EU.

9.1.3. The proper management of money laundering and terrorist financing risks, when an Insurance Undertaking operates in other jurisdictions, involves examining the legal requirements of the host country. Given the risks, each Group should develop policies and procedures to prevent money laundering and terrorist financing at Group level and implemented consistently and supervised within the whole Group. In turn, the policies and procedures at the branch or subsidiary level, although reflecting the local business considerations and the requirements of the host jurisdiction, must be compatible and support the broader Group policies and procedures. In cases where the host country's requirements are more stringent than the group's requirements, the Group's policy must allow the relevant branch or subsidiary to adopt and apply the local requirements of the host country.

9.1.4. ***Article 68A(3) of the Law*** requires Insurance Undertakings which operate facilities in another member state to comply with the provisions of that other member state which have been transposed into the national laws for the purpose of harmonization with the EU Directive.

9.1.5. Article ***68A(4) of the Law*** requires branches or majority-owned subsidiaries of an Insurance Undertaking located in a third country, where the minimum requirements for preventing money laundering and terrorist financing are less strict from those provided in the Law and the Orders and Circulars issued by the Superintendent of Insurance, the said branches and subsidiaries apply the requirements provided in the Law and the orders and circulars issued by the Superintendent of Insurance, including data protection requirements, to the extent permitted by the laws of the third country where they are located.

9.1.6. ***Article 68A(5) of the Law*** provides that If the legislation of a third country does not permit the application of the aforementioned policies and procedures, the Insurance Undertaking which maintains branches and majority-owned subsidiaries in that third country must immediately inform the Superintendent of Insurance and take additional measures to effectively address the risk of money laundering or terrorist financing. In addition, the Superintendent of Insurance might, if necessary, ask the Group to terminate its activities in the third country, in case the additional measures which the Insurance Undertakings have to take are not sufficient.

9.1.7. Insurance Undertakings with branches or subsidiaries in another Member State or third country should designate the AMLCO as coordinator to:

(a) Assess the potential risks arising from the activity indicated by branches and subsidiaries of the Group and where it is considered necessary to assess the risks on the Group by a particular customer or category of customers.

(b) Manage the risk arising from money laundering and terrorist financing,

(c) Ensure implementation, by all branches and subsidiaries of the group, of the Group policy as well as adequate and appropriate systems and procedures for the effective prevention of money laundering and terrorist financing offences.

(d) Monitor on a continuous basis the compliance of obligations through on-site or distance audits.

9.1.8. Insurance Undertakings should determine the purpose and extend of the exchange of information based on the sensitivity of the information and relevance/relation/importance in the management of risks arising from money laundering activities and terrorist financing. The policies and procedures should provide for the required exchange of information allowing the effective and efficient mitigation of the risks for money laundering and terrorist financing.

10. WITHDRAWAL AND CANCELLATION OF PREVIOUS CIRCULARS, ORDERS AND AMENDMENTS

10.1.1. Orders for obliged entities (FOURTH ISSUE) for the prevention of money laundering and terrorist financing of April 2014 and the subsequent amendments issued by the Superintendent of Insurance in accordance with article 59(4) of the "Prevention and Suppression of Money Laundering Activities Law" are revoked and cancelled.

APPENDIX 1

INTERNAL MONEY LAUNDERING SUSPICION REPORT

REPORTER

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

Branch/Dept. ..... Fax .....

Position ..... E-mail .....

CUSTOMER

Name: ....

Address: ....

..... Date of birth .....

Contact/Tel/Fax/E-mail ..... Occupation/Employer .....

..... Details on employer: .....

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

ID Card No ..... Other ID .....

INFORMATION/SUSPICION

Brief description of activities/transaction ....

....

....

Reason(s) for suspicion ....

....

REPORTER'S SIGNATURE ..... **Date** .....

FOR MONEY LAUNDERING COMPLIANCE OFFICER'S USE

Date received ..... Time received ..... Ref .....

MOKAS Advised Yes/No Date ..... Ref .....

APPENDIX 2

ANTI-MONEY LAUNDERING COMPLIANCE OFFICER'S INTERNAL EVALUATION REPORT

Reference.....Customer.....

Reporter.....Branch/Dept.....

ENQUIRIES UNDERTAKEN (Brief description)

.....

.....

.....

DOCUMENTS RESEARCHED/ATTACHED

.....

.....

.....

DECISION OF THE AMLCO

.....

.....

.....

FILE REFERENCE .....

MONEY LAUNDERING
COMPLIANCE OFFICER'S Signature.....Date .....

APPENDIX 3

EXAMPLES OF ACTIVITIES RELATED TO MONEY LAUNDERING AND TERRORIST FINANCING OPERATIONS AND OTHER IMPORTANT ADVICE

The following examples may be indicators of a suspicious transaction report, however it must be noted that the list is not exhaustive.

- **Large Sum of Premiums**

  Obliged entities should be particularly cautious when clients are asking to conclude a single premium life insurance contract with a large sum of premiums paid in cash. It is commonly accepted that in the insurance sector the single premium policies can more easily be used for money laundering purposes. Therefore, obliged entities are encouraged to be particularly cautious when the single premium is greater that the annual salary of the client and even more cautious in cases of cancellations of those policies before maturity.

- **Return Premiums**

  There are several cases where the early cancellation of policies with return of premium has been used to launder money. This has occurred where there have been:

  - a number of proposals entered into by the same insurer/Insurance Intermediary for small amounts and then cancelled at the same time.
  - return premium being credited to a insurance policy or person different from the original insurance policy/ person
  - requests for return premiums in currencies different to the original premium.

- **Overpayment of premiums**

  Another simple method by which funds can be laundered is by arranging for excessive numbers or excessively high values of insurance reimbursements by cheque or wire transfer to be made. A money launderer may well own legitimate assets or business as well as an illegal enterprise. In this method, the launderer may arrange for insurance of legitimate assets and "accidentally", but on a recurring basis, significantly overpay his premiums and request a refund for the excess. Often, the person does so in the belief that his relationship with his representative at the company is such that the representative will be unwilling to confront a customer who is both profitable to the company and important to his own success.

The overpayment of premiums has been used as a method of money laundering. Insurers should be especially vigilant where:

- the overpayment is over a certain size (say €1.000 or equivalent)
- the request to refund the excess premium was to a third party
- the assured is in a jurisdiction associated with money laundering or terrorist financing and
- where the size or regularity of overpayments is suspicious
- reinstatement of contracts with high sums assured.

➢ **Additional Indicators of suspicious transactions**

- Application for a policy from a potential client in a distant place where a comparable policy could be provided "closer to home".
- Any request of information or delay in the provision of information to enable verification to be completed.
- The client accepts very unfavorable conditions unrelated to his or her health or age
- Large funds flows through non-resident accounts with Insurance Intermediary firms
- The client requests an insurance product that has no discernible purpose and is reluctant to divulge the reason for the investment.
- Insurance policies with values that appear to be inconsistent with the client's insurance needs and means.
- The client conducts a transaction that results in a conspicuous increase of investment contributions
- The applicant for insurance business requests to make a lump sum payment by a wire transfer or with foreign currency
- The applicant for insurance business wants to borrow the maximum cash value of a single premium policy, soon after paying for the policy.

➢ **Important advice to Insurance Undertakings**

Obliged entities should be extremely cautious in the following cases:

- When designing new products, the obliged entities should take into consideration whether the particular product can be used for money laundering or terrorist financing.
- Obliged entities should encourage their clients not to pay their premiums in the form of cash. They should, also, include certain provisions in their contracts, for the payment of extra amounts, especially when those are in cash.
- To avoid any misuse of the claims payment procedure, the Insurance Undertakings are advised to make the payments of the relative amounts only through Insurance Undertaking transfers and not make any cash or cheque payments. The name of the insurance policy holder always has to match with the authorized receiver of the money.
- To consider making a STR where higher risks are identified in relation to life insurance policies with the involvement of a PEP as a beneficiary or the beneficial owner of the beneficiary.