CENTRAL BANK OF CYPRUS

UNOFFICIAL TRANSLATION OF THE PREVENTION OF MONEY LAUNDERING AND TERRORIST FINANCING DIRECTIVE OF 2025

This translation is not official. It has been prepared by the Central Bank of Cyprus to assist users

THE PREVENTION AND SUPRESSION OF MONEY LAUNDERING AND TERRORIST FINANCING LAWS OF 2007 TO 2024 - DIRECTIVE PURSUANT TO ARTICLE 59(4)

Directive pursuant to Article 59(4)

CONTENTS

188(I)/2007
58(I)/2010
80(I)/2012
192(I)/2012
101(I)/2013
184(I)/2014
18(I)/2016
CORRECTION OJ, Appendix I(I), No 4564
13(I)/2018
158(I)/2018
81(I)/2019
13(I)/2021
CORRECTION OJ, Appendix I(I), No 4816
22(I)/2021
61(I)/2021
CORRECTION OJ, Appendix I(I), No 4880, d.o.b. 18.3.2022
40(I)/2022
98(I)/2023
118(I)/2024
141(I)/2024

The Central Bank of Cyprus, exercising the powers conferred on it under Article 59(4) of the Prevention and Suppression of Money Laundering Activities Laws of 2007 to 2024, and for the adoption of the European Banking Authority Guidelines on risk factors (EBA/GL/2021/02), the role of the Anti-Money Laundering Compliance Officer (EBA/GL/2022/05), the use of remote customer onboarding solutions (EBA/GL/2022/15) and Article 36 of Regulation (EU) 2023/1113 (EBA/GL/2024/11), adopts this Directive.

		PART 1 TITLE, DEFINITIONS, SCOPE OF APPLICATION AND PURPOSE.
Short title	1.	This Directive shall be referred to as the Prevention of Money Laundering and Terrorist Financing Directive of 2025.
Definitions	2.	(1) In this Directive, unless the text provides a different interpretation:
RAA 560/2014 O.G. Sch III(I), No 4838, 12.12.2014		' Bureaux de Change Businesses' shall have the meaning assigned to it in the Central Bank of Cyprus Directive on Bureaux de Change Businesses.
31(I)/2018 32(I)/2019 16(I)/2022 36(I)/2023 81(I)/2012 30(I)/2018		'agent' has the same meaning as that given to (a) the term 'agent of payment institutions' in Article 2 of the Provision and Use of Payment Services and Access to Payment Systems Laws of 2018 to 2023 and (b) the term 'e-money agent' in Article 2 of the Electronic Money Laws of 2012 to 2018;
		'senior executive management' means the persons responsible for the day-to-day management of the obliged entity, including the chief executive officer (CEO) and/or the executive members of the management body;
		'management body' means the board, committee, and/or body of an entity, which has the power to determine the strategy, objectives and overall direction of that entity and oversees and monitors the decision-making process with respect to management,

		including a person who effectively directs the business of that entity;
81(I)/2012 30(I)/2018		'distributor' means the person referred to in Article 19 of the Electronic Money Laws of 2012 and 2018;
		'risk appetite' means the aggregate level and types of risks that an obliged entity is willing to assume within its risk-taking capacity, in line with its business model, to achieve its strategic objectives;
		'National Risk Assessment' means the national assessment carried out by the Republic of Cyprus in accordance with Article 57(1)(b1) of the Law to identify, assess, understand and mitigate risks related to money laundering and terrorist financing;
72(I)/2016 67(I)/2020		'financial leasing companies' means undertakings authorised by the Central Bank of Cyprus on the basis of the provisions of the Leasing Laws of 2016 and 2020;
EBA/GL/2021/02 1/03/2021		'EBA Risk Factors Guidelines' means Joint Guidelines EBA/GL/2021/02 of 1 March 2021 pursuant to Article 17 and Article 18(4) of Directive (EU) 2015/849 on 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 that repeal and replace Joint Guidelines JC/2017/37, as amended from time to time;
EBA/GL/2022/05 14/6/2022		'EBA Guidelines on the role of the Compliance Officer' means Guidelines EBA/GL/2022/05 of 14 June 2022 on policies and procedures in relation to compliance management and the role and responsibilities of the AML/CFT compliance officer, in accordance with Article 8 and Chapter VI of Directive (EU) 2015/849, as amended from time to time;
EBA/GL/2022/15 22/11/2022		'EBA Guidelines on the use of remote customer onboarding solutions' means Guidelines EBA/GL/2022/15 of 22 November 2022 on the use of remote customer onboarding solutions in accordance with Article 13(1) of Directive (EU) 2015/849, as amended from time to time;
EBA/GL/2024/11 4/7/2022		'EBA Guidelines on travel rules under Article 36 of Regulation (EU) 2023/1113' means the Guidelines on information requirements in relation to transfers of funds and certain crypto-assets transfers under Regulation (EU) 2023/1113, as amended from time to time;
Official Journal of the EU: *L 203, 10.8.2018, p. 2–6*		'Delegated Regulation 2018/1108' means Commission Delegated Regulation 2018/1108 of 7 May 2018 supplementing Directive (EU) 2015/849 of the European Parliament and of the Council with regulatory technical standards on the criteria for the appointment of central contact points by electronic money issuers and payment service providers and with rules on their functions;
Official Journal of the EU: *L 125, 14.5.2019, p. 4–10*		'Delegated Regulation (EU) 2019/758' means Commission Delegated Regulation (EU) 2019/758 of 31 January 2019 supplementing Directive (EU) 2015/849 of the European Parliament and of the Council with regard to regulatory technical standards for the minimum action and the type of additional measures credit and financial institutions must take to mitigate the risk of money laundering and terrorist financing in certain third countries;
Official Journal of the EU: *L 150, 9.6.2023, p. 1–39*		'Regulation (EU) No 2023/1113' means Regulation (EU) No 2023/1113 of the European Parliament and of the Council of 31 May 2023 on information accompanying transfers of funds and certain crypto-assets and amending Directive (EU) 2015/849;
Official Journal of the EU: *L 150, 9.6.2023, p. 40–205*		'Regulation (EU) No 2023/1114' means Regulation (EU) No 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937;
Official		'Regulation (EU) No 910/2014' means Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive

Journal of the EU: *L 257, 28.8.2014, p. 73–114*		1999/93/EC;
Official Journal of the EU: *L 284, 12.11.2018, p. 9–21*		'Regulation (EU) 2018/1672' means Regulation (EU) 2018/1672 of the European Parliament and of the Council on controls of cash entering or leaving the Union. and repealing Regulation (EC) No 1889/2005;
Official Journal of the EU: L119 04.05.2016 pp. 1-88.		'Regulation (EU) 2016/679' means Regulation (EU) 2018/1672 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation);
		'risk' means the impact and likelihood of money laundering and terrorist financing taking place;
		"Anti-Money Laundering Compliance Officer" means the natural person defined in Article 69(a) of the Law;
188(I)/2007 58(I)/2010 80(I)/2012 192(I)/2012 101(I)/2013 184(I)/2014 18(I)/2016 CORRECTION OJ, Appendix I(I), No 4564 13(I)/2018 158(I)/2018 81(I)/2019 13(I)/2021 CORRECTION OJ, Appendix I(I), No 4816 22(I)/2021 61(I)/2021 CORRECTION OJ, Appendix I(I), No 4880, d.o.b. 18.3.2022 40(I)/2022 98(I)/2023 118(I)/2024 141(I)/2024		'Law' means the Prevention and Suppression of Money Laundering Activities Laws of 2007 to 2024;
63(I) of 2022		'Cash Control Act' means the Control of Cash entering or leaving the European Union and the Exercise of Intra-Community Controls on Cash Available Act;
		'Group of connected persons' means: (a) The members of a family, i.e. the spouse, children, and parent; (b) a natural person and a business entity in which the natural person and any member of his family is a partner or shareholder or director or beneficial owner or has in any other way control , or holds a substantial interest either on his own or together with other members of his family or together with other partners. Control of a company in this Article means the ability to exercise, directly or indirectly, significant influence and enforce relevant decisions within the company; (c) in the case of a customer that is a legal person, the parent company, any subsidiaries, co-dependent, affiliated companies or other entities which have a substantial interest in the legal person concerned; and (d) two or more persons, natural or legal who have economic dependency or are associated in such a way that may be considered to represent a single risk;
		'substantial interest' means the interest in any class of shares in the capital of a legal

		entity of 25% or more or an interest which enables a person to decide, by any means, to elect a majority of the directors of the legal entity or to exercise significant influence;
		'risk factors' means variables that, either on their own or in combination, may increase or decrease the risk of money laundering and terrorist financing arising from an individual business relationship or occasional transaction;
		''Non-face to face customers' means customers who enter into a transaction or business relationship without being physically present in the physical location of the obliged entity or of the person acting on behalf of the obliged entity, including where the customer's identity is verified via a video link or similar technological means;
		'Supranational Risk Assessment' means the European Commission's Supranational Risk Assessment published in accordance with Article 6(1) of Directive (EU) 2015/849;
		(2) (a) In this Directive, any reference to a legislative act of the European Union, such as a Directive, Regulation or Decision, means that act as corrected, amended or replaced from time to time, unless the text of this Directive gives a different meaning. (b) In this Directive, any reference to a law or regulatory administrative act of the Republic shall mean that law or regulatory administrative act as corrected, amended or replaced from time to time, unless the text of this Directive gives a different meaning. (3) Without prejudice to the above provisions, terms used in this Directive and not otherwise interpreted shall have the meaning assigned to them by the Law.
Scope of application	3.	(1) This Directive shall be applied by the following persons who, for the purposes of this Directive, shall be referred to as 'obliged entities':. (a) credit institutions, including branches of credit institutions authorised by a competent authority of a Member State, in relation to the activities specified in the Business of Credit Institutions Law; (b) electronic money institutions, including branches and agents of electronic money institutions authorised by a competent authority of a Member State and operating in accordance with the right of establishment, in relation to the activities specified in the Electronic Money Law of 2012, as amended from time to time, for which supervisory responsibilities have been conferred on the Central Bank; (c) payment institutions, including branches and agents of payment institutions authorised by a competent authority of a Member State and operating in accordance with the right of establishment, in relation to the activities specified in the Payment Services Law, as applicable, for which supervisory responsibilities have been conferred on the Central Bank of Cyprus; (d) bureaux de change businesses; (e) financial leasing companies; (f) credit servicers as defined in paragraph (a1) and (a2) of the definition of the term "financial institution" in Article 2 of the Law; and (g) persons supervised by the Central Bank of Cyprus in relation to the activities specified in the Central Bank of Cyprus Laws of 2002 to 2024 or in relation to activities specified in any other law for which the Central Bank of Cyprus exercises supervision.
Purpose of this Directive	4.	This Directive lays down the requirements relating to the establishment of appropriate policies, procedures and controls to be applied by all obliged entities supervised by the Central Bank of Cyprus in order to achieve the objectives of the Law and effectively address money laundering and terrorist financing risks.
		PART 2 PRINCIPLE OF PROPORTIONALITY
Proportionality	5.	(1) When applying the provisions of this Directive, obliged entities shall take into account the nature, scale and complexity of their activities and transactions. In addition, they shall take into account the degree of risk associated with such activities and transactions as regards possible attempts by their customers to commit offences relating to money laundering and terrorist financing. (2) For the purpose of applying the principle of proportionality as referred to in subparagraph (1), the following criteria shall be taken into account by the obliged entity: (a) its legal form; (b) whether or not it belongs to a group;

		(c) its business model, taking into account: (i) the geographical presence of the obliged entity and the size of its activities in each jurisdiction; (ii) the nature and complexity of its transactions; (iii) the type of customers and the complexity of the products and/or services offered; (iv) outsourced functions and distribution channels. (d) its organisational structure, (e) its ownership structure; (f) the size of the obliged entity, taking into account: (i) total assets, including subsidiaries; (ii) turnover; and (iii) the number of employees.
		PART 3 INTERNAL GOVERNANCE AND INTERNAL AUDIT PROCEDURES
General requirements	6.	(1) The management body, the senior executive management and, in the case of obliged entities with a physical presence in Cyprus, the director of the Cyprus branch, shall have the ultimate responsibility for ensuring that the obliged entity complies with the provisions of the Law, this Directive, the Directives and Circulars issued by the Central Bank of Cyprus, the provisions of Regulation (EU) 2023/1113 and the EBA Guidelines. They shall also ensure the introduction and implementation of adequate and effective internal control systems and procedures that reduce the risk of the obliged entity's products and services being used in relation to money laundering and terrorist financing. (2) Obliged entities' policies and procedures shall set out how the management body and senior executive management ensure the development and implementation of an appropriate internal control system to prevent money laundering and terrorist financing. (3) An effective internal governance and management oversight framework requires at least: • the allocation of clear roles and responsibilities; • segregation of duties; • appropriate systems, controls and procedures; • ongoing education. (4) The management body and senior executive leadership lead by example, clearly articulate the underlying values of corporate culture and compliance, ensuring that their behavior reflects the values they embrace.
Role and responsibilities of the management body	7.	The management body of the obliged entity shall: (a) set out, record and approve the general principles of the obliged entity to prevent money laundering and terrorist financing; (b) establish, approve and oversee the overall risk strategy to prevent money laundering and terrorist financing, including risk appetite, as well as the risk management framework; (c) collectively possess adequate knowledge, skills and experience to be able to understand the money laundering and terrorist financing risks related to the business model of the obliged entity, including the knowledge of the legal and regulatory framework relating to those risks; (d) appoint an Anti-Money Laundering Compliance Officer, in accordance with the requirements of Article 69 of the Law. The Anti-Money Laundering Compliance Officer of a branch of an obliged entity operating in Cyprus shall be appointed by the management body of the parent company; (e) oversee and monitor the implementation of the internal governance and internal control framework to ensure compliance with the requirements relating to the prevention of money laundering and terrorist financing; (f) for the purposes of complying with subparagraph 7(e) above, the management body shall: (i) receive regular, adequate and objective information from the Anti- Money Laundering Compliance Officer on the level of money laundering and terrorist financing risk to which the obliged entity is exposed through its operations/activities and/or business relationships;

		(ii) assess the annual Risk identification and Assessment Report of money laundering and terrorist financing risks prepared by the Anti-Money Laundering Compliance Officer and determine whether all necessary measures have been taken to manage and minimise them, in accordance with the risk appetite of the obliged entity; (iii) oversee and monitor the extent to which policies and procedures to prevent money laundering and terrorist financing are appropriate and effective in light of the money laundering and terrorist financing risks to which the obliged entity is exposed and take appropriate measures to ensure that remedial action is taken, where necessary; (iv) receive and assess the Anti Money Laundering Compliance Officer's Annual Report prepared in accordance with paragraph 17 of this Directive and ensure that all appropriate measures are taken in a timely and effective manner to correct any weaknesses and/or omissions identified therein; (v) receive and assess interim updates from the Anti Money Laundering Compliance Officer in relation to activities that expose the obliged entity to higher money laundering and terrorist financing risks; (vi) assess, at least once a year, the effective functioning of the department/unit/section responsible for the prevention of money laundering and terrorist financing, taking into account, inter alia, the conclusions and recommendations of supervisory reports, any internal and/or external audits on the prevention of money laundering and terrorist financing that may have been carried out, including with regard to the appropriateness of the human and technical resources allocated to the Anti-Money Laundering Compliance Officer; (g) receive adequate, regular and objective information from the Anti-Money Laundering Compliance Officer and the Internal Audit Function on the effectiveness of anti-money laundering and counter-terrorist financing measures and controls, as well as the findings and observations of external auditors, where these exist. Furthermore, is promptly informed of the findings, observations and any supervisory measures imposed by the Central Bank of Cyprus, as well as of any related communication with MOKAS. In addition, it shall ensure that timely corrective measures are taken to address any deficiencies identified by the above-mentioned persons; (h) appoint a member of the management body in accordance with the provisions of Article 58D of the Law, who is responsible for the implementation of the Law and the directives and/or circulars and/or regulations issued pursuant to it, including any relevant European Union acts. Where there is an Audit Committee of the management body, the management body appoints the Chairman of the Audit Committee who will be responsible for the implementation of the Law and the aforementioned acts. Otherwise, it shall appoint a non-executive member. In the case of branches operating in Cyprus, the person responsible for the application of the Law and the aforementioned acts shall be the Manager of the branch. It is understood that the management body, as a collegiate body, remains responsible in its entirety. The role and responsibilities of the above-mentioned member must be recorded and approved by the management body; (i) ensure that the member referred to in subparagraph (h): (i) possess sufficient knowledge, skills, and professional experience necessary to identify, assess and manage money laundering and terrorist financing risks to which the obliged entity is exposed, and to implement the relevant policies, procedures, and controls; (ii) fully understands the business model of the obliged entity and the sectors in which it operates, and the extent to which that business model exposes the obliged entity to money laundering and terrorist financing risks; and (iii) is informed in a timely manner of decisions that may affect the risks to which the obliged entity is exposed.
Role and responsibilities of the senior executive	8.	The senior executive management must: (a) implement the appropriate and effective organisational and operational structure necessary to comply with the strategy for preventing money laundering and terrorist financing adopted by the management body, ensuring that the Anti-Money Laundering Compliance Officer has the sufficient authority and appropriateness of the human and technical resources corresponding to his or her tasks, including the need to establish a dedicated unit/department/section to support him or her; (b) ensure the implementation of internal policies and procedures to prevent money

		laundering and terrorist financing; (c) take into account the interim reports, the Annual Report of the Anti-Money Laundering Compliance Officer, the Annual Risk Identification and Assessment Report and the Annual Risk Assessment Report on financial sanctions;
Other internal control and risk management measures and procedures	9.	(1) The staff and agents of the obliged entity are informed about the person appointed as Anti-Money Laundering Compliance Officer to whom they will report any information on transactions and activities which they consider or suspect to be related to money laundering or terrorist financing. (2) The obliged entity shall establish a clear and concise procedure, with a designated communication channel, clearly documented in the procedures and risk management manual, under which information on suspicious transactions or activities is transmitted directly and without delay to the Anti-Money Laundering Compliance Officer. (3) The obliged entity implements policies, procedures and appropriate measures to ensure that the risk of money laundering and terrorist financing is identified, assessed and managed in its day-to-day operations in relation to: (a) the development of new products, new services, new business practices, including new delivery channels; (b) the use of new or developing technologies for new or existing products; and (c) any changes in the obliged entity's business model (e.g. expansion into new markets, opening of branches/subsidiaries in new countries/regions, etc.). That risk assessment should take place prior to the launch of the new products, business practices, the use of new or developing technologies, or changes to the obliged entity's business model. (4) Where the obliged entity maintains branches or subsidiaries outside the Republic, it shall implement group-wide policies and procedures in accordance with the provisions of Part 14 of this Directive. (5) Obliged entities shall ensure an adequate level of data quality is maintained in the customers' files in the IT systems. In this regard, the obliged entity shall implement policies, controls, and procedures to ensure the quality, accuracy, validity, and integrity of the data. The roles and responsibilities for data quality must be clearly defined. (6) In accordance with the provisions of Article 58(k) of the Law, obliged entities shall apply clear procedures and standards when recruiting and assessing the integrity of employees, whether this concerns new recruitments or existing staff.
Obligations of the Internal Audit Function	10.	(1) The internal audit function of the obliged entity must: (a) inspect and assess, at least annually, the effectiveness and adequacy of the policy, procedures and controls applied by the obliged entity to prevent money laundering and terrorist financing; (b) assess the level of compliance of the obliged entity with the Law, this Directive and Regulation (EU) 2023/1113, periodically and depending on the risk incurred, by carrying out regular or special or extraordinary audits; (c) prepare an audit plan commensurate with the size, nature and complexity of the obliged entity's activities and risk profile; (d) submit to the management body, through the audit committee where it exists, a report on its findings and observations from the audits it has carried out, together with its recommendations to address any weaknesses. The above report shall be communicated to the senior executive management and the Anti-Money Laundering Compliance Officer; (e) monitor on a regular basis, through progress reports or other means, the implementation of its recommendations. (2) Taking into account the size and nature of the obliged entity's activities, the work of the internal audit function may be outsourced to a third party, provided that the provisions of the Central Bank of Cyprus's Directives on outsourcing arrangements are met, as appropriate, and that there is no prohibition on such outsourcing under any legislation or in another directive issued by the Central Bank of Cyprus.
Policies and procedures	11.	(1) The obliged entity shall establish, maintain, and effectively implement on a daily basis policies, procedures and controls that are commensurate with the money laundering and terrorist financing risks that the obliged entity has identified. (2) Subject to the provisions of Article 58C of the Law, the policies, procedures, and controls shall be recorded in a manual of procedures and risk management, which shall be communicated to all executives and competent staff responsible for their

		implementation. (3) Obliged entities shall clearly set out in a manual of procedures and risk management, at least the following: (a) The obliged entity's business-wide and individual risk assessment methodology as well as the obliged entity's risk appetite; (b) the obliged entity's customer acceptance policy; (c) the 'know your customer' (KYC) procedure and, where applicable, who is the beneficial owner for each type of customer and category of products and services, and who should be identified for the purposes of this Directive. In addition, obliged entities shall take into account the sectoral guidelines in Title II of the EBA Risk Factors Guidelines, which contain further details on the identification of customers and their beneficial owners; (d) what constitutes an occasional transaction in the context of their business and when a series of individual transactions constitutes a business relationship rather than an individual transaction, taking into account factors such as the frequency or regularity with which the customer returns for occasional transactions and the extent to which the relationship is expected to have, or appears to have, an element of duration; (e) the type and appropriate level of due diligence measures they apply when establishing business relationships or executing occasional transactions; (f) how they expect the identity of the customer and, where applicable, the beneficial owner to be verified and how they expect the nature and purpose of the business relationship to be established, including the documents and information necessary to establish the business relationship and execute transactions; (g) the level of monitoring to be applied depending on the circumstances; (h) how, and in which situations, weak forms of certification and verification of a customer's identity are compensated through enhanced monitoring; (i) the procedures and controls for detecting unusual and/or suspicious transactions and reporting them to the Anti-Money Laundering Compliance Officer and MOKAS; (j) the record keeping procedures ; (k) the procedures for complying with Regulation (EU) 2023/1113; (l) procedures for identifying emerging risks; (m)the protection of personal data, and (n) the exchange of information in the case of Groups. Provided that where, in accordance with the provisions of Regulation (EU) 2016/679, a Data Protection Officer is appointed, his/her timely, effective, and continuous involvement and assistance in any process relating to the processing and/or protection of personal data shall be ensured. (4) The obliged entity shall periodically assess the manual of procedures and revise it when deficiencies are identified or when there is a need to adapt the obliged entity's procedures to address the risk of money laundering and terrorist financing more effectively or when new risks arise. It should be noted that any updates to the manual should be approved by senior management.
Customer acceptance policy	12.	(1) Obliged entities shall develop and implement a clear policy and procedures for accepting new customers, fully in line with the provisions of the Law and the requirements of this Directive. (2) The customer acceptance policy shall be prepared after a thorough assessment of the risks faced by the obliged entity in relation to its customers and/or their transactions and/or the countries of origin or conduct of their business in accordance with Part 6 of this Directive. (3) The customer acceptance policy shall be prepared by the Anti-Money Laundering Compliance Officer and submitted through the senior executive management of the obliged entity to the management body for assessment and approval. Once approved by the management body, the policy shall be communicated to the staff of the obliged entity. It is understood that the Anti-Money Laundering Compliance Officer is responsible for submitting proposals for amending this policy, taking into account the risks that need to be addressed. (4) The customer acceptance policy shall specify at least: • the criteria for accepting new customers ; • types of customers who are not accepted to enter into business relationships;

EBA/GL/2023/04 31/03/2023		• the categories of customers considered to be high risk as well as the risk factors for the existence of potentially high risk; • the procedures, conditions, and circumstances under which the relationship with a customer is terminated. (5) When determining the obliged entity's risk appetite and customer acceptance policy, due consideration should be given to shell companies, complex business structures and risks that business relationships may accumulate, taking into account the various risk factors, and enhanced measures should be required to effectively monitor and mitigate those risks. (6) The customer categorisation should take into account factors such as the type and nature of the customer's business, the country of origin and/or residence, the anticipated amount and nature of the business transactions, as well as the expected source and origin of the money and other factors as appropriate. (7) Obliged entities should ensure that the implementation of their policies, procedures and controls does not result in the general refusal or termination of business relationships with entire categories of customers who, in their judgement, present a higher risk of money laundering and terrorist financing. In this context, they must assess each business relationship individually, document their decisions and consider alternative risk mitigation measures before proceeding with a refusal or termination. Such decisions shall be proportionate, justified and made available to supervisory authorities upon request. (8) For the purpose of complying with subparagraph (7) above, obliged entities are required to use EBA Guidelines EBA/GL/2023/04 on policies and controls to effectively manage money laundering and terrorist financing risks when providing access to financial services.
		PART 4 THE ROLE OF THE MEMBER OF THE MANAGEMENT BODY RESPONSIBLE FOR PREVENTING MONEY LAUNDERING AND TERRORIST FINANCING
Role and duties of the member of the management body	13.	(1) The member of the management body appointed by the management body as referred to in paragraph 7(h) above to be responsible for preventing money laundering and terrorist financing must: (a) have sufficient knowledge, skills, and professional experience in identifying, assessing, and managing money laundering and terrorist financing risks and in implementing the relevant policies, procedures and controls; (b) have a very good knowledge of the business model and the sectors in which the obliged entity operates and the degree of money laundering and terrorist financing risk to which the business model exposes the obliged entity; (c) commit sufficient time and have adequate resources for the effective performance of his tasks in relation to the prevention of money laundering and terrorist financing; (d) submit comprehensive reports on his tasks as referred to in this paragraph and regularly inform, where necessary and without undue delay, the management body. (2) Without prejudice to the overall and collective responsibility of the management body prior to the appointment of the member of the management body referred to in subparagraph (1), consideration shall be given to whether such appointment may give rise to a conflict of interest and appropriate measures shall be taken to avoid or minimise that possibility. (3) The member of the management body shall ensure that the entire management body and senior executive management are aware of the impact of money laundering and terrorist financing risks on their business-wide risk profile. (4) The responsibilities of the member of the management body, in particular with regard to the implementation of policies, controls, and procedures to mitigate and manage money laundering and terrorist financing risks, should include at least the following: (a) ensuring that policies, procedures and internal control measures to prevent money laundering and terrorist financing are appropriate and proportionate, taking into account the characteristics of the obliged entity itself as well as the money laundering and terrorist financing risks to which it is exposed; (b) supporting the management body in assessing the need for a dedicated unit/service to support the Anti-Money Laundering Compliance Officer in the performance of his/her duties in relation to anti-money laundering and countering

		the financing of terrorism requirements, taking into account the size and complexity of the obliged entity's operations and its exposure to money laundering and terrorist financing risks. The staff of this unit/service should posses the necessary expertise, skills, and knowledge to support the Anti-Money Laundering Compliance Officer, who should be involved in the recruitment process; (c) ensuring the submission of periodic reports to the management body regarding the activities carried out by the Anti-Money Laundering Compliance Officer, and the adequate and timely provision to the management body of information and data concerning money laundering and terrorist financing risks, as well as compliance with anti-money laundering and countering the financing of terrorism requirements, which are necessary to enable the management body to carry out the role and functions entrusted to it. Such information must also cover the obliged entity's obligations towards the Central Bank of Cyprus and MOKAS, without prejudice to the confidentiality of suspicious transaction reports, as well as any supervisory findings, measures or sanctions identified or imposed by the Central Bank of Cyprus; (d) informing the management body of any serious or significant issues and breaches related to the prevention of money laundering and terrorist financing and recommending actions to remedy them; (e) ensuring that the Anti-Money Laundering Compliance Officer: (i) has direct access to all information necessary to perform his tasks; (ii) has sufficient human and technical resources and tools to be able to adequately perform the tasks assigned to him; and (iii) is well informed about incidents and deficiencies related to the prevention of money laundering and terrorist financing identified by internal control systems as well as by the Central Bank of Cyprus and, in the case of groups, by foreign supervisory authorities. (5) The member of the management body shall be the main contact point for the Anti-Money Laundering Compliance Officer within the management of the obliged entity. Furthermore, that member of the management body should ensure that any concerns raised by the Anti-Money Laundering Compliance Officer regarding the prevention of money laundering and terrorist financing are appropriately addressed and, where this is not possible, are duly considered by the senior executive management. If the senior executive management decides not to follow the recommendations of the Anti-Money Laundering Compliance Officer, it must duly justify and document its decision in light of the risks and concerns raised by the Anti-Money Laundering Compliance Officer. In the case of a significant incident, the Anti-Money Laundering Compliance Officer must have direct access to the management body.
		PART 5 THE ROLE OF THE ANTI-MONEY LAUNDERING COMPLIANCE OFFICER
Appointment of the Anti-Money Laundering Compliance Officer	14.	(1) Obliged entities shall inform the Central Bank of Cyprus in writing of their intention to appoint an Anti-Money Laundering Compliance Officer in accordance with the requirements of Article 69 of the Law, at least two months before the completion of the procedure, submitting the following information: (a) its position/hierarchy and reporting lines in the organisational structure of the obliged entity, as well as its contact details; and (b) his curriculum vitae. (2) Within the two-month period referred to above, the Central Bank of Cyprus may request further information or clarifications. In such a case, the obliged entity shall not proceed with the appointment until the Central Bank of Cyprus has been satisfied with the above and informs the obliged entity in writing in this respect. (3) The Central Bank of Cyprus may object to the appointment, giving reasons for its decision, if it considers that the fitness and propriety criteria, as set out in Article 69(a) of the Law, for the fulfilment of its responsibilities, are not met. In such a case, the obliged entity shall not proceed with such an appointment. (4) The Anti-Money Laundering Compliance Officer shall be appointed by the management body of the obliged entity in accordance with the provisions of Article 69 of the Law. The Anti-Money Laundering Compliance Officer of a Cypriot branch of an entity from another country shall be appointed by the management body of that entity and shall report directly to the Manager of the Cypriot branch and to the Head Anti-Money Laundering Compliance Officer of the Group. (5) The Central Bank of Cyprus has the discretion to request the replacement of the Anti-Money Laundering Compliance Officer if it considers that the fitness and propriety

		criteria, as set out in Article 69(a) of the Law, are no longer met for the fulfilment of his responsibilities. (6) Obliged entities must communicate to their staff members, as well as to their agents or other persons acting on behalf of the obliged entity, the contact details of the Compliance Officer. (7) In the event of termination of the employment relationship or resignation of the Anti-Money Laundering Compliance Officer, the obliged entity must immediately inform the Central Bank of Cyprus in writing and initiate procedures for the appointment of a new Anti-Money Laundering Compliance Officer. (8) The Anti-Money Laundering Compliance Officer must be a member of the staff of the obliged entity, be established in the Republic, and act independently and autonomously in the performance of his/her duties. In addition, it should have sufficient authority to propose to the management body and senior executive management, on its own initiative, all necessary or appropriate measures to be taken to ensure the obliged entity's compliance with the legal and regulatory framework and the effective implementation of internal procedures and controls to prevent money laundering and terrorist financing. The Anti-Money Laundering Compliance Officer may be the same person as the head of the compliance function and may fall under the compliance unit, where such unit exists, or operate as an independent control function. It is understood that the Anti-Money Laundering Compliance Officer, regardless of whether he is part of the compliance function or a separate control function, he should submit reports and statements directly to the management body as provided for in this Directive. (9) Taking into account the principle of proportionality, in accordance with the criteria set out in Part 2 of this Directive, the management body should determine whether the Anti-Money Laundering Compliance Officer may have other tasks and/or responsibilities within the obliged entity, examine possible conflicts of interest and take the necessary measures to avoid or, where that is not possible, manage and minimise them. In this case, the Anti-Money Laundering Compliance Officer may not be the same person as the Data Protection Officer, as designated, in accordance with the provisions of Regulation (EU) 2016/679. The management body shall ensure that the Anti-Money Laundering Compliance Officer can have sufficient time to perform his/her duties as an Anti-Money Laundering Compliance Officer. (10) The Anti-Money Laundering Compliance Officer may act for two or more entities within the same group or be entrusted with other tasks, provided that the obliged entity ensures that such multiple appointments continue to enable him to carry out his tasks effectively. (11) Where necessary in view of the volume and/or geographical spread of the work, obliged entities may also appoint "Assistants anti-money laundering compliance officers" by division, geographical district or otherwise, for the purpose of assisting the Anti-Money Laundering Compliance Officer. It is understood that the Anti-Money Laundering Compliance Officer may delegate part of his/her tasks, as set out below, to staff members working under his/her direction and supervision, provided that the ultimate responsibility for the effective performance of these tasks remains with him/her. (12) Obliged entities that maintain branches or subsidiaries in the domestic market, or in another Member State or in a third country, shall appoint the Anti-Money Laundering Compliance Officer as a coordinator to ensure the implementation of the group's policy by all group companies engaged in financial activities. Furthermore, the Anti-Money Laundering Compliance Officer should ensure that adequate and appropriate systems and procedures are implemented for the effective prevention of money laundering and terrorist financing offences. (13) Obliged entities authorised by the Central Bank of Cyprus that provide services through agents and/or distributors shall appoint the Anti-Money Laundering Compliance Officer as coordinator to ensure, on behalf of the obliged entity, compliance of agents and/or distributors with the relevant requirements of the Law and this Directive and to facilitate supervision by the Central Bank of Cyprus. (14) The Anti-Money Laundering Compliance Officer forms part of the second line of defence, and as such, part of an independent function. The obliged entity must therefore ensure that the following conditions are met: a) the Anti-Money Laundering Compliance Officer must be independent of the business lines or units he controls and he can not be subordinate to a person who has responsibility for managing any of those business lines or units; b) the obliged entity has established internal procedures to ensure that the Anti-Money Laundering Compliance Officer has, at all times, unrestricted and direct

		access to all information necessary for the performance of his or her duties. In this context, the decision on the information to which he/she should have access is taken solely by the Anti-Money Laundering Compliance Officer himself/herself; c) in the case of a significant incident, the Anti-Money Laundering Compliance Officer must be able to report and have direct access to the management body. (15) In order to comply with Articles 58(k) and 69(a) of the Law and paragraph 9(6) of this Directive, obliged entities shall, before appointing the Anti-money Laundering Compliance Officer, assess whether he or she possesses: a) the reputation, honesty and integrity required to perform his or her duties; b) the appropriate skills and expertise to prevent money laundering and terrorist financing, including knowledge of the applicable legal and regulatory framework and the implementation of relevant controls, procedures, and policies to prevent money laundering and terrorist financing; c) adequate knowledge and understanding of the money laundering and terrorist financing risks associated with the business model of the obliged entity to perform his functions effectively; d) relevant experience regarding the identification, assessment and management of money laundering and terrorist financing risks; and e) sufficient time and seniority to perform his functions effectively, independently and autonomously. (16) For business continuity purposes, the obliged entity shall appoint an Alternate Anti-Money Laundering Compliance Officer with appropriate skills and expertise in anti-money laundering and countering the financing of terrorism, who shall replace the Anti-Money Laundering Compliance Officer in his or her absence for a certain period of time, or the integrity of the Anti-Money Laundering Compliance Officer is called into question. (17) Obliged entities shall immediately inform the Central Bank of Cyprus in writing of the appointment of the Alternate Anti-Money Laundering Compliance Officer by submitting his name, position and contact details and shall communicate to staff members, their agents or other persons acting on behalf of the obliged entity the contact details of the Alternate Anti-Money Laundering Compliance Officer.
Tasks of the Anti-Money Laundering Compliance Officer	15.	(1) The role and responsibilities of the Anti-Money Laundering Compliance Officer, the Alternate Anti-Money Laundering Compliance Officer and the Assistant anti-money laundering compliance officers must be clearly defined, recorded and documented in a relevant manual, which shall be reviewed periodically. (2) The Anti-Money Laundering Compliance Officer shall have at least the following tasks: (a) records and assesses, on an annual basis, the risks of money laundering and terrorist financing at the business-wide level and individual risk assessments, in accordance with the requirements of Part 6 of this Directive; (b) prepares, in accordance with the provisions of paragraph 23 of this Directive, the Annual Risk Identification and Assessment Report as well as any other reports relating to the outcomes of the risk assessment or any changes thereto. The Annual Risk Identification and Assessment Report, along with any other reports on the results of the risk assessment or any changes thereto, must be submitted to the management body with a copy to the member of the management body as specified in Part 4 of this Directive. It is noted that interim reports on new or changing risks to which the obliged entity is exposed through its operations/activities and/or business relationships should be submitted every three months or earlier if necessary. The Anti-Money Laundering Compliance Officer should propose to the management body specific measures to mitigate those risks; (c) submits a copy of the Annual Risk Identification and Assessment Report to the Central Bank of Cyprus, together with the Annual Report of the Anti-Money Laundering Compliance Officer as well as the Annual Risk Assessment Report on financial sanctions; (d) prepares and develops the customer acceptance policy referred to in paragraph 12 of this Directive and submit it to the management body through the senior executive management; (e) takes or recommends, as appropriate, measures to prevent money laundering and terrorist financing, taking into account the National and Supranational Risk Assessment Report;

		(f) ensures that appropriate policies and procedures are in place and effectively implemented. Therefore, the Anti-Money Laundering Compliance Officer must at least: (i) set out the policies and procedures to be established by the obliged entity as defined in paragraph 11 of this Directive, as well as the controls and systems to be implemented by the obliged entity, in accordance with the requirements of Article 58 of the Law; (ii) ensure that policies and procedures to prevent money laundering and terrorist financing are effectively implemented by the obliged entity, in accordance with the provisions of subparagraph (g) below; (iii) ensure that policies and procedures to prevent money laundering and terrorist financing are reviewed regularly and amended or updated where necessary; (iv) prepare proposals in cases of changes to the legal and/or regulatory framework and/or to the risks faced by the obliged entity and/or when deficiencies are identified and/or when there is a need to adjust the processes of the obliged entity in order to better address the weaknesses and/or deficiencies identified through monitoring or supervisory activities; (g) monitors and assesses the proper and effective implementation of the policy, procedures and controls by the business lines and departments/units (first line) of the obliged entity to prevent money laundering and terrorist financing, as well as at group level, where applicable. Therefore, the Anti-Money Laundering Compliance Officer shall: (i) implement appropriate monitoring mechanisms, including offsite monitoring and on-site visits to units/branches /business lines, agents and distributors where it receives the necessary information on the extent to which the obliged entity complies with the relevant legal and regulatory framework; (ii) record the results of the audits and, in the event deficiencies and/or weaknesses are identified in the implementation of the required procedures and controls , provide appropriate guidance for the adoption of corrective measures and apply mechanisms to monitor the implementation of those measures; (iii) inform the management body periodically of the results of those audits and the level of compliance of the obliged entity, as well as of any findings resulting from audits by the Central Bank of Cyprus as the competent supervisory authority, or the internal audit function, or an external auditor, and submit proposals to the management body to take corrective measures on those findings. The Anti-Money Laundering Compliance Officer of a branch shall inform the branch Manager and the Head Anti-Money Laundering Compliance Officer of the head office of the branch; (h) advises the management body on the measures to be taken to ensure compliance with applicable laws, regulations and standards, and submit his assessments of the possible impact that any changes to the legal or regulatory framework, activities and compliance framework of the obliged entity may have; (i) brings to the attention of the member of the management body responsible for preventing money laundering and terrorist financing: (i) the areas where the operation of anti-money laundering and countering the financing of terrorism controls needs to be implemented or improved; (ii) the appropriate improvements proposed in relation to subparagraph (i) above; (iii) a progress report on any significant remedial programmes, submitted at least once a year as part of the annual report referred to in paragraph 23 of this Directive, and, in addition, on an ad hoc basis or periodically, depending on the improvements, to provide information on the level of the obliged entity's exposure to money laundering and terrorist financing risks, and the measures taken or recommended to reduce and effectively manage those risks; (iv) the needs to reinforce the human and technical resources of its department/unit/service in case they are not sufficient. (j) subject to the provisions of Article 69 of the Law and Part 12 of this Directive, submits a suspicion report to MOKAS (hereinafter referred to as the "Suspicious Activity Report to MOKAS) as soon as possible through the secure communication channels specified by MOKAS. The Anti-Money Laundering Compliance Officer, in his role under this provision, must:

		(i) understand the functioning and design of transaction monitoring systems, including the scenarios defined and used in accordance with the money laundering and terrorist financing risks faced by the obliged entity, as well as the internal procedures for handling alerts generated by such systems; (ii) receive internal reports (hereinafter referred to as 'Internal Suspicion Reports') from employees, agents or distributors of the obliged entity, or reports otherwise generated by the obliged entity's systems, of knowledge or suspicion of money laundering and terrorist financing, or on the fact that a person may have been, be, or will be connected, to money laundering and terrorist financing; (iii) immediately assess and examine the information received pursuant to subparagraph (2)(j)(ii) above, with reference to available sources of information, and exchange information with other persons in compliance with the provisions of Articles 48 and 49 of the Law. The assessment of the information contained in the Internal Suspicion Reports submitted to the Anti-Money Laundering Compliance Officer must be made on a separate form (hereinafter referred to as the 'Internal Evaluation Suspicion Report') which is filed in a relevant file and kept in the safe custody of the Anti-Money Laundering Compliance Officer; (iv) establish, document and implement a prioritisation process for internal reporting received in order to prioritise internal reporting on particularly high-risk cases; (v) if he decides not to disclose the relevant information to MOKAS after carrying out the relevant evaluation described in subparagraph (2)(j)(iii) above, to fully explain and record the reasons for his decision in the 'Internal Evaluation Suspicion Report' form; (vi) ensure that knowledge or suspicion of money laundering and terrorist financing or of a person's connection to money laundering and terrorist financing is reported immediately to MOKAS, by submitting together with the Suspicious Activity Report to MOKAS all data, facts, information and documents necessary to substantiate the suspicion or cases of reasonable grounds for suspicion of money laundering and terrorist financing. Obliged entities must have a system in place that allows them to produce such suspicion reports in printed form for audit purposes; (vii) archive in relevant files under his custody, all internal suspicion reports and internal suspicion reports assessments that have been carried out, as well as the suspicion reports to MOKAS together with any related correspondence with MOKAS, in order to enhance the detection of future suspicious transactions; (viii) act as the first point of contact with MOKAS, both at the beginning and throughout the investigation of a case considered after the submission of the suspicion report to MOKAS and ensure a prompt and exhaustive response to any request for information made by MOKAS, providing MOKAS with all required information and documents; (ix) regularly examine the reasons why alerts of unusual activity or transactions were not submitted as internal reports, in order to determine whether there are weaknesses and/or deficiencies that need to be addressed so as to ensure the effective detection of suspicious activities or transactions; (x) keep statistics on internal suspicion reports and suspicion reports filed to MOKAS, with at least the following information: • district and branch/agent/distributor where the business relationship or customer accounts involved are maintained, or where the transaction took place; • the date of submission of the internal suspicion report; • the date of evaluation; and • the date of submission of the suspicion report to MOKAS. (k) monitor the transactional behaviour of the customer as well as of other persons for whom a suspicion report has been submitted to MOKAS; (l) ensure that the obliged entity's internal control systems enable him to comply with any instructions provided by MOKAS; (m) ensure that staff members assisting in the fulfilment of the obligation to submit suspicious reports to MOKAS have the necessary knowledge, skills and suitability to assist in this task. In addition, particular attention should be paid to

		sensitive and confidential information that may be disclosed as well as to cases where the obliged entity has an obligation not to disclose such information; (n) subject to the provisions of Articles 48 and 49 of the Law, the Anti-Money Laundering Compliance Officer must carefully consider to whom, within the obliged entity, information is provided regarding any reports submitted to MOKAS, as well as any requests for information received from MOKAS. The reporting procedure must be confidential and the identity of the persons involved in the preparation and transmission of the report must be protected by a confidentiality policy; (o) ensure that branches and subsidiaries in which the obliged entity has a majority ownership and which operate in third countries have taken all necessary measures to fully comply with the requirements of this Directive in relation to customer identification and due diligence procedures and record-keeping procedures; (p) subject to the provisions of Article 68A(3), ensure that, in cases where obliged entities maintain establishments in another Member State, such establishments comply with the relevant anti-money laundering and countering the financing of terrorism legislation of that Member State; (q) ensure that group-wide policies and procedures have been established for the purpose of complying with the requirements of the Law, policies and procedures for the exchange of information and the proper processing of personal data, within the group as required by the Law; (r) has the overall responsibility for the timely and correct submission to the Central Bank of Cyprus of the statements, information and reports submitted to the Central Bank of Cyprus. Furthermore, it evaluates the above-mentioned data and information submitted to the Central Bank of Cyprus and, where appropriate, investigates trends that may indicate risks of getting involved in transactions or activities related to money laundering or terrorist financing and proceeds promptly with the implementation of additional measures where necessary. The Anti-Money Laundering Compliance Officer responds promptly to any queries or clarifications requested by the Central Bank of Cyprus in relation to the information contained in the aforesaid statements and/or reports; (s) examine and approve foreign currency cash transactions imported from abroad, in accordance with the provisions of paragraph 55 of this Directive; (t) maintain records containing full details of the customers or groups of connected customers (name, address, account number(s), account holder(s)) for whom he has given his written approval to accept an occasional foreign currency cash transaction or series of foreign currency cash transactions on a continuous and regular basis, in accordance with paragraph 55 of this Directive. In this respect, the Anti-Money Laundering Compliance Officer must keep separate records for customers who have: (i) occasional cash transactions, and (ii) cash transactions on a continuous and regular basis; (u) maintains a register of all cases of persons (prospective customers) with whom the establishment of a business relationship was not allowed either due to risk avoidance or for reasons of non-compliance with the relevant legal and/or regulatory framework, subject to the provisions of Regulation (EU) 2016/679. The maintenance of this register is limited to cases of documented high risk or attempted circumvention of procedures, and the data are retained for a maximum period of twelve (12) months, unless a risk-based assessment justifies an extension of the retention period. The inclusion of a prospective customer's name in the register does not imply automatic rejection of a new application, and each request is re-evaluated based on updated information. (v) respond to all questions, requests for information and clarifications requested by the Central Bank of Cyprus, provide all requested information and data and cooperate fully with the Central Bank of Cyprus; (w) ensure that he and the Alternate Anti-Money Laundering Compliance Officer acquire the knowledge and skills required for his duties, in order to improve the procedures for the timely recognition, prevention and obstruction of any transactions and activities that may be aimed at money laundering and terrorist financing; (x) provide advice and guidance to the staff and to the agents/distributors of the obliged entity on matters related to the framework for the prevention of money laundering and countering the financing of terrorism and ensure that the provisions of Part 13 of this Directive on training are implemented;

		(y) verify that the third person on whom the obliged entity intends to rely for carrying out customer identification procedures and customer due diligence measures is an obliged person as defined in Article 67(2)(a) of the Law and give his written approval for such cooperation which should be duly justified and documented and kept in the third person's individual file; (z) assess the quality of customers recommended by third parties in accordance with the requirements of paragraph 29(6)(e) of this Directive; (aa) maintain records with the data/information of the third persons with whom the obliged entity has entered into cooperation, as referred to in paragraph 29(6)(g) of this Directive, in compliance with the provisions of Regulation (EU) 2016/679; (bb) maintain records with the data/information referred to in paragraph 29(6)(h) of this Directive regarding third persons with whom cooperation has been terminated or rejected, in compliance with the provisions of Regulation (EU) 2016/679; (cc) ensure that the obliged entity has in place policies, procedures and controls, as defined in Article 64(1)(b) of the Law as well as in paragraphs 48 and 49 of this Directive, in cases of cross-border correspondent relationships with institutions from other Member States or third countries; (dd) consult prior to the final decision by senior management regarding the acceptance or continuation of business relationships with high-risk customers as well regarding the reclassification of high-risk customers. (ee) ensure that the obliged entity is able to generate, at any time, customer lists by risk category, which include the names of customers and ultimate beneficial owners, the account number or customer number (if no accounts are maintained), the branch where the account is held and the date the business relationship was established. In the case of high-risk customers, the system must be able to generate lists based on the categories of customers defined in the Law, this Directive and as determined by the obliged entity itself (e.g. politically exposed persons, trusts, high-risk countries, etc.); (ff) ensure that the obliged entity is able to generate reports of occasional transactions per person from whom a transaction has been entered into, indicating the person's name, unique identification number, the branch where the transaction was conducted, the transaction date, and the classification assigned to the transaction based on the assessed risk; (gg) ensure that the obliged entity takes into account the public statements of the Financial Action Task Force ("FATF") disclosing the names of countries that have significant strategic weaknesses in the area of money laundering and terrorist financing and ensure that enhanced due diligence and monitoring of business relationships/transactions with those countries are implemented. Furthermore, he must ensure that enhanced due diligence measures are applied to business relationships and transactions with high-risk countries, as announced by the European Commission and/or classified as such by the obliged entity itself; (hh) prepare the following Annual Reports in accordance with the requirements of paragraphs 17 and 23 of this Directive and paragraph 14 of the Central Bank of Cyprus' Directive for Compliance with the Provisions of UN Security Council Resolutions and the Decisions/Regulations of the Council of the European Union: • Annual Report of the Compliance Officer, indicating his/her activities. • Annual Risk Identification and Assessment Report on the Prevention of Money Laundering and Terrorist Financing. • Annual Risk Assessment Report concerning financial sanctions.
Outsourcing of operational tasks of the Anti-Money Laundering Compliance Officer EBA/GL/2019/02 25/02/ 2019	16.	(1) Obliged entities shall apply, in relation to outsourcing policy and procedures, the EBA Guidelines on outsourcing arrangement and Part 4.2.6 of the EBA Guidelines on the role of the Compliance Officer (EBA/GL/2022/05). Where applicable, they apply the provisions of the Central Bank of Cyprus Directives on internal governance arrangements, including outsourcing arrangements. (2) Without prejudice to the requirements of subparagraph (1) above, obliged entities are required to inform the Central Bank of Cyprus in writing and in a timely manner before assigning operational tasks to the Anti-Money Laundering Compliance Officer within the group or to a service provider. (3) Obliged entities may not delegate the full role of the Anti-Money Laundering Compliance Officer to service providers.

Annual report of the Anti Money Laundering Compliance Officer	17.	(1) The Anti-Money Laundering Compliance Officer must prepare and submit the Annual Report within three months after the end of each calendar year (i.e. by 31 March at the latest) to the management body with a copy to the member of the management body responsible for the prevention money laundering and terrorist financing. In the case of an obliged entity operating in the Republic in the form of a branch, the Annual Report should be submitted to the Manager of the branch, the management body of the obliged entity, as well as to the Group's Anti-money laundering Compliance Officer. (2) The management body and the member of the management body responsible for the prevention of money laundering and terrorist financing shall evaluate the Annual Report and ensure that all appropriate measures are taken in a timely and effective manner to address any weaknesses and/or deficiencies identified in the Report. (3) A copy of the Annual Report submitted to the management body shall be forwarded simultaneously to the Central Bank of Cyprus. A copy of the approved minutes of the management body must be submitted to the Central Bank of Cyprus within one (1) month from the date of the meeting. It is understood that the minutes shall include any remarks/comments regarding the content and conclusions of the Report, the measures decided to be taken to address any weaknesses and/or deficiencies identified in the Annual Report, the timetable for their implementation, as well as any issues that have not been resolved. (4) The Annual Report shall be proportionate to the size and nature of the obliged entity's activities and shall cover issues related to the prevention of money laundering and terrorism financing during the year under review and shall contain, as a minimum, the following: (a) a general description of the obliged entity's business activities and business model during the last year, mentioning the products/services it offers, the countries where it operates, any changes to its operations and/or structure, or the introduction of new products, services, technological developments that affected the procedures and controls for money laundering procedures and controls; (b) a summary of the most significant measures taken and/or procedures introduced during the reporting year, including a brief description of any problems, deficiencies, and irregularities identified; (c) a summary of the main findings of the business-wide money laundering and terrorist financing risk assessment conducted during the reporting year; (d) a description of any changes made to the methodology used by the obliged entity to assess the risk profile of its business relationships, highlighting how such changes are aligned with the business-wide money laundering and terrorist financing risk assessment of the obliged entity; (e) a summary of the main findings of the financial sanctions risk assessment, including statistical data on frozen accounts (e.g. number of customers, number of accounts, countries subject to sanctions, total frozen amounts); (f) information on audits and inspections carried out by the Anti-money Laundering Compliance Officer, the Internal Audit function and the External Auditor indicating the number of audits carried out, the departments/agent /distributors audited and the main deficiencies and weaknesses identified in the policy and procedures implemented by the obliged entity to prevent money laundering and terrorist financing. In this regard, the report must highlight the seriousness of the omissions and weaknesses, the associated risks, as well as the actions and measures taken or to be taken to remedy the situation, as well as relevant timetables for their implementation; (g) information on audits or other supervisory activities carried out by the Central Bank of Cyprus or, where applicable, by the Single Supervisory Mechanism of the European Central Bank, indicating any deficiencies and weaknesses identified, the risks associated with those deficiencies and weaknesses and the actions and corrective measures taken or to be taken, indicating the stage of implementation of those actions, without prejudice to any other periodic reports that may be required in the case of supervisory activities or corrective actions; (h) a brief description of the automated/electronic IT systems applied by the obliged entity for the ongoing monitoring of business relationships and transactions, with a description of their main functions and how they operate (e.g. in real time or after the completion of the transaction). Furthermore, a brief description of any changes (e.g. scenarios, new systems, upgrades) made to the operation of these systems during the reporting year as well as a general assessment of the adequacy of the above-mentioned systems and scenarios;

		(i) statistical data and information on: (i) The customer base • the total number of active customers per type of customer (natural or legal persons); • the total number of customers per risk category; • the total number of new customers, per type of customer (natural and legal persons), • the number of customers per risk category pending their update and the percentage of all customers with overdue updates; • the number of dormant business relationships; • the number of persons who were prevented from entering into a business relationship for compliance purposes; and • the number of customers whose business relationship was terminated for compliance purposes. (ii) The electronic system • the number of alerts generated by the electronic system, • the number of alerts investigated; • the number of false positive alerts, and • the number of reports submitted to MOKAS as a result of these messages. (iii) Unusual or suspicious transactions • the total number of internal suspicion reports submitted by staff and agents/distributors, summarising data by district and branch/agent /distributor, • the total number of reports submitted to MOKAS, • the total number of cases investigated by the Anti-money Laundering Compliance Officer, for which no reports were submitted to MOKAS; • the number of accounts frozen following the issuance of a court order/ instructions by MOKAS in the context of the implementation of the Law; • the number of requests for information received from MOKAS; • the number of requests for information received from the Police and other competent authorities (e.g. Tax Department), and • the number of requests for information received from correspondent banks. For the above information (points (i), (ii) and (iii) provide the percentage change compared to the previous year. (iv) Transactions: 1. Credit institutions • Summary data on an annual basis of the total number of transactions and the total amount in cash, both in euro and in foreign currency, exceeding the threshold of EUR 10 000, as well as corresponding data for the previous year. The total number of transactions and the total amount of incoming and outgoing wire transfers for amounts in excess of EUR 500 000, as well as corresponding data for the previous year, as reported in the statements submitted monthly to the Central Bank of Cyprus, where applicable, by obliged entities. For the above data, comments, and observations shall be provided where significant variations are observed in relation to the corresponding data of the previous year. • Analysis of deposits and loans, based on the permanent residence of the beneficial owner. The above analysis takes into account the balances on deposits and loans as at 31 December of the reporting year.

		Any trends identified in the above data that may increase the risk of money laundering and terrorist financing shall be analysed. 2. Other financial institutions • Summary data on an annual basis, as reported in the reports submitted monthly to the Central Bank of Cyprus, where applicable, regarding: (aa) payment transactions/transfers of incoming and outgoing transfers carried out by payment service providers authorised to provide services 1-4, 6 and 7 both in euro and in foreign currency along with corresponding data from the previous year; (bb) the number of cards issued by payment service providers authorised to provide the service number 5, along with the corresponding data of the previous year; (cc) the number of electronic accounts (wallets) opened, the number of cards issued as well as electronic transactions carried out by electronic money issuers. (j) in relation to the suspicion reports submitted by the Anti-Money Laundering Compliance Officer to MOKAS during the reporting year, a summary of key reasons for the suspicions shall be recorded and presented along with information on the country of origin of the customer and the ultimate beneficial owner, the country of activity and any trends observed. (k) information on circulars and other communications with staff/agents/distributors on matters related to the prevention of money laundering and terrorist financing; (l) details of the obliged entity's branches/subsidiaries operating in third countries, as well as information on the measures taken to ensure that the obliged entity's branches/subsidiaries comply with the requirements of this Directive regarding procedures for the identification and assessment of money laundering and terrorist financing risks, customer identification and due diligence measures, the reporting of suspicious transactions, record-keeping procedures, internal controls and comments and information on the degree of their compliance with those requirements; (m) if the obliged entity in Cyprus is the parent entity of a group, data, and information as required under Part 14, paragraph 69(5) of this Directive; (n) a brief description of the training seminars attended by the Anti-money Laundering Compliance Officer, the Alternate anti-money Laundering Compliance Officer, members of the anti-money laundering department/unit/section (where applicable), staff and agents /distributors of the obliged entity during the year; (o) information on the training programme of the obliged entity for the following year; (p) results of the assessment of the adequacy and effectiveness of the training and education provided to the persons referred to in subparagraph (n) above (q) information on the organisational structure and staffing of the Anti-Money Laundering Compliance Officer's department/unit/section, any significant changes that occurred during the reporting year, and the rationale behind them; (r) a brief description of the human and technical resources allocated by the obliged entity to the Anti-Money Laundering Compliance Officer's department/unit/section, as well as recommendations for any additional needs in personnel or technical equipment aimed at strengthening the measures and procedures for the prevention of money laundering and terrorist financing. Where no such needs arise, confirmation to that effect shall be provided; (s) a copy of the register containing data and information on third persons who refer customers or potential customers to the obliged entity and with whom the obliged entity has established cooperation. As a minimum, the following shall be included: (i) For the third person: ➢ Name, ➢ Business address, ➢ professional sector of activity, ➢ supervisory authority, ➢ date of commencement of cooperation; ➢ date of last assessment, ➢ date of the next assessment.

		(ii) For customers recommended to the obliged entity by the third person: ➢ number of customers per year over the past three years, ➢ results of the evaluation of referred customers; ➢ number of customers for whom a report was submitted to MOKAS. (t) a copy of the register containing data and information on third persons who have been rejected by the Anti-Money Laundering Compliance Officer or who the cooperation has been terminated: (i) For the third person: ➢ Name, ➢ business address, ➢ professional sector of activity, ➢ supervisory authority, ➢ date of rejection (to be completed as appropriate), ➢ date of commencement of cooperation (to be completed as appropriate), ➢ date of termination of cooperation (to be completed as appropriate), and ➢ grounds for rejection or termination of co-operation (to be completed as appropriate). (ii) For customers recommended to the obliged entity by the third party (to be completed as appropriate): ➢ number of customers per year over the past three years, ➢ results of the evaluations of referred customers; ➢ number of customers for whom a report was submitted to MOKAS. (u) a copy of the register containing data and information on the agents and distributors with whom the obliged entity has entered into a business relationship, both in Cyprus and abroad, exercising the right of establishment and the freedom to provide services. The following information shall be provided for each agent and distributors: ➢ Name, ➢ address, ➢ date of commencement of business relationship; ➢ the latest assessment date, and ➢ the next assessment date. (v) information on the outsourcing of tasks in relation to the tasks of the Anti-money Laundering Compliance Officer, including a description of the supervision exercised by the obliged entity in relation to those tasks; (w) the programme of activities of the Anti-Money Laundering Compliance Officer for the following year; (x) an overall assessment of the effectiveness of the systems and controls, the adequacy of the monitoring tools used by the obliged entity, as well as areas that may constitute breaches of the legal and regulatory framework, outlining in order of priority, the corrective/preventive actions deemed necessary and the expected deadline for completion.
		PART 6 IDENTIFICATION, RISK ASSESSMENT AND APPLICATION OF APPROPRIATE MEASURES AND PROCEDURES BASED ON CALCULATED RISK (“RISK BASED APPROACH”)
General requirements	18.	(1) The obliged entity must ensure that it has a thorough understanding of the money laundering and terrorist financing risks to which it is exposed. (2) In order to comply with Article 58(d) of the Law, the obliged entity shall, at regular intervals, assess: (a) the risks to which it is exposed as a result of the nature and complexity of its business (the business-wide risk assessment); and (b) the risks it is exposed to as a result of entering into a business relationship or carrying out an occasional transaction (individual risk assessments).

		(3) To achieve the purposes of subparagraphs (1) and (2) above, the obliged entity shall take into account risk factors related to its customers, countries or geographic regions, products, services, transactions or service channels, as well as information recorded in the National Risk Assessment. (4) The obliged entity shall implement appropriate risk-based measures and procedures to focus its efforts on those areas where there is a greater need to address money laundering and terrorist financing risks. The calculated risk is managed and reduced according to the risk appetite. (5) When assessing the overall level of residual money laundering and terrorist financing risk associated with their business and individual business relationships and occasional transactions, obliged entities should consider both the level of inherent risk, and the quality of controls and other risk mitigating factors. (6) The obliged entity shall assess whether the residual risk is consistent with the risk appetite and consider whether to take that risk or avoid it. (7) Where the residual risk is inconsistent with the risk appetite, the obliged entity shall reassess its measures, controls, and procedures to mitigate that risk to further enhance their effectiveness and reduce the residual risk within acceptable parameters.
Risk identification and assessments	19.	(1) The Anti-Money Laundering Compliance Officer is responsible for identifying, recording and assessing all possible risks, with the full support of the senior executive management and the active cooperation of the other units of the obliged entity. (2) Obliged entities are required to assess and evaluate the risk they face in relation to their general business, as well as the risks arising from entering into a business relationship with customers or carrying out occasional transactions, for the potential use of their services for the purpose of money laundering and terrorist financing purposes. (3) Obliged entities are required to form a holistic view of the risk factors to which they are exposed. This includes identifying and assessing the money laundering and terrorist financing risks associated with the products and services they offer, the countries in which they operate, the customers they attract and the transactions or delivery channels they use to service their customers. (4) In this respect, obliged entities shall: (a) identify risk factors based on information received from a variety of internal and external sources, including the sources listed in subparagraphs (16) and (17) below; (b) take into account the risk factors as referred to in the 'EBA Risk Factors Guidelines'; (c) take into account additional, broader, contextual factors, such as outsourcing, sectoral risk or geographical risk, which may have an impact on their own risk profile. It is understood that the risk factors are not exhaustive and obliged entities are not expected to consider all risk factors in all cases. (5) Obliged entities should ensure that their business -wide money laundering and terrorist financing risk assessment is tailored to their business profile and takes into account the factors and risks specific to their business. Furthermore, obliged entities must ensure that a comprehensive assessment of the risks of money laundering and terrorist financing, related to the business they carry out in the Republic of Cyprus or through the freedom to provide services in another Member State, or in a third country through a network of agents, distributors, etc., is carried out. (6) Where the obliged entity is part of a group that prepares a group wide-risk assessment, the obliged entity is required to consider whether the group-wide risk assessment is sufficiently detailed and specific to reflect the obliged entity's business and the risks to which it is exposed as a result of the group's links with countries and geographical areas and, if necessary, to carry out a supplementary group-wide risk assessment. (7) If the group is headquartered in a country associated with a high level of corruption, the obliged entity should reflect this specificity in its own risk assessment, even if the group-wide risk assessment does not mention anything specific in this regard. (8) Obliged entities are required to use the findings from their business-wide risk assessment and adapt their anti-money laundering and terrorist financing policies, controls and procedures accordingly, as provided for in Article 58 of the Law. In addition, obliged entities are required to ensure that the business-wide risk

		assessment reflects the measures taken to assess the money laundering and terrorist financing risk associated with the individual business relationships or occasional transactions, as well as the risk appetite of each obliged entity. (9) For the purposes of complying with subparagraph (8) above and taking into account the requirements of subparagraphs (11) and (12) below, obliged entities shall use the business-wide risk assessment to assist in determining the level of initial customer due diligence measures to be applied in specific situations as well as to particular types of customers, products, services and service channels. (10) Individual risk assessments should contribute to, but not replace, the business-wide risk assessment. (11) Obliged entities should identify the risks of money laundering and terrorist financing that they are, or could be, exposed to as a result of establishing or maintaining a business relationship or carrying out an occasional transaction. (12) When identifying money laundering and terrorist financing risks associated with a business relationship or occasional transaction, obliged entities should consider the relevant risk factors, including the identity of their customer, the countries or geographical areas in which they operate, the specific products and services and transactions required by the customer, as well as the channels used by the obliged entity to provide those products, services and transactions, taking into account the non-exhaustive list of factors referred to in Annexes II and III to the Law and the EBA Risk Factors Guidelines. (13) Obliged entities should collect sufficient information to identify, to the greatest extent possible, all relevant risk factors before entering into a business relationship with a customer and throughout that relationship or before carrying out an occasional transaction. Where necessary, obliged entities are required to apply additional due diligence measures and assess the relevant risk factors to form a holistic view of the risk associated with a specific business relationship or occasional transaction. (14) Information on money laundering and terrorist financing risk factors should come from a wide range of sources, accessed either individually or through commercially available tools or databases that gather information from different sources. (15) Obliged entities should determine the type and number of sources on a risk-sensitive basis, taking into account the nature and complexity of their activities. Obliged entities should not normally rely on a single source to identify money laundering and terrorist financing risks. (16) Obliged entities should always consider the following sources of information: (a) the European Commission's Supranational Risk Assessment; (b) information from governments, such as national risk assessments, policy statements and alerts, as well as explanatory memorandums for the respective legislation; (c) information from regulatory authorities, such as circulars, guidelines, instructions and the reasoning given when administrative measures are imposed; (d) information from MOKAS and the Police, such as threat reports, warnings and typologies; (e) the information obtained as part of the process for identifying the customer and establishing his financial and risk profile, prior to the commencement of the business relationship as well as continuous monitoring; (f) the European Commission's list of high-risk third countries. (17) Other sources of information that obliged entities may consider in this context are: (a) the knowledge and professional know-how of the obliged entity; (b) information from industryprofessional associations, such as typologies and information on emerging risks; (c) information from civil society, such as corruption indicators and country reports; (d) information from international standard-setting bodies, such as mutual evaluation reports or legally non-binding blacklists, including those set out in paragraphs 2.11 to 2.15 of the EBA Risk Factors Guidelines; (e) information from creditble and reliable open sources, such as reports in reputable newspapers; (f) information from credible and reliable commercial organisations, such as risk and intelligence reports; and (g) information from statistical organizations and academia.

		(18) Obliged entities should use the risk factors they have identified to assess the overall level of money laundering and terrorist financing risk. (19) Obliged entities should form a holistic view of the money laundering and terrorist financing risk factors they have identified that, taken together, will determine the level of money laundering and terrorist financing risk associated with a business relationship or an occasional transaction, or with their business activities. (20) Unless specified in the Law or in this Directive, the existence of isolated risk factors does not necessarily imply the categorisation of a customer relationship as high or low risk. (21) When assessing the risk of money laundering and terrorist financing, obliged entities may weigh the risk factors differently depending on their relative importance. (22) When weighting risk factors, obliged entities should document their decision regarding the significance of various risk factors within the context of a business relationship or occasional transaction or within the context of their business activities. (23) As the weighting coefficient given to each of the risk factors is likely to vary, both between products and between customers (or categories of customers) and between obliged entities, when weighting the risk factors, obliged entities should ensure that: (a) the risk weighting is not unduly influenced by a single factor; (b) the risk rating is not influenced by economic or speculative considerations; (c) the risk weighting does not lead to a situation where no business relationship qualifies as high risk; (d) the provisions of the Law and of this Directive relating to situations which always present a high risk of money laundering cannot be circumvented by the weighting of the obliged entity; and (e) they are able to override any risk score generated automatically when deemed necessary. The rationale for the decision to override such scores should be properly documented. (24) Where an obliged entity uses automated IT systems to obtain an overall risk score in order to categorise business relationships or occasional transactions, and does not develop those systems internally but purchases them from an external provider, the obliged entity shall ensure that they meet the requirements of Regulation (EU) 2016/679, and understand how the system works and how the system combines risk factors to form the overall risk score. The obliged entity must ensure that the scores allocated reflect the awareness of the money laundering and terrorist financing risk of the obliged entity itself and should also be able to demonstrate this awareness to the Central Bank of Cyprus. (25) Insufficient data quality, correctness and completeness of data may lead to incorrect alert messages, management reports and decisions. For this reason, obliged entities shall evaluate the data on an ongoing basis and take measures to optimise the quality, correctness and completeness of the data held in their computer systems and databases. (26) Obliged entities should decide on the most appropriate way to classify their customers into different risk categories. That decision shall take into account, inter alia, the nature, type, and size of the obliged entity's business and the types of risk to which it is exposed. Although obliged entities often categorise risk as high, medium, and low, it is possible to classify it in other categories. (27) Following the risk assessment, and after the obliged entity has taken into account the inherent risks as well as any risk management/mitigation measures, it should categorise its business lines as well as its business relationships and occasional transactions according to the estimated level of money laundering and terrorist financing risk. (28) These categories will be based on criteria that reflect the possible causes of risk and each category will be accompanied by corresponding due diligence, periodic monitoring and control measures.
Planning and implementation of controls to manage and reduce risks	20.	(1) When an obliged entity identifies the risks it faces, it should design and implement appropriate policies, procedures, systems and controls to manage and mitigate them, in accordance with the procedures provided for in this Directive. (2) Obliged entities should ensure that their policies and procedures to prevent money laundering and terrorist financing are based on and reflect their risk assessments.

		(3) In order to properly manage and minimise the risks associated with money laundering and terrorist financing, the obliged entity shall establish measures and procedures, including for the identification of customers and ultimate beneficial owners, the collection of information to establish their economic and risk profile, and the continuous monitoring of their transactions and activities. (4) Obliged entities should apply the due diligence measures provided for in Article 61 of the Law, and taking into account the assessed risk, should determine the type and extent of measures they should take to manage and minimise risks. These measures include, but are not limited to: (a) adjusting customer identification and due diligence measures according to the estimated risk of money laundering and terrorist financing; (b) application of minimum standards for the quality and extent of the identity data required for each customer category (indicatively: documents from independent and reliable sources, information from third parties and evidence); (c) requiring customers to provide additional data and information, where necessary for a proper and comprehensive understanding of their activities and sources of income and assets, so as to effectively address any increased risks arising from a specific business relationship or occasional transaction; and (d) monitoring on a continuous basis of customers' transactions, activities and relationships, on the basis of assessed risk. (5) The decision on the due diligence measures to be applied by the obliged entity should take into account, in addition to the requirements of this Directive, the EBA Risk Factors Guidelines.
		(6) Subject to the provisions of Article 63 of the Law, obliged entities may not apply simplified customer due diligence measures where there are indications of attempted money laundering or terrorist financing or where the obliged entity has doubts as to the accuracy of the information received. Furthermore, simplified due diligence measures cannot be applied in cases where there is an obligation to apply enhanced due diligence measures.
		(7) Subject to the provisions of Article 64 of the Law and paragraphs 42 to 51 of this Directive, obliged entities must apply enhanced customer due diligence measures. The category of high-risk customers must include business relationships identified as high-risk under Articles 64(1)(a), (b) and (c) of the Law and paragraphs 42 – 51 of this Directive, as well as any other business relationship that the obliged entity itself has decided to classify as such, pursuant to Article 64(3) of the Law.
Monitoring and improving the functioning of internal procedures	21.	(1) Obliged entities are required to assess, on a regular basis, the effectiveness of their internal policies, procedures, systems and controls, they apply for the purposes of preventing money laundering and terrorist financing, and to determine the frequency and intensity of these assessments, taking into account the level of risk to which they are exposed. (2) In this context, obliged entities shall apply: (a) appropriate procedures for the early detection of changes in the economic and risk profile of their customers; (b) procedures for identifying and assessing the risk of money laundering and terrorist financing that may arise in relation to the development of new products and services, new business practices, including new delivery channels, as wll as the use of new or developing technologies for new or existing products; (c) procedures for assessing the adequacy of the education and training provided to staff and agents/distributors; (d) control mechanisms and assessing the level of compliance (e.g. compliance unit, internal audit function); (e) appropriate automated systems and non-automated controls; (f) appropriate management information systems; (g) procedures for reporting by competent officers to the management body and senior executive management; (h) mechanisms for effective communication with the Central Bank of Cyprus and MOKAS.
Dynamic risk management	22.	(1) The risk management process must be ongoing and carried out on a dynamic basis. Obliged entities must have systems and controls in place to review their assessments regarding the money laundering and terrorist financing risk associated

		with their activities, as well as their individual business relationships, ensuring that their assessments remain up-to-date and relevant. (2) Systems and controls must be subject to regular review to continuously and effectively address risks arising from changes in the characteristics of existing customers, new customers, products and services and geographical dispersion. (3) Obliged entities shall assess the information received as part of the ongoing monitoring of a business relationship and consider whether this affects the risk assessment in order to identify changes in the activities of their customers. (4) Obliged entities must ensure that they have systems, procedures and controls in place to identify emerging money laundering and terrorist financing risks and to be able to assess those risks and, where appropriate, promptly integrate them both in their individual risk assessments and in their business-wide risk assessment. (5) For the purposes of subparagraph (4) above, the systems to be in place and the controls and procedures to be applied by obliged entities must include, inter alia, the following: (a) procedures to ensure that internal information, such as information obtained as part of the ongoing monitoring of business relationships is reviewed on a regular basis to identify any trends and emerging risks in relation to both the individual business relationships and the activities of the obliged entity; (b) procedures to ensure regular review of information sources as defined in paragraphs 19(16) and 19(17) of this Directive. These procedures shall include, in particular, the following elements: (i) regarding individual risk assessments: 1) warnings of terrorist attacks and decisions imposing a financial sanctions regime, or changes related to such measures, once adopted or notified, and taking the necessary measures to ensure their implementation; and 2) media references relating to the sectors or jurisdictions in which the obliged entity operates. (ii) regarding the business-wide risk assessment: 1) alerts and reports from law enforcement authorities (for example: police authorities); 2) thematic reviews and similar publications issued by competent authorities; 3) procedures for understanding and reviewing information regarding the risks, in particular those related to new customer categories, countries or geographical areas, new products, new services, new delivery channels and new compliance systems and controls. (c) cooperation with other industry representatives and competent authorities (e.g. tour de table, conferences and seminars) and procedures to inform relevant staff of any findings. (6) Obliged entities shall have at least the following systems, procedures and controls in place to ensure that business-wide risk assessment and individual risk assessments are up to date: (a) determination of a date of each calendar year when the next update of the business-wide risk assessment of the obliged entity will take place, as well as setting a date, depending on risk level, to update individual risk assessments ensuring that new or emerging risks are incorporated into the risk assessments; (b) where new risks are identified before the date set out in point (a) above, or where an increase in existing risk is observed, this shall be taken into account in the risk assessments as soon as possible; (c) recording, on a continuous basis, cases that could have an impact on risk assessments, such as internal suspicious transaction reports, non-compliance cases and information from customer service staff and agents/distributors, requests for information from the Central Bank of Cyprus and other competent authorities; (d) where the obliged entity introduces new products, services or business practices or significantly changes them, including the introduction of a new channel for the provision of products or services or the adoption of innovative technology within the systems and control mechanisms to prevent money laundering and terrorist financing, it must assess its exposure to money laundering and terrorist financing risk prior to the introduction of those products, services or business practices. Where those products, services or business practices have a significant impact on the obliged entity's exposure to money laundering and terrorist financing risk,

		the obliged entity must reflect that assessment in its own business-wide risk assessment and corresponding policies and procedures. (7) Like the initial risk assessments, any update of a risk assessment and adjustment of accompanying due diligence measures must be proportionate and commensurate with the risk of money laundering and terrorist financing.
Risk Identification and Assessment Report	23.	(1) Subject to the provisions of Article 58A(2) of the Law, obliged entities must keep records and document their overall risk assessment identified from their activities, their business relationships and individual transactions carried out, as well as the methodology they follow to assess and evaluate these risks. Furthermore, they shall record any changes in the relevant risk assessments made in the context of their review and monitoring and ensure that they are able to demonstrate to the Central Bank of Cyprus the accuracy of those risk assessments and the adequacy of the related risk management measures. All the above are documented in the Risk Identification and Assessment Report, which includes the detailed recording, evaluation and monitoring of the relevant risks and their management measures. (2) Obliged entities, by detailing the measures they have taken, should be able to present: (a) the methodology they use to identify and assess risks; (b) how they have resulted in the introduction and implementation of specific policies, procedures, and controls to manage and reduce risks; (c) how to monitor and improve, where necessary, specific policies, procedures, and controls; and (d) the arrangements for reporting to the management body in relation to the operation of the control procedures. (3) The Risk Identification and Assessment Report must be kept fully up-to-date. It is therefore necessary to reassess the risks, on an annual basis, even where obliged entities consider that there is no need to revise the relevant assessment report. (4) The Anti-Money Laundering Compliance Officer shall prepare and submit the above-mentioned annual report within three (3) months of the end of each calendar year, i.e. no later than 31 March, to the management body of the obliged entity, with a copy to the member of the management body responsible for preventing money laundering and terrorist financing, so that the members of the management body are adequately informed, understand and obtain understanding of the risk to which the obliged entity is exposed. (5) A copy of the above-mentioned report shall be submitted simultaneously to the Central Bank of Cyprus. In addition, copies of the minutes of the meeting of the management body, recording, inter alia, the views and decisions of the management body in relation to the report, as well as the risk acceptance statement, should be submitted to the Central Bank of Cyprus within one month from the date of the relevant meeting. (6) Provided that in addition to the above-mentioned annual information to the management body on the risks faced by the obliged entity, the Anti-Money Laundering Compliance Officer must inform the management body of any diversification of these risks during each year. The obliged entity must send the relevant minutes of the meeting of the management body where the update was discussed to the Central Bank of Cyprus.
		PART 7 CUSTOMER IDENTIFICATION PROCEDURES AND DUE DILIGENCE MEASURES
Identification and due diligence procedures	24.	(1) Obliged entities shall implement identification procedures and take due diligence measures: (a) when the conditions of Article 60 of the Law are met; (b) where the conditions laid down in Articles 5(3)(a) and 7(4)(a) of Regulation (EU) 2023/1113 are met; (c) when entering into an agreement with an agent/distributor; (d) for any third party who intends to act on behalf of a customer in accordance with Article 61(1) of the Law; and (e) for each transaction to buy or sell foreign exchange for amounts equal to or greater than the equivalent of one thousand euros (€1,000) per transaction, in accordance with Article 11 of the Central Bank of Cyprus Directive on Bureaux de Change Businesses of 2014 (Regulatory Administrative Act 560/2014).

		(2) The risk assessment carried out by an obliged entity must determine the actions to be taken in relation to risk management in the context of preventing money laundering and terrorist financing, both at the time of accepting a new customer and throughout the duration of their business relationship. (3) Obliged entities are required to collect and maintain sufficient data and information regarding a customer for the purpose of identifying their identity, establishing its economic and risk profile, which will serve as the basis of all other anti-money laundering and countering the financing of terrorism procedures, including the ability to detect and identify suspicious transactions/activities.
Demonstrate due diligence and update the identity of existing customers	25.	(1) Subject to the provisions of Articles 61(d) and 62(6) of the Law, obliged entities must ensure that the identity information they maintain about their customers, as well as the information comprising their economic and risk profile, remains fully up-to-date throughout the duration of the business relationship. (2) In this regard, obliged entities are required to examine and verify on a regular basis the validity and adequacy of the identity information, economic and risk profile of their customers, as well as other information held regarding their customers, in order to be able to identify whether the risk associated with the business relationship has changed. (3) The anti-money laundering and countering the financing of terrorism policy and procedures must set out the timeframe within which regular review, verification and updating of customer identity data and other data and information shall take place, depending on the risk category of the customer.
		(4) Notwithstanding the provisions of subparagraph (3) above, and taking into account the level of risk, if it is perceived at any time during the business relationship that reliable or sufficient data and information is missing from the identity and financial profile of an existing customer, then the obliged entity must immediately take all necessary steps, applying the identification procedures and due diligence measures provided for in this Directive, in order to collect the missing data and information as soon as possible. (5) In order to comply with the requirements of Article 62(6) of the Law, obliged entities must check whether they keep up-to-date data and information on the customer and that the risk associated with the business relationship remains the same çwhenever one of the following events or incidents occurs: (a) A transaction is carried out which appears to be unusual and/or significant compared to the customer's usual type of transactions, business activity and economic profile. (b) a significant change in the status and/or legal status of the customer such as: (i) change of directors/secretary; (ii) change of registered shareholders and/or beneficial owners; (iii) change of registered office; (iv) change of trustor, trustees, protectors, beneficiaries; (v) change of company name and/or trade name; (vi) change of main business partners; (vii) undertaking new significant business activities; (viii) change of business activities; (ix) expansion of activities to other countries. (c) a significant change in the functioning of the business relationship and accounts, such as: (i) a change in the persons authorised to handle the accounts; (ii) request to open new accounts or provide new services and/or products; (iii) activation of a dormant account or business relationship. (d) a change in the customer's risk level (e.g. a client from a lower risk level is classified to a higher risk). (e) identification of negative customer information in the press or on the internet or in commercial databases or information obtained from a competent supervisory authority or MOKAS or another institution or due to an investigation, indicating the need to update the customer and/or a possible change in the risk profile of the customer. It is understood that obliged entities must check the validity and reliability of the information, in particular that found in the press or on the internet or on commercial information bases. When conducting this verification, obliged entities must take

		into account the independence of the source as well as the cross-checking of the information through its reappearance in several independent sources. (6) It is understood that in the above cases, obliged entities may not need to apply all due diligence measures. Obliged entities must, however, determine which due diligence measures apply and the extent to which shall apply those measures. For example, in low-risk situations, obliged entities may be able to use the information obtained during the business relationship to update customer's information already held. (7) The results of the process of updating customer data/information must be recorded in a separate note, which is recorded in the file kept for each customer.
Creation of an economic profile and customer identification	26.	(1) Obliged entities must be satisfied that they are dealing with a real legal or natural person and, for that purpose, must obtain sufficient evidence of the identity of that person. (2) The identity of all customers must be ascertained and verified on the basis of reliable data, documents and information issued or obtained from independent reliable sources, that is, those data, documents and information which are difficult to falsify or obtain in an unlawful manner. (3) Evidence of identification must always be retained by the obliged entities and filed in customer records. (4) Since no specific element of customer identification can guarantee the correctness of a person's identity, obliged entities are required to apply customer identification procedures on an ongoing basis. (5) In order to ensure the validity and accuracy of the customer's and beneficial owner's identity data and for the purposes of complying with the provisions of Article 62 of the Law, obliged entities must use, as an additional measure to verify such data, the information held in the central beneficial ownership registers, as provided for in Articles 61A, 61B and 61C of the Law. It is provided that, obliged entities may need to take additional measures to verify and certify the identity of the beneficial owner, in particular in the event of an increase in the risk of the business relationship or where the obliged entity doubts that the person listed in the above registers is the ultimate beneficial owner, and where it is necessary to submit a suspicion report to MOKAS. (6) The residential address is considered a key element of identification of a person and therefore a separate procedure must be followed to verify the customer's address, in accordance with the requirements of paragraph 30(6). (7) Obliged entities must also identify and verify the identity of the beneficial owners/beneficiaries of the accounts and individual transactions and, for legal persons, must obtain sufficient information, data and documents issued by independent and reliable sources to understand the ownership and control structure of the customer's assets. (8) The measures taken by obliged entities to understand the ownership and control structure of the customer must be sufficient for the entity to be reasonably satisfied that it understands the risk associated with the different levels of ownership and control. In particular, obliged entities must ensure that: (a) the ownership and control structure of the customer is not unnecessarily complex or opaque; or (b) complex or opaque ownership and control structures are justified by an obvious economic or clear legitimate reason. (9) In the case of customers with complex or multi-layered ownership structures, enhanced due diligence measures regarding customer identification may be appropriate. The use of complex or multi-layered structures, with no apparent legitimate commercial or economic purpose, may give rise to suspicion and indicate a potentially increased risk of money laundering or terrorist financing. Obliged entities must therefore report to MOKAS whether the ownership and control structure of the customer raises suspicions and have reasonable grounds to suspect that the funds may constitute money laundering or terrorist financing. (10) Regardless of the type of customer, obliged entities must request and ensure that they receive adequate data and information, proportionate to the risk associated with the business relationship, on customer's business activities and the expected type and amount of its transactions. The obliged entity needs to understand the purpose and intended nature of the business relationship and the expected use of its products and services in order to be able to assess whether that proposed relationship is in line with the risk appetite and to provide a substantive basis for ongoing monitoring.

		(11) The data and information must be collected prior to the establishment of the business relationship and prior to the execution of any transactions, for the purpose of establishing the client's economic and risk profile and, as a minimum, must include the following: (a) the purpose and reason for which the potential customer requests to enter into a business relationship and use of products and/or services; (b) the anticipated use of the products and services, including the estimated volume of account or activity; (c) the nature of transactions; (d) the expected source (e.g. countries and names of main partners) and the expected amount of incoming transfers to be credited to the customer; (e) the expected destination (e.g. countries and names of main partners) and the expected amount of outward transfers/payments; (f) a clear and detailed description of the main business/professional activities/operations; (g) the ownership structure (where applicable), information on the group to which the entity belongs (e.g. company) such as country of incorporation of parent, subsidiary and affiliated companies, main activities, financial figures, etc.; and (h) whether the customer has other business relationships with other parts of the obliged entity or with its broader group, and whether this affects the obliged entity's understanding of the customer. (12) All data and information composing the client's economic profile must be recorded in a separate form which is archived in the client's file, together with all other documents and account opening details, as well as internal notes from minutes of meetings with the client in accordance with paragraph 29 of this Directive or whenever deemed appropriate. This form is updated on a regular basis or whenever new information arises regarding any changes and/or additions to the data that make up the customer's economic profile. (13) In order to better understand the activities of their customers (including companies, cooperatives, foundations, associations, trusts and other legal entities, self-employed natural persons, etc.), obliged entities must obtain copies of recent audited financial statements. In cases where there is no legal obligation to prepare audited financial statements or where there are no recent audited financial statements (at least for the previous two years), obliged entities to obtain recent management accounts.
Remote customers	27.	(1) Where a business relationship is initiated or an individual transaction is carried out remotely (without the physical presence of the parties), obliged entities must pursuant to Guidelines (EBA/GL/2022/15) on the use of remote customer identification solutions: (α) take satisfactory steps to satisfy themselves that the customer is indeed the person they claim to be; (β) assess whether that remote business relationship or individual transaction creates an increased risk of money laundering and terrorist financing and, if so, adapt the due diligence measures accordingly, taking into account the relevant risk factors. (2) Where the risk from such a business relationship or individual transaction is high, obliged entities must apply enhanced due diligence measures in accordance with paragraph 42 of this Directive. In particular, obliged entities must consider whether enhanced customer identification measures or enhanced ongoing monitoring of the business relationship are appropriate. (3) Obliged entities are required to apply the provisions of this Directive and comply with the requirements of the 'EBA Guidelines on the use of remote customer onboarding solutions in accordance with Article 13(1) of Directive (EU) 2015/849'. (4) Obliged entities must take into account the fact that the use of electronic identification means does not create an increased risk of money laundering and terrorist financing, in particular where such electronic means provide a high level of assurance in accordance with Regulation (EU) 910/2014.
Use of technological means to identify persons	28.	(1) Obliged entities that use or intend to use technological means for the purposes of identification and verification of a person must assess the extent to which the use of innovative technological solutions may address or potentially increase the risks of money laundering and terrorist financing, in particular in remote situations. As part of their assessment, obliged entities must have a clear understanding of the following issues:

Official Journal of the EU L 119, 4.5.2016, p. 1–88 125(I)/2018 26(I)/2022		(a) the risks related to information and communication technology and security risks, in particular the potential risk that the technological solution is inappropriate, unreliable or compromised; (b) qualitative risks, in particular the risk that the sources of information used for identity verification purposes may not be sufficiently independent and reliable and therefore may not comply with the provisions of the Law, and the risk that the degree of identity verification through these technological solutions is not proportionate to the level of money laundering and terrorist financing risk associated with the business relationship; (c) the legal risks, in particular the risk that the provider of the technological solution may not comply with applicable data protection law, For this purpose, obliged entities must take due account of their obligations under Regulation (EU) 2016/679 and Law 125(I)/2018, in their capacity as data controllers, including, but not limited to, the need to carry out a personal data protection impact assessment, where necessary; and (d) the risks of impersonation, i.e. the risk that the customer is not who he claims to be, or is not a real person. (2) Obliged entities using an external provider, instead of developing their own technological solution, bear the ultimate responsibility for fulfilling their obligations regarding the implementation of the due diligence measures. The nature of the relationship of the obliged entities with the provider of the technological solution must be clearly defined, and it must be precisely determined whether it is an outsourcing relationship or whether the use of such solution constitutes a form of operational or technological dependence on a third party, as set out in Article 67 of the Law. In any case where this relationship falls within the scope of Article 28 of Regulation (EU) 2016/679, i.e. it is a data controller-processor relationship, it is mandatory, inter alia, to conclude a written delegation agreement that meets all the requirements of Article 28(3) of Regulation (EU) 2016/679. (3) Obliged entities must take adequate measures to ensure that the provider of the technological solution: (a) provide sufficient assurances that the intended processing of personal data complies with the requirements of Regulation (EU) 2016/679 and Law 125(I)/2018 and ensures the protection of data subject's rights; (b) access and use a wide range of data from different sources over time, taking into account in particular the following: (i) electronic certification elements based on the customer's passport are unlikely to be sufficient in a remote context without additional checks to ensure that the customer is who he claims to be, and that the document has not been falsified; and (ii) in most situations a single data source or a single point in time is unlikely to sufficiently meet the verification standards; (c) is contractually bound to comply with the provisions of the agreement between them, and with the binding EU and the Law, and to inform the obliged entity immediately in the event of any change; and (d) operates in a transparent manner so that the obliged entity is aware at all times of the checks carried out, the sources used, the results and the reliability of those results. (4) Where the external provider is an undertaking established in a third country, the obliged entity shall ensure that in any event the conditions laid down in Chapter V of Regulation (EU) 2016/679 and the relevant measures supplementing the data transfer tools are met to ensure that the level of protection of the personal data of natural persons by the provider established in a third country is commensurate with the level in the EU. (5) Obliged entities must be able to substantiate to the Central Bank of Cyprus that the use of a specific technological solution is appropriate. (6) Obliged entities must apply the provisions of this Directive and comply with the requirements of the 'EBA Guidelines on the use of remote customer onboarding solutions pursuant to Article 13(1) of Directive (EU) 2015/849' of 22 November 2022.
Ability to accept customer identification verified by a third party	29.	(1) Subject to the provisions of Article 67 of the Law, obliged entities may rely on third parties to carry out identification procedures and customer due diligence measures as set out in Article 61(1) (a), (b) and (c) of the Law only when establishing the business relationship for the purposes of identifying and verifying the identity of their customers.

		(2) Any data and information for the purposes of updating the client's economic profile during the business relationship must be obtained directly from the natural person in whose name the account is held or, in the case of legal persons, from the natural persons who are the beneficial owner of the share capital of the legal persons or who exercise effective control over the legal persons or who are responsible for decision-making and direct the operations of the legal person. It is understood that the certification of documents may be carried out by third parties as described in subparagraph (1) above. (3) All documents, information and identification data received by the obliged entity shall be in one of the formats set out in Part 11 of this Directive. (4) The obliged entity must arrange a face-to-face meeting with customers who enter into a business relationship following a referral by a third party, as defined in Article 67 of the Law, and for whom the third party has carried out identification procedures and due diligence measures. The purpose of the meeting is to confirm the information and data obtained by the obliged entity from the third party, which form the economic and risk profile of the client, as well as to collect any additional data and information deemed necessary for obtaining first-hand knowledge of the customer. In the case of legal persons, the meeting must be held with the natural person or persons who are the beneficial owner of the share capital of the legal persons or who exercise effective control over the legal persons or who are responsible for decision-making and direct the operations of the legal person. This meeting must take place before any transaction takes place. The meeting can be held online, provided that adequate safeguards are in place, such as recording/visualization of the meeting. All evidence of the meeting, the names of the participants as well as a summary of the of the matters discussed in the meeting, must be kept in the client's file and be readily available at the Central Bank of Cyprus. (5) Any meetings with third persons who referred the customer to the obliged entity or with persons who are directly or indirectly linked to those third persons or registered shareholders, acting as nominee shareholders of the beneficial owner, shall not be considered as compliance by the obliged entity with the provisions of subparagraphs (1) to (4) above.
		(6) An obliged entity that relies on third parties to carry out identification procedures and due diligence measures shall, as a minimum, apply the following: (a) define and implement a relevant policy and procedures, in accordance with the requirements of the Law and this Directive; (b) the Anti-Money Laundering Compliance Officer shall verify that the requirements of Article 67(2) of the Law are met; (c) the obliged entity enters into an agreement with the third person setting out the obligations of each party, including the financial conditions, as well as the persons acting on behalf of the third person who are entitled to certify documents. A document containing a specimen of the signatures of the persons concerned shall be annexed to the Agreement; (d) apply identification procedures and due diligence measures for each third person, prior to the commencement of the business relationship; (e) the Anti-Money Laundering Compliance Officer assesses the quality of customers reccomended by third parties, taking into account, inter alia, the total number of customers established by the third party, the number of customers with whom the relationship was terminated for compliance purposes, the number of internal customers' suspicion reports, as well as any reports of suspicion to MOKAS. In the event that the quality of the customers is deemed unsatisfactory, then the relationship with the third party must be terminated; (f) the Anti-Money Laundering Compliance Officer keeps a separate file in which the identity of the third person is recorded, the data certifying that the third person is subject to supervision under the Law, the quality assessment report of the customers recommended by the third person, as well as the assessment report of the third person. These assessments should be reviewed annually; (g) the Anti-Money Laundering Compliance Officer must keep a record of the following data/information regarding third persons with whom the obliged entity has established cooperation: (i) For the third person: ➢ Name, ➢ address of business, ➢ professional field of activity,

		➢ supervisory authority, ➢ start date of cooperation; ➢ date of last assessment, ➢ date of the next evaluation. (ii) For customers recommended to the obliged entity by the third person: ➢ number of customers per year in the previous three years, ➢ results of customer evaluations that have been recommended; ➢ number of customers reported to MOKAS. (h) the Anti-Money Laundering Compliance Officer shall keep a record of data and information on third persons whom the Anti-Money Laundering Compliance Officer has rejected the cooperation or terminated the cooperation: ➢ Name, ➢ address of business, ➢ professional field of activity, ➢ supervisory authority, ➢ For customers recommended to the obliged entity by the third party, (to be completed as appropriate): o number of customers per year in the previous three years, o results of customer evaluations that have been recommended; o number of customers reported to MOKAS, ➢ date of cooperation rejection (to be completed as appropriate), ➢ start date of cooperation, (to be completed as appropriate), ➢ termination date of cooperation (to be completed as appropriate), ➢ grounds for rejecting or terminating cooperation. (i) the Anti-Money Laundering Compliance Officer approves in writing the commencement of cooperation with the third party and the acceptance of customer identification by the third party and keeps the approval in the third party's personal file, together with a relevant explanatory report for the commencement of cooperation.
Specific customer identification cases – Natural persons	30.	(1) Obliged entities shall establish the identity of natural persons by obtaining the following information: (a) the real name and/or forenames as they appear on the valid identity card or passport; (b) the full address of permanent residence, including the postal code; (c) telephone number; (d) the e-mail address; (e) date and place of birth; (f) details of professional and other business activities, including the name of the employer/enterprise, position in the undertaking; and (g) any other information deemed necessary, depending on the assessed risk. (2) Verification of the identity of a customer or a person who intends to carry out an individual transaction must be carried out on the basis on a valid: a) identity card (physical or electronic form), or b) passport. (3) Without prejudice to the provisions of subparagraph (2) above, in the case of payment service providers offering service No.(6) (Remittance Service), the identification of customers or persons carrying out individual transactions may be based on the valid Residence Permit of a foreign person (plastic identity card) issued by the Republic of Cyprus. (4) Provided that the obliged entities are satisfied with the identity of the customer from the identification documents presented to them, they shall keep copies thereof. The documentation must be kept in accordance with the requirements of Part 11 of this Directive. (5) Obliged entities may check the security features of identity cards or passports against the Public Online Register of Authentic Identity and Travel Documents - PRADO.

		(6) In addition to the verification of the name, the customer's permanent residence address is also verified, in one of the following ways: (a) a visit to the place of residence by an officer of the obliged entity. After the visit, this officer prepares and files a relevant note in the customer's file; (b) presenting a recent (up to 6 months old) utility bill (e.g. electricity, water), or a home insurance document, or a municipal tax bill or income tax document, or a document from another government department/service and/or bank statement; (c) by mail with a double-registered letter to the address previously verified by the obliged entity from independent and reliable sources. For example, communication may include sending documents for account opening or initiating the business relationship, which the customer must return to the obliged entity or sending a code by which the customer accesses his/her accounts online. In any case, the obliged entity shall keep evidence in the customer's file proving that correspondence has been sent and received at the stated address. (7) Where the authentication is carried out using electronic utility bills, the obliged entity shall take additional measures and checks to verify that the information received on the address is correct. (8) Obliged entities shall request and obtain information on public positions held or previously held by the customer over the past twelve months, including whether the customer is a "direct" close relative or close associate of such a person, in order to determine whether that customer is a politically exposed person.
		(9) (a) Obliged entities are required to collect, verify and retain customer identification data in order to ensure compliance with both the requirements to prevent money laundering and terrorist financing and with the obligations to apply financial sanctions, trade embargoes and measures related to terrorism or proliferation of weapons of mass destruction, which are imposed by United Nations Security Council Resolutions, Decisions and Regulations of the European Union or by other bodies with which the obliged entity is required to comply under its applicable domestic legal framework. (b) For this purpose, obliged entities must ensure that the identification documents they receive include at least the following information: (i) the number of the identification document; (ii) date and country of issue, (iii) customer's name, and (iv) customer's date of birth so that the obliged entity is able to verify whether the customer is on a list of persons subject to sanctions adopted by the United Nations and/or the European Union on the basis of a relevant resolution of the United Nations Security Council and a Regulation or Common Position of the Council of the European Union, respectively.
Customers without standard identification documents	31.	(1) Without prejudice to paragraph 30 above, in cases where a natural person is reasonably unable to present official identification documents as defined in paragraph 30, the obliged entity may apply an individual personalised and risk-based approach to confirm his or her identity, provided that no increased risk of money laundering or terrorist financing is identified. The provisions of subparagraph (7)-(8) of paragraph 12 of this Directive shall also apply to natural persons who are not reasonably able to present official identification documents as defined in paragraph 30, such as reasons of health or physical incapacity. (2) Before deciding to apply an individual, personalised approach to confirm the identity of the natural person in accordance with subparagraph (1) above, the obliged entity must examine and determine that the requirements of paragraph 30 are not reasonably applicable due to the specific circumstances of the natural person concerned. (3) For the cases of natural persons referred to in this paragraph, identification may be carried out using other evidence, provided that such evidence is deemed by the obliged entity to be sufficient and reliable. (4) The data collected for the purpose of applying this paragraph shall be assessed in conjunction with the customer's risk profile and fully documented in customer's file, along with the justification for their acceptance. The obliged entity is responsible for ensuring that the approach applied is appropriate, proportionate to the assessed risk and allows for compliance with the applicable legal and regulatory framework for the prevention of money laundering and the application of restrictive measures.
Customers of credit institutions falling within	32.	(1) Without prejudice to the provisions of paragraphs 30(1) and (2) of this Directive for the identification of natural persons, by way of exception, and only for the purposes

the scope of Law 64(I)/2017 – 64(I)/2017 124(I)/2020 76(I)/2021		of Part IV of the Comparability of Fees, Payment Account Switching and Access to Payment Accounts with Basic Features Laws of 2017 to 2021 (hereinafter 'Law 64(I)/2017'), the identification of persons legally resident in the European Union, within the meaning of Article 2 of Law 64(I)/2017, may be carried out by presenting to the obliged entity official documents issued by the competent Cypriot authorities, provided that they contain the following data of the holder: (a) surname and forename; (b) date of birth, (c) nationality and country of origin; and (d) the expiry date of the document. Such document shall bear a photograph of the holder, a unique number or code and shall be valid.
		(2) Obliged entities shall require natural persons who apply to start a business relationship and who fall within the scope of Law 64(I)/2017 to provide, when opening an account, their identity card or passport or copies thereof, or any other documents that may be ancillary to their identification, where available.
		(3) With regard to identification and verification of identity under subparagraph (1) above, for persons who have applied for international protection or have already been recognised as political refugees or beneficiaries of subsidiary protection status, if the obliged entities have information or reasonable suspicions as to the authenticity of the documents presented by these persons, then the obliged entities must not apply to the Embassy or Consulate of the country of origin of these persons in the Republic, nor to financial institutions of the country of origin of these persons for verification of the authenticity of these documents, except to the competent issuing authority of the Republic, by virtue of a written authorisation to that effect, which they receive from the customer when opening the account.
		(4) Without prejudice to the provisions of paragraph 30(1)(b) of this Directive, only in the case of the persons referred to in subparagraph (1) above and solely for the purposes of applying Law 64(I)/2017, the verification of the address of the customer's home/residence may be carried out either by one of the means referred to in paragraph 29(7) of this Directive or by one of the following means: (a) the address indicated on one of the official documents referred to in subparagraph (1) above, which may even represent the temporary address of the person requesting to initiate a business relationship (e.g. the address of a governmental reception center for asylum seekers or of a non-governmental organisation assisting that person); (b) with a sworn affidavit specifying their home/residence address and acknowledging their obligation to inform the obliged entity as soon as possible in the event of a change of address.
		(5) Obliged entities shall establish policies and procedures, take measures and implement control procedures based on calculated risk for business relationships with persons falling within the scope of Law 64(I)/2017.
		(6) Obliged entities are required to implement appropriate measures and procedures based on the calculated risk in relation to the identification of persons falling within the scope of Law 64(I)/2017, taking into account the combination of geographical risk and uncertainty related to the identification documents of those persons. These measures aim to manage any increased risk of money laundering and terrorist financing. For example, obliged entities may apply the following measures: (a) limits/restrictions, on the basis of calculated risk, on the products and services to be provided by obliged entities with the ultimate aim of better managing the risk of money laundering without compromising the compliance of obliged entities with the provisions of Article 18(1) of Law 64(I)/2017; (b) control procedures, which ensure that the account holder provides the required documents in a timely manner as soon as they expire; (c) integration of the specificities of persons falling within the scope of Law 64(I)/2017 (e.g. asylum seekers, political refugees, beneficiaries of subsidiary protection status, victims of trafficking and/or exploitation of persons) into the measures, procedures and systems of obliged entities. These specificities may concern frequent changes of the residence address of the persons concerned, frequent small transactions with the countries of origin and receipt of state aid (e.g. beneficiaries of a guaranteed minimum income);

		(d) sending the correspondence of those persons by registered mail or by a member of staff of the obliged entity as an additional measure of diligence to ascertain their address.
		(7) Provided that the obligation of obliged entities to apply the necessary due diligence measures, such as the creation of the economic profile of customers and the continuous monitoring of transactions, applies as to all customers and that such measures are proportionate to their risk level.
		(8) Where obliged entities decide to refuse to open an account with basic features or restrict the terms of operation of such an account to comply with the prevention of money laundering and terrorist financing, they must justify the reason for such actions and be prepared to demonstrate to the Central Bank of Cyprus that such measures were appropriate and proportionate to the risk posed by the business relationship with the natural person concerned.
		(9) For all cases of persons falling within the scope of Law 64(I)/2017, the special residence permit and, in the case of political refugees, the refugee travel document, issued by the Civil Registry and Migration Department of the Ministry of Interior of the Republic, shall meet the criteria (a) to (c) of paragraph 32(1) of this Directive. Obliged entities must therefore request and receive these documents in the case of persons falling within the scope of Law 64(I)/2017. Copies of the necessary documents, which must be presented as originals by the person requesting to open an account with basic features, are available on the PRADO platform: (i) For the special residence permit: https://www.consilium.europa.eu/prado/en/CYP-HO-05001/index.html (ii) For the refugee travel document: https://www.consilium.europa.eu/prado/en/CYP-JO-02001/index.html (iii) For the Certificate of Foreigners Registration : https://www.consilium.europa.eu/prado/en/CYP-HO-04006/index.html
		(10) As an additional control measure, obliged entities must ask natural persons falling within the scope of Law 64(I)/2017 to provide, when opening an account, if they have an identity card or passport or copies thereof, or any other documents issued by their country of origin that may assist in their identification.
Fourth Annex Fifth Annex		(11) Applicants for international asylum whose application is under examination by the competent authorities of the Republic and therefore do not have the special residence permit and the refugee travel document that meet the criteria (a) to (c) of paragraph 32(1) above may request to open a payment account with basic features, by presenting the certificate of application (Fourth Annex) from the Asylum Service of the Ministry of Interior as well as the Certificate of Foreigners Registration. Due to the fact that the above-mentioned documents do not have an expiry date, the obliged entities provide the applicant with a specific form by which the applicant gives his/her consent to the obliged entity to receive information regarding the stage of examination of his/her asylum application from the Asylum Service of the Ministry of Interior. This form is sent by fax or e-mail to the Asylum Service, which indicates the status of the application (e.g. under examination/completed) signed and stamped by the Service and sent back to the credit institution in the same way. Obliged entities must follow the above-mentioned procedure on a risk-basis approach and for as long as the application of the natural person concerned is under examination. (12) Victims of trafficking and/or exploitation of persons may present the certificate of recognition issued by the Cyprus Police (Fifth Annex), which meets the criteria (a) to (c) of paragraph 32(1) above and is valid for one month, until the issuance of the special residence permit by the Civil Registry and Migration Department. Obliged entities are required to request and obtain from the customer the specific residence permit as soon as it is issued.
Joint accounts	33.	In cases of joint accounts held by two or more persons, the identity of all persons holding and/or entitled to manage the account must be verified, in accordance with the procedures for identifying natural persons.
Authorised representatives or representatives of third parties	34.	Subject to the provisions of Article 61(1) of the Law, in every case where a third party acts on behalf of a customer, obliged entities must obtain and keep a copy of the relevant authorisation agreement concluded between the customer and the third party.
Associations, societies, clubs, provident funds	35.	(1) Where a business relationship is established with associations, societies, clubs, povident funds and charities, obliged entities must ascertain their operating purposes

and charities		and ascertain their legitimacy by requesting the submission of their constitutional and other important documents, including, where necessary, their certificate of registration from the competent authorities. (2) Obliged entities must obtain a list of, and identify, the members of the organisation's Management Board/Committee and all persons entitled to manage the account or to carry out a transaction for and on behalf of that organisation in accordance with the identification procedures for natural persons. Obliged entities shall also receive a copy of the minutes of the relevant decision of the Board regarding the opening and management of accounts.
Sole proprietorships /partnerships	36.	(1) Where a business relationship is established with sole proprietorships, partnerships and other entities without legal identity, obliged entities must identify the directors/partners/beneficial owners and all persons entitled to manage the account or to carry out transactions in accordance with the procedures applicable to natural persons. (2) For partnerships, a certificate of registration of the partnerships must be obtained. (3) Obliged entities must obtain evidence of the address of the undertaking's main management offices, establish the nature and size of the undertaking's business and obtain all the information required under paragraph 26 of this Directive to create the undertaking's economic profile. (4) Where there is a formal partnership agreement, the obliged entity must obtain a copy of it, as well as to request for the written decision of the partnership authorising the establishment of a business relationship or the opening and management of the account or the execution of transactions by authorised persons.
Legal persons	37.	(1) When entering into a business relationship with legal persons (companies), obliged entities are required to take all appropriate measures to fully ascertain the ownership and control structure of the companies and to identify the beneficial owners and the natural persons who effectively control the company.
		(2) The term "shell company/entity" refers to a limited liability company or any other legal entity which has the following characteristics: a) It has no physical presence or activity in its country of incorporation/registration, except usually a postal address. The physical presence of a company/legal entity is interpreted as the existence of a place of business or activity (owned or rented buildings) in the country of incorporation/registration. Furthermore, the absence of substantial management (meaningful mind) and administration can be interpreted as a lack of physical presence. The presence of a third person who merely provides the services of a representative /authorised person, including company secretary duties, shall not in itself constitute an indication of physical presence; and/or b) It has no established business activity, has little or no independent economic value and no evidence to the contrary can be provided. Notwithstanding the above, the following circumstances may indicate business activity: (i) the company/entity was established/incorporated for the purpose of holding share capital or shares or equity instruments of another business entity or entities engaged in legitimate business with identifiable ultimate beneficiary(ies); (ii) the company/entity was established/incorporated for the purpose of holding intangible or other assets, including immovable property , ships, aircraft, investment portfolio, debt and financial instruments; (iii) the company/legal entity was established/incorporated to facilitate monetary transactions and asset transfers, corporate mergers, as well as to perform asset management activities and share trading; (iv) the company/ entity acts as treasurer for companies recognised as a group or manages the activities of the group; (v) any other case where convincing evidence can be provided that the company/entity is engaged in a legitimate business activity, with identifiable ultimate beneficiary(ies). (3) Legal persons engaged in the remote execution of commercial activities may be excluded from the above definition, including: • the sale of products or services to customers; • content production (e.g. digital marketing, affiliate marketing), • the provision of professional or technological services (e.g. planning, consulting).

		(4)The above exemption is allowed provided that the obliged entity takes appropriate measures to verify the activity of the legal persons in question, based on the assessed risk. (5) To substantiate the business activity, the obliged entity must, indicatively, collect, assess and file the following evidence: • the company's financial statements, • active bank accounts reflecting commercial transactions; • tax returns; • data for maintaining a business website, online shops or other public sales points; • details of customers and business partners, • contracts and purchase and sales documents.
		(6) Where a legal person falls within the definition of 'shell company' as described in paragraph 37(2) of this Directive; and a) is registered in a jurisdiction where companies/entities are not obliged to submit to the authorities audited financial statements by independent auditors /accountants and does not voluntarily prepare financial statements by independent approved certified auditors/accountants; and/or b) is tax resident in a jurisdiction listed in the EU list of non-cooperative jurisdictions for tax purposes or in the Global Forum on Transparency and Exchange of Information for Tax Purposes list of non-cooperative jurisdictions or in any other list issued by a reputable organisation in relation to harmful tax practices, tax havens or has no tax residence; then, the business relationships with such an entity shall not be established or, if they exist, must be terminated.
		(7) In all cases of legal persons, falling under the definition of 'shell company' in accordance with subparagraph (2), the obliged entity shall decide whether to establish or maintain the business relationship, applying a risk-based approach in accordance with the legal and regulatory framework and providing a fully documented justification for such a decision, which shall be duly justified/documented and recorded.
		(8) In order to comply with subparagraphs (2)-(7) above, the obliged entity shall establish policies, procedures and controls to ensure its effective implementation and full compliance with the above requirements.
		(9) The verification of the identity of a company that requests the initiation of a business relationship or the carrying out of an individual transaction requires the receipt of data / information on the following: (a) registration number; (b) registered name and trade name used; (c) address of the registered office; (d) full addresses of the head office/principal management office; (e) telephone, fax (where available) and e-mail numbers; (f) members of the Board of Directors; (g) persons authorised by the company to operate the company's account alongside the obliged entity and to act on behalf of the company; (h) beneficial owners of private and public companies which are not listed on a stock exchange of a country of the European Economic Area or of a third country with equivalent information and transparency requirements applicable in the European Union; (i) registered shareholders acting as proxies (nominees) of the beneficial owners; (j) any other information necessary to create the economic profile of the company on the basis of the provisions of paragraph 25 above.
		(10) The obliged entity shall verify the information referred to in subparagraph (9) through independent and reliable sources. Verification should be done by taking into account: (a) certificate of company incorporation; (b) certificate of registered office; (c) certificate of directors and secretary;

		(d) in the case of private companies, a certificate of registered shareholders; (e) the memorandum and articles of association of the company; (f) a resolution of the Board of Directors of the company, certified by the secretary of the company, to open the account, giving the necessary authorisation to the persons who will operate the account; (g) where the registered shareholders act as nominees of the beneficial owners, a copy of the signed contract concluded between the nominee and the beneficial owner (trust deed) by virute of which the shares are registered in the name of the nominee on behalf of the beneficial owner; (h) the ownership structure of the company, certified by the beneficial owner or the person exercising effective control of the legal person or the person ultimately responsible for decision-making and managing customer's operations; (i) documents and information to verify, in accordance with the provisions of this Directive, the identity of the authorised signatories, registered shareholders and beneficial owners of the company; (j) certificate of registered shareholders for companies which participate in the ownership structure of the customer (company) and which hold directly or indirectly the share capital of the customer in accordance with Article 2 of the Law; (k) recent audited financial statements. In cases where there is no legal obligation to prepare audited financial statements or where there are no recent audited financial statements (for at least the previous two years), recent management accounts must be obtained.
		(11) For legal persons incorporated outside Cyprus, obliged entities must request and receive documents and information corresponding to those set out in subparagraph (10) above.
		(12) Obliged entities, as an additional due diligence measure and on the basis of the assessed risk emanating from the business relationship with the legal person, could carry out a search and obtain information from the register of the Department of Registrar of Companies and Intellectual Property in Cyprus for domestic legal persons, and for non-Cypriot legal persons of the respective competent authority in the country of incorporation of the legal person abroad, and/or obtain information from other valid sources, in order to ascertain that the legal person has not been dissolved, is not in the process of being wound up or liquidated or removed from the register of the Department of Registrar of Companies and Intellectual Property, and is duly registered as a going concern in the relevant register of the competent authority in Cyprus or of another relevant competent authority outside the Republic. (14) The obliged entity should carry out a further reviews if at any later stage there are changes in the structure or ownership of the company or suspicions arise due to changes in the nature, economic and commercial purpose of the transactions carried out by the company. The objective of the review is to ascertain the nature and possible consequences of these changes in the documents and information held by the obliged entity for the company and to collect all necessary and additional information and data to complete and update company's economic.
		(13) Subject to the provisions of paragraph 5(b) of Article 61A of the Law, if the information provided by the customer differs from that available to the official authorities, then an investigation must be carried out by the obliged entity and, where necessary, a suspicion report must be submitted to MOKAS.
		(14) Where the person requesting the establishment of a business relationship is a company whose direct sole or major shareholder is another company (parent/holding) registered in Cyprus or abroad, then the obliged entities must, before initiating the business relationship, establish the ownership structure and verify the identity of the natural persons who are the beneficial owners and/or exercise control over the parent/holding company.
Investment funds and businesses providing of financial services and investment services	38.	(1) Obliged entities may establish and maintain business relationships with persons engaging in the provision of financial services and/or investment services and who are established and/or operated and supervised by a competent authority of a country in the European Economic Area or a third country which, on the basis of Annex II to the Law, is considered to be potentially low-risk, by applying, according to the assessed risk, appropriate due diligence measures, in accordance with the requirements of the Law and this Directive.
		(2) In the case of investment funds, obliged entities are required to obtain sufficient information on the legal existence of the fund, its purpose, investment objectives and control structure.

		(3) Furthermore, and depending on the risk assessment, obliged entities are required to obtain data and information to ascertain the identity of the investment managers and advisers, administrators and custodians, investors or any other person with significant involvement in the management/administration/operation of the Fund.
Crypto-asset service providers regulated and supervised in accordance with Regulation (EU) No 2023/1114	39.	Obliged entities may establish and maintain business relationships with a crypto-asset service provider that is regulated and supervised in accordance with Regulation (EU) No 2023/1114 by applying, in accordance with the assessed risk, appropriate due diligence measures, in accordance with the requirements of the Law and this Directive.
Safekeeping services and safe deposit box rentals	40.	Obliged entities shall follow identification procedures and apply customer due diligence measures as defined by the Law and this Directive based on the assessed risk when requesting safe deposit box rental services from persons who do not maintain a business relationship with the obliged entity.
Simplified identification and due diligence procedure	41.	(1) Obliged entities may apply simplified due diligence measures in accordance with Article 63 of the Law provided that they have first ascertained that the risk associated with a business relationship or transaction has been assessed as low and provided that there is no suspicion of money laundering or terrorist financing. It is understood that the application of simplified due diligence measures shall not result in an exemption from any due diligence measure. However, obliged entities may adjust the extent, timing or type of each or all due diligence measures to be proportionate to the assessed low risk they have identified. Obliged entities must have in place adequate transaction and business relationship monitoring procedures to detect suspicious or unusual transactions in a timely manner. (2) The simplified due diligence measures that obliged entities may apply include but are not limited to the following: (a) Adjusting the timing of due diligence measures, e.g. where the product or transaction sought has features that limit its use for money laundering or terrorist financing purposes, for example by: (i) verifying the identity of the customer or beneficial owner at the time of entering into the business relationship; or (ii) verifying the identity of the customer or beneficial owner as soon as the transactions exceed a predetermined threshold or after a reasonable period of time has elapsed. Obliged entities must ensure that: 1. this does not entail a de facto exemption from the application of due diligence measures, i.e. obliged entities must ensure that the identity of the customer or beneficial owner is ultimately verified; 2. the limit or period of time is set at a reasonably low level. It is understood that, with regard to terrorist financing, the mere setting of a low threshold may not be sufficient to reduce the risk; 3. have systems in place to be able to detect when that threshold has been reached or the time has elapsed; and 4. do not postpone the application of due diligence measures or delay the collection of relevant customer information in a way that would infringe the provisions of the Law, this Directive or European Regulations (e.g. EU Regulation 2023/1113). (b) Adjusting the scope of information obtained for identification, verification or monitoring purposes, for example by: (i) verifying identity based on information obtained from a single valid, reliable, and independent document or data source; or (ii) taking into account the nature and purpose of the business relationship, because the product is designed solely for a specific use, such as a company's pension plan or a shopping mall gift card. (c) Adapting the quality or source of information obtained for the purposes of identification, verification or monitoring, for example by: (i) accepting information received from the customer and not from an independent source to verify the client's business and risk profile. It is noted that this is not allowed as part of the identity verification process; or (ii) where the risk associated with all aspects of the relationship is very low, the source of funds may be used to satisfy certain requirements of the due diligence measures, e.g. where the funds are government benefits or where the funds have been transferred by an authorised credit or financial institution established within the European Economic Area from an account in the customer's name.

		(d) Adjusting the frequency of updating and reviewing the business relationship in terms of applying due diligence measures e.g. carrying out an update and review only if specific events occur, such as when the customer is seeking to provide a new product or service or when the threshold of a specific transaction has been reached. Obliged entities are required to ensure that this does not result in a de facto exemption from updating information for due diligence purposes. (e) Adjust the frequency and intensity of transaction monitoring, e.g. by monitoring only transactions exceeding a defined threshold. Where obliged entities choose this measure, they must ensure that the threshold is set at a reasonable level and that they have systems in place to identify linked transactions that, in aggregate, exceed that threshold. Even if customer transactions involve small amounts, the obliged entity must check the origin and destination of funds . (3) Obliged entities must take into account the additional simplified due diligence measures referred to in Title II of the 'EBA Risk Factors Guidelines', which may be of particular relevance in different areas. Those measures do not apply where this Directive explicitly sets out the due diligence measures to be applied.
		(4) The information that an obliged entity receives when applying simplified due diligence measures must enable it to reasonably ensure that its assessment of the low risk associated with the business relationship is justified. They must also be sufficient to provide it with adequate information about the nature of the business relationship to be able to detect any unusual or suspicious transactions. The application of simplified due diligence measures does not exempt an obliged entity from the obligation to report suspicious transactions to MOKAS. (5) Where there are indications that the risk may not be low or where 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, the obliged entity shall not apply simplified due diligence measures. Furthermore, simplified due diligence measures must not be applied in cases where specific high-risk scenarios may apply and consequently, there is an obligation to apply enhanced due diligence measures.
Enhanced due diligence measures	42.	(1) Obliged entities are required to apply enhanced and additional due diligence measures, in cases of higher risk of money laundering or terrorist financing, to manage and mitigate those risks appropriately. Enhanced due diligence measures do not replace the standard measures provided for in the Law and this Directive but are applied in addition to them. The extent and number of checks carried out for identification vary depending on the assessed risk. (2) In addition to the cases referred to in Article 64(1) of the Law for which obliged entities are required to apply enhanced due diligence measures, obliged entities are required to apply enhanced due diligence measures when entering into a business relationship with the following categories of customers: (a) Trust and foundation accounts. (b) Client accounts in the name of a third person. (c) Investment funds, financial services firms and firms providing investment services from third countries considered medium or high-risk. (d) Crypto-asset service providers not regulated and supervised in accordance with Regulation (EU) 2023/1114.
		(3) The obliged entity must specify in its customer acceptance policy the categories of customers considered to be high-risk, as defined in the Law and in this Directive, as well as the cases of business relationships and transactions that the obliged entity has classified as high-risk based on its risk assessment and the policy it has developed.
		(4) The appropriate enhanced due diligence measures, including the extent of additional information received by the obliged entity and its enhanced monitoring, depend on why the business relationship or individual transaction has been identified as high-risk. (5) In all high-risk cases, obliged entities shall make informed decisions regarding the enhanced due diligence measures they apply. (6) Where an obliged entity classifies a business relationship or individual transaction as high risk and the type of business relationship or individual transaction is not explicitly mentioned in the Law or in this Directive, the obliged entity shall apply the due diligence measures set out in subparagraph (8) below. It is understood that

		obliged entities are not obliged to apply in all cases all the enhanced due diligence measures listed below. (7) Without prejudice to subparagraph (6) above, high-risk business relationships must be updated at least once a year or earlier if deemed necessary.
		(8) The enhanced due diligence measures that obliged entities should apply may include the following: (a) obtaining additional information for the purpose of applying due diligence measures: (i) information on the identity of the customer or beneficial owner, or the ownership and control structure of the customer, in order to ensure that the risk associated with the relationship is well understood. In this context, it may be necessary to obtain and assess information on the reputation of the customer or beneficial owner, as well as to assess any negative allegations made against the customer or beneficial owner. Indicatively: 1. information on family members and close business partners; 2. information on past and current business activities of the customer or the beneficial owner; and 3. negative references in the media. (ii) information on the intended nature of the business relationship in order to ascertain the legitimacy of the nature and purpose of the business relationship and to facilitate the obliged entity in establishing a more comprehensive customer risk profile. This may include obtaining information about the following items: 1. the number, size and frequency of transactions likely to be carried out through the account to enable the obliged entity to identify deviations that may raise suspicions of money laundering and terrorist financing; 2. the reason why the customer requests a particular product or service, in particular where it is not clear why the customer's needs cannot be better met in another way or in another jurisdiction; 3. the destination of the funds; 4. the nature of the customer's or beneficial owner's business so that the obliged entity can better understand the likely nature of the business relationship. (b) Increasing the quality of information, obtained for the purpose of applying due diligence measures, to identify the customer or the beneficial owner, through means including: (i) requiring that the first transaction to be carried out through a verifiable account held in the customer's name with a credit institution that applies due diligence measures that are no less stringent than the corresponding standards set out in Chapter II of Directive (EU) 2015/849; or (ii) ensuring that the client's assets and funds used in the context of the business relationship do not constitute proceeds of criminal activity and that the source of wealth and source of funds are consistent with the information at the disposal of the obliged entity. Where the risk from a business relationship is particularly high, verification of the source of wealth and the source of funds may be the only appropriate means to reduce the risk. The source of funds or wealth may be verified, inter alia, on the basis of VAT and income tax returns, copies of audited accounts, payslips, public documents or references to independent media. Obliged entities must bear in mind that even funds from legitimate business activities may constitute money laundering or terrorist financing as defined in Article 1(3) to (5) of Directive (EU) 2015/849. (c) Increasing the frequency of the review and reassessment of the business relationship to ensure that the obliged entity remains able to manage the risk associated with the individual business relationship or to conclude that the relationship no longer corresponds to the obliged entity's risk appetite and to facilitate the identification of any transactions requiring further reassessment, including by: (i) increasing the frequency of reassessment of the business relationship in order to ascertain whether the customer's risk profile has changed and whether the risk remains manageable; (ii) obtaining senior management approval to enter into or continue the business relationship in order to ensure that senior management is aware of the risk to

		which the obliged entity is exposed and can make an informed decision as to whether they have the appropriate means to manage that risk; (iii) reassessing the business relationship on a more regular basis to ensure that any changes to the customer's risk profile are identified and assessed and steps are taken if necessary; or (iv) conducting more frequent and thorough monitoring of transactions to identify any unusual or unexpected transactions that give rise to suspicions of money laundering or terrorist financing. This may include verifying the destination of the funds or the reason why certain transactions are carried out. (9) In addition to the above, obliged entities are required to take into account the additional enhanced due diligence measures referred to in Title II of the EBA Risk Factors Guidelines , which may be of particular relevance in different areas.
		(10) The Anti-Money Laundering Compliance Officer must be informed of the new high-risk clients that the obliged entity intends to accept as well as existing high-risk clients and must be consulted before senior management takes a final decision on establishing a business relationship with high-risk persons or maintaining business relationships with high-risk clients, in accordance with the obliged entity's internal policies to prevent money laundering and terrorist financing, and in particular in cases where the approval of senior management is explicitly required by law and this Directive. If senior management decides not to follow the advice of the Anti-Money Laundering Compliance Officer, they must duly justify and record their specific decision and set out how the risks raised by the Anti-Money Laundering Compliance Officer are being mitigated. (11) In the event of a change in the categorisation of high-risk clients to a lower level of risk, the Anti-Money Laundering Compliance Officer shall be informed accordingly and, if he disagrees, shall give an opinion accordingly. (12) Obliged entities must treat and classify as high risk the situations referred to in paragraphs 43 to 51 of this Directive and apply the enhanced due diligence measures referred to in those paragraphs. In addition, in such cases, and where not explicitly stated, as a minimum, enhanced due diligence measures must include obtaining senior management approval to initiate or continue the business relationship or to carry out an individual transaction, taking sufficient steps to identify the source of assets, and systematically and thoroughly monitoring the client's transactional behaviour.
Complex and unusually large transactions or unusual types of transactions	43.	(1) The obliged entity must have adequate policies and procedures in place to detect complex transactions or unusually large transactions or unusual patterns of transactions. Where the obliged entity detects such transactions, it is required to apply enhanced due diligence measures. Transactions may be considered unusual because: (a) are different from the transactions that the obliged entity would normally expect based on its knowledge of the customer, the business relationship or the category to which the customer belongs. The difference may relate to value, frequency, complexity or other similar elements, including where transactions involve larger amounts or are more frequent than usual. Also, where transactions involve small amounts and are unusually frequent, or where there are successive transactions without obvious economic justification. Such as transactions that are segmented in order to circumvent benchmarks or align unusual transactions with normal expected behaviour and patterns. Such transactions shall be assessed on the basis of information gathered during customer identification and ongoing monitoring of business relationships. (b) constitute an unusual or unexpected pattern of transaction compared to the customer's usual activity or to the pattern of customer transactions with similar activities, products or services; or (c) they are particularly complex compared to other, similar transactions linked to similar types of customers, products or services, while the obliged entity does not know the economic rationale or the legitimate purpose of the transaction or has doubts as to the accuracy of the information received. (2) Such enhanced due diligence measures shall be sufficient to assist the obliged entity in determining whether the transactions in question give rise to suspicions of money laundering and terrorist financing and shall include at least the following: (a) taking reasonable and sufficient steps to understand the history and purpose of such transactions, for example by tracking the source and destination of funds or obtaining more information about the client's business, to ascertain the likelihood that those transactions will be executed by the client; and

		(b) monitoring the business relationship and transactions more frequently and paying more attention to details. For example, an obliged entity may decide to monitor individual transactions if this measure is proportionate to the identified risk.
Trust and foundation accounts	44.	(1) Trusts are not a separate legal entity and therefore the business relationship is established through the trustees, who act on behalf of the trust. Therefore, trustees together with the trust should be considered as customers of the obliged entity. (2) When obliged entities enter into such relationships they shall: (a) establish the legal existence of the trust, the name, the country of administration and the law governing the trust, the date of its establishment, its operations, and verify the identity of the beneficial owners of the trust as defined in Article 2 of the Law, as well as obtain information on the original property at the time of its establishment. (b) establish the nature and purpose of the trust and its activities, as well as the source and origin of the funds.
196(I)/2012 109(I)/2013 117(I)/2014 142(I)/2015 114(I)/2020		(3) The above information must be verified by obtaining reliable and independent documents or information. Obliged entities shall therefore examine the original trust agreement, take copies of the relevant extracts from that agreement. In addition, they shall receive a certified copy of the trust's registration certificate from the relevant register, as provided for by the Law Regulating Companies Providing Administrative Services and Related Matters of 2012 to 2020, or any other equivalent law of another country or region, as well as other relevant information from the trustees.
		(4) Where the obliged entity enters into a business relationship or carries out an occasional transaction with foundations, it must verify the identify of the founder, the beneficiaries, its board of directors and other persons holding important roles or positions in the foundation (e.g. the protector). Furthermore, they must obtain information such as the purpose of its establishment, its registered address and other relevant information. The obliged entity must obtain copies of the memorandum or articles of association, where available, in order to verify the above information. (5) It is provided that in the case of another legal arrangement which has a structure or functions similar to trusts, similar data/information shall be collected. In all cases, the relevant data and information are recorded and kept in the customer's file.
'Client accounts' in the name of a third person ('client accounts')	45.	(1) Obliged entities may open accounts with third parties who, in the course of their normal professional activities, acting as intermediaries, hold money on behalf of their customers in dedicated "Customer Accounts" in the name of a third person. These accounts may be pooled accounts, in which the funds of multiple customers are credited, or they may be opened specifically to credit money belonging to a specific client of the third person (specific client account). (2) Obliged entities shall take reasonable steps to determine and document the purpose of opening client accounts and shall have at their disposal information such as: the types of clients whose funds are held in client accounts, the amount of transactions carried out, and exposure to sectors and geographical areas considered high risk for money laundering, terrorist financing or corruption. (3) The risk assessment carried out by the obliged entity should include, among other parameters, the assessment it has made of the business of the third person – ('customer'), the types of clients served by the customer's business and the jurisdictions to which the client's business is exposed. (4) The obliged entity must apply appropriate customer due diligence measures including verifying the identity of the customer and ultimate beneficial owners, conducting ongoing monitoring of the business relationship to manage the risks involved, the determination that the funds belong to clients of their customers and are not used for their own use, and verifying the identity of the beneficial owners of the funds transferred into the client account, depending on the case. (5) Where the obliged entity has identified on the basis of its money laundering and terrorist financing risk assessment that the level of risk associated with the business relationship and the use of the customer account is high, it should apply enhanced due diligence measures where appropriate.

37(I)/2019 CORRECTION OG, Appendix I(I), No 4701, date 03/05/2019 120(I)/2020 162(I)/2024		(6) Where the risk associated with the business relationship is low, according to the individual risk assessment, the obliged entity may apply simplified due diligence measures, subject to the conditions set out below: (a) the client is a financial institution from a European Economic Area country or a low-risk third country, as defined in paragraph 3 of Annex II to the Law, and is effectively supervised for compliance with those requirements; (b) the customer is a licensed bookmaker, as defined in the Betting Laws of 2012 to 2024, and holds a license from the National Betting Authority or a corresponding competent authority of an EU Member State and is subject to supervision for the purposes of compliance with the prevention of money laundering and terrorist financing; (c) For the two above cases, the following apply: (i) the risk of money laundering and terrorist financing associated with the business relationship is low, based, among other parameters, on the obliged entity's assessment of the customer's business activity, the types of clients with which the customer deals, and the jurisdictions in which the customer's business is exposed; (ii) the obliged entity ensures that the customer applies adequate and appropriate due diligence measures towards its own customers and the beneficial owners of its customers. In this regard, obliged entities may, depending on their risk assessment, take steps to assess the adequacy of the customer's due diligence measures by obtaining sample data and documentation from the customer for specific clients and transactions; (iii) the obliged entity takes measures depending on the risk level to ensure that the customer will provide information and documentation on the due diligence measures applied to its own clients who are the beneficial owners of the funds transferred to the 'clients account' immediately upon request, including incorporating relevant clauses in a contract with the customer or by conducting sample checks on customer's ability to provide information on the due diligence measures applied upon request. (7) Where the conditions referred to in subparagraph (6) above are met, the simplified measures that the obliged entity may apply are the following: (a) Identification and verification of the customer's identity, including the identity of the customer's beneficial owner; (b) an assessment of the purpose and intended nature of the business relationship; and (c) ongoing monitoring of the business relationship.
124(I)/2015 107(I)/2020 192(I)/2022		(8) Obliged entities may open and maintain a general client account at a casino (hereinafter referred to as "customer"), as defined in the Casino Operations and Control Laws of 2015 to 2022, provided that the following conditions are met: (a) obliged entities apply appropriate customer due diligence measures, commensurate with the calculated risk, including identification and verification of the customer's identity and the customer's beneficial owner; (b) the customer holds a license from the Cyprus Gaming and Casino Supervision Commission and is subject to supervision for the purposes of compliance with the prevention of money laundering and terrorist financing; (c) the obliged entity has carried out a documented individual risk assessment regarding, inter alia, the customer's business, the types of clients served by the customer's business and the jurisdictions in which the customer's business is exposed, the services and products it offers, and the channels of service provision; (d) the obliged entity has reviewed the customer's policies and procedures and ensures that they are aligned with the applicable legal framework. This includes assessing the customer due diligence measures, final beneficiaries, and procedures for monitoring transactions and reporting suspicious transactions that the customer has introduced; (e) the obliged entity ensures that the customer applies adequate and appropriate due diligence measures towards its own customers and the final beneficiaries of its customers in accordance with the Law. In this regard, the obliged entity shall take steps to assess the effective implementation of its due diligence policies and procedures by requesting sample data and documentation from the customer for its specific customers and transactions;

		(f) the obliged entity has taken measures depending on the level of risk to ensure that the customer will provide information and documentation on the due diligence measures applied to its own customers, who are the beneficial owners of the funds transferred to the 'client account', immediately upon request, including by incorporating relevant provisions in a contract with the customer or by testing the customer's ability to provide information on the due diligence measures applied upon request; (g) the business relationship is continuously monitored and updated every year.
		(9) Obliged entities may hold 'client accounts in the name of a third person from a person acting as auditor/accountant/tax advisor or independent legal professional /lawyer or trust and corporate services provider or real estate agent, and the person acting as such comes from a country of the European Economic Area or a low-risk third country, as defined in paragraph 3 of Annex II to the Law, provided that, in addition to the requirements of subparagraphs (1) to (5) above, the following conditions are cumulatively met: (a) for amounts equal to or greater than EUR 15.000, irrespective of whether the transaction is carried out in a single transaction or in several transactions between which there appears to be a link, the identification of the beneficial owners of credit transactions shall be required; Provided that if the beneficial owner of the credit transaction is a legal person, then the identity of the beneficial owners of the legal person is also verified. (b) appropriate customer due diligence measures are applied based on the estimated risk associated with the transaction and/or the beneficial owner of the transaction and information is obtained on the source and destination of the funds, the purpose of the transaction, as well as the appropriate supporting documentation for such transactions. (c) all information and documents necessary to identify the beneficiaries must be duly certified by the third person as true copies of the originals and must be obtained when the account is opened or, where applicable, before any credit transaction is carried out; (10) Obliged entities may hold 'pooled accounts' provided that they are able to hold sub-accounts or 'connected accounts' in their computerised system and are able to know and identify the beneficial owners of credit transactions for amounts equal to or in excess of EUR 15.000. Where it is not possible to hold sub-accounts or connected accounts, obliged entities are required to open a client account belonging to a specific client of the third person (specific client account') and to verify the identity of the beneficial owner before opening the account. (11) Without prejudice to the generality of the above paragraph, transactions for amounts equal to or greater than EUR 15.000 relating to payments to government departments (e.g. Department of Registrar of Companies and Intellectual Property, Tax Commissioner) may be carried out from the pooled account without the use of sub-accounts or connected accounts. For the above cases, obliged entities must verify the identity of the beneficial owners of credit transactions for amounts equal to or greater than EUR 15.000, as well as obtain documentary evidence of the transactions.
		(12) Obliged entities may open client accounts with persons who are not defined as third persons in accordance with Article 67(2) of the Law, and who, in the course of their standard professional activities, manage money belonging to their clients, provided that, in addition to the requirements of subparagraphs (1) to (5) above, the following conditions are cumulatively met: (a) obtain a copy of the relevant agreement or document assigning the management of funds, which has been concluded between the obliged entity's customer and the latter's own client; (b) the beneficial owners of credit transactions for amounts equal to or exceeding EUR 10.000 carried out in one or more transactions or connected transactions below the above amount are identified; (c) appropriate customer due diligence measures are applied based on the estimated risk associated with the transaction and/or the beneficial owner of the transaction and information is obtained on the source and destination of the funds, the purpose of the transaction as well as the appropriate supporting documentation for such transactions. (d) all information and documents necessary to identify the beneficiaries must be obtained in accordance with Part 11 of this Directive when opening the account or, as the case may be, before carrying out any credit transaction;

		(13) Obliged entities may hold 'pooled accounts' provided that they are able to hold sub-accounts or 'connected accounts' in their computerised system and are able to know and identify the beneficial owners of credit transactions for amounts equal to or in excess of EUR 10.000. Where it is not possible to hold sub-accounts or connected accounts, obliged entities are required to open a client account belonging to a specific client of the third person (specific client account') and to verify the identity of the beneficial owner before opening the account.
Politically exposed persons' accounts	46.	(1) Obliged entities shall put in place appropriate risk management systems including procedures to identify existing or potential customers who are politically exposed persons. Such procedures should include, depending on the degree of risk faced by each obliged entity, the implementation and use of a reliable electronic database of politically exposed persons, the receipt of information from the customer himself and the search for publicly available information, for example on the internet or in the media, as well as the list of prominent public functions issued by the European Commission in accordance with Article 20a(3) of Directive (EU) 2015/849. In the case of companies, legal entities, trusts and similar legal arrangements ("legal arrangements"), the above procedures should aim at verifying whether the beneficial owners, authorised signatories, directors and persons duly authorised to act on behalf of the above persons are politically exposed persons. If one of the above natural persons is identified as a politically exposed person, then automatically the business relationship and accounts of the company, legal entity or legal arrangement are subject to enhanced due diligence measures, adjusting the extent of such measures according to the level of risk. (2) Subject to the provisions of Article 64(1)(c) of the Law, obliged entities shall adopt, in addition to the usual due diligence measures, the following enhanced due diligence measures: (a) the decision to establish or maintain a business relationship with a politically exposed person is taken by a senior management official of the obliged entity at an appropriate hierarchical level and commensurate with the level of risk associated with the business relationship, on the basis of a short report on the customer's profile, in order to take informed decisions on issues that directly affect the risk profile of the obliged entity; (b) when a business relationship is established with a customer and it is subsequently found that the natural persons involved are or have become politically exposed persons, then an approval decision must be taken as point (a) above for the continuation of the business relationship. Therefore, the obliged entity shall at regular interval scarry out checks on existing customers and related persons, with a frequency of at least once a month, in order to identify any cases of persons who have become politically exposed persons; (c) when deciding whether to approve a relationship with a politically exposed person, the senior management shall base its decision on the level of money laundering and terrorist financing risk to which the obliged entity might be exposed if that business relationship was to be established, and on the extent to which the obliged entity has the appropriate means to effectively manage that risk; (d) before entering into a business relationship with a politically exposed person, the obliged entity shall receive sufficient evidence to enable it to verify not only his or her identity, but also to assess his or her professional reputation and integrity (e.g. checking any negative reports/information); (e) the obliged entity creates the financial profile of the customer who is a politically exposed person by requesting at least the data and information referred to in paragraph 26 above. The obliged entity must be particularly careful and diligent in cases of customers operating in sectors vulnerable to corruption, such as trade in oil, cigarettes, alcoholic beverages, etc.; (f) obliged entities should be even more cautious when such politically exposed persons come from or operate in a country which is widely known to face widespread problems of corruption in public life and economic destabilisation and whose anti-money laundering and counter-terrorist financing laws and regulations are not equivalent to internationally accepted standards. To address potential risks from the above, obliged entities should assess the countries from which their customers originate in order to identify those countries that are considered most vulnerable to symptoms of corruption or that have laws and regulations that fall significantly short of the FATF Recommendations against Money Laundering and Terrorist Financing;

		(g) the obliged entity takes appropriate measures to identify the source of wealth and the source of funds to be used in the context of the business relationship with a politically exposed person to ensure that it does not manage proceeds from corruption or other criminal activity. The measures that the obliged entity should take to determine the source of wealth and the source of funds of the politically exposed person depend on the level of high risk associated with the business relationship. Where the risk is particularly high, the obliged entity must verify the source of wealth and the source of funds, on the basis of reliable and independent data, documents or information; (h) the obliged entity is required to perform enhanced and ongoing monitoring of both the transactions and the risk profile of the politically exposed person. Any unusual transactions must be identified, and the information at its disposal must be reviewed on a regular basis to ensure that any new or emerging information that could affect the risk assessment is identified in a timely manner. The frequency of monitoring should be determined by the level of high risk associated with the relationship. Without prejudice to the above, the customer's business relationship, account and economic profile must be reviewed at least annually, subject to a decision by the senior management on whether to allow them to continue operating; (i) the officer, who is responsible for monitoring the business relationship, is required to prepare a short report stating the results of the review. The report shall be submitted to a senior management official of the obliged entity for consideration and approval and shall be recorded in customer's file.
Investment funds, financial services firms and investment services firms	47.	(1) Where a business relationship is established and maintained with persons active in the provision of financial services and investment services and established and/or operating in a medium- or high-risk third country, obliged entities shall apply enhanced due diligence measures. As a minimum, obliged entities shall apply the following enhanced measures and procedures, in addition to the due diligence measures and customer identification procedures laid down by law and this Directive, to identify and verify the identity of natural and legal persons, including beneficial owners: (a) obtain the approval of the Anti-Money Laundering Compliance Officer before the commencement of the business relationship; (b) receive a copy of the authorisation or approval granted to that person by a competent supervisory/regulatory authority of their countries of incorporation and operation, the authenticity of which is verified either by direct communication with that supervisory/regulatory authority or through other independent and reliable sources; (c) ensure that the legal entity concerned is subject to supervision for the purposes of preventing money laundering and terrorist financing; (d) ensure that their authorisation provides for the provision of investment advice in financial instruments and/or portfolio management; (e) obtain sufficient data and information to fully understand the ownership and control structure of the business activities and the nature of the investment services and financial services they provides; (f) have procedures in place to monitor transactions on a regular basis; (g) assess the findings for fines or other administrative/supervisory measures imposed on that entity by their supervisory authority; (h) in the case of investment funds, to obtain information on the legal status of the investment fund, the objectives, the investment goals and the control structure of the fund. In addition, obliged entities shall receive data and information to identify and verify the identity of investment managers and advisers, administrators and custodians, investors or any other significant person involved in the operation of the Fund. It is understood that persons involved in the provision of financial and investment services and established and/or operating in a medium or high-risk third country may not hold "Client Accounts" in the name of a third person (client accounts). (2) Where a business relationship is established with a company whose parent company provides financial and/or investment services, obliged entities must also apply the provisions of the above paragraph in relation to the parent company.
Cross-border correspondent relationships with a customer institution from a third country	48.	(1) Obliged entities (correspondent institutions) when entering into cross-border correspondent relationships with a customer-institution must apply the standard due diligence measures provided for in Article 61 of the Law, as well as the enhanced customer due diligence measures provided for in Article 64(1)(b) of the Law, adapt

		the extent of such measures according to the level of risk, and adequately document the due diligence measures taken and the decision-making procedures applied. (2) In order to comply with Articles 64(1)(b), 66(1)(a) and 66(1)(b) of the Law, obliged entities must ensure that: (a) the customer-institution requesting the opening of a correspondent account is affiliated to a regulated financial group or maintains a physical presence with a fully staffed office in its country of incorporation from which it conducts actual banking services, i.e. the customer- institution is not a shell bank as defined in Article 2 of the Law. The existence and operating status of the customer-institution, as well as the regulatory framework governing its operations, must be verified by the obliged entities in one of the following ways: (i) verification with data from the Central Bank of Cyprus or other competent supervisory authority of the country of incorporation of that institution; or (ii) taking appropriate evidence of the structure of the group to which that customer institution belongs and of its licence or authorisation to carry out banking and/or financial operations; and (iii) obtain written assurance as well as extracts from the policies and procedures of the customer institution in which the institution declares that it does not deal with shell banks or alternatively identifies publicly available information, such as, for example, legal provisions prohibiting that institution from dealing with shell banks. (b) collect sufficient information about the customer institution to fully understand the nature of that customer business and thus be able to determine the extent to which the customer institution's business exposes the correspondent institution to a higher risk of money laundering. To that end, steps should be taken to understand and assess the risk as to the nature of the customer institution's client base and the type of activities that the customer institution will carry out through the correspondent account or, where applicable, the type of crypto-assets for which the CASP client institution will transact through the correspondent account; (c) determine, on the basis of publicly available information, the reputation of the institution and the quality of the supervision to which it is subject, including information in relation to any current or past regulatory or criminal investigation relating to money laundering or terrorist financing and/or any supervisory measures imposed on the customer institution. This means that the correspondent institution shall assess the degree of certainty it can have that the customer institution is adequately supervised for compliance with its anti-money laundering and countering the financing of terrorism obligations. In this regard, correspondents may be assisted in their work by various publicly available sources, such as, for example, the FATF or the Financial Sector Assessment Programme (FSAP) assessments, which contain sections on effective supervision; (d) assess the anti-money laundering and countering the financing of terrorism controls carried out by the customer institution. This means that the correspondent institution is required to carry out a qualitative assessment of the customer institution's anti-money laundering and countering the financing of terrorism control framework, and not only to obtain the relevant policies and procedures on anti-money laundering and countering the financing of terrorism of the customer institution. That assessment should include the tools to monitor the transactions used by the customer institution in order to ensure that they are appropriate to the type of business carried out by the customer institution. This assessment must be duly documented. In accordance with the risk-based approach, where the risk is particularly high and, in particular, where the volume of correspondent transactions is significant, the correspondent institution should consider carrying out on-site visits and/or spot checks to ensure that the customer institution's anti-money laundering policies and procedures are effectively implemented; (e) obtain approval from senior management before establishing new correspondent relationships. The senior manager responsible for granting approval must be different from the officer recommending the establishment of the relationship, and the higher the risk associated with that relationship, the higher the hierarchical position must be held by the senior manager responsible for granting approval. Correspondent institutions shall keep their senior management informed of their high-risk responsive relationships and the measures they take to manage risk effectively;

		(f) document the responsibilities of each customer institution. Where the standard contract does not already contain such an arrangement, correspondent institutions shall conclude a written contract specifying, inter alia, at least the following matters: (i) the products and services provided to the customer institution; (ii) how this correspondent service and its beneficiary can be used (e.g. whether it can be used by other banks or financial institutions through their relationship with the customer institution), as well as the responsibilities to prevent money laundering and terrorist financing of the correspondent institution; (iii) how the correspondent institution will monitor the relationship in order to verify that the customer institution is fulfilling its obligations under that contract (e.g. through ex-post monitoring of the transaction); (iv) the information that should be provided by the customer institution at the request of the correspondent institution (in particular for the purpose of monitoring the business relationship) and a reasonable timeframe within which that information should be provided (taking into account the complexity of the correspondent institution's payment or chain). (g) for payable through accounts and nesting accounts, ensure that the customer institution has verified the identity of the client and applies ongoing customer due diligence that has direct access to the correspondent's accounts, and that it can provide customer due diligence data at the request of the correspondent institution. Correspondent institutions shall seek to obtain confirmation from the customer that the relevant data can be transmitted by the customer to the correspondent upon request.
Correspondent relationships involving high-risk third countries or with a customer institution from a high-risk third country	49.	(1) Obliged entities (correspondent institutions) when establishing correspondent relationships from a third country, must specify which of their relationships concern a high-risk third country, identified in Article 2 of the Law. (2) Correspondent institutions shall also, as part of their due diligence measures, determine the likelihood of initiating transactions by the customer institution involving high-risk third countries, including where a significant proportion of the customer institution's customers have relevant professional or personal links with high-risk third countries. (3) In order to fulfil their obligation under Article 64(1)(a) of the Law, correspondent institutions must ensure that they also apply Articles 61 and 64(1)(b) of the Law. (4) In order to fulfil their obligations laid down in Article 64(1)(a)(iii) of the Law, correspondents must apply paragraph 48(2)(d) above and ensure that the adequacy of the policies and procedures of the customer institution for identifying the source and wealth of their clients is assessed, carry out on-site visits or sample checks, or request the customer institution to provide them with evidence of the legitimate origin of the source of wealth or source of funds of the respective client. (5) In the event that the Central Bank of Cyprus invites obliged entities to apply additional measures in accordance with Article 59(13) of the Law, correspondent institutions must apply, as appropriate, one or more of the following measures: (a) increasing the frequency of reviewing the information and due diligence measures relevant to the customer institution as well as the risk assessment for that customer institution; (b) applying to the customer institution for a more in-depth assessment of the customer institution's anti-money laundering and countering the financing of terrorism controls. In such cases of higher risk, correspondents shall consider reviewing the independent audit report on anti-money laundering and countering the financing of terrorism controls of the customer institution, conducting interviews with Anti-Money Laundering Compliance Officers, outsourcing a review to third parties or conducting an on-site visit. (c) requesting increased and more intrusive monitoring. Real-time monitoring of transactions is one of the due diligence measures that correspondents should consider in cases of a particularly high risk of money laundering and terrorist financing. In this context, correspondents shall consider an ongoing dialogue with the customer institution to improve the understanding of the risks associated with the correspondent relationship and to facilitate the rapid exchange of material information, where necessary. (d) requesting increased monitoring of the transfer of funds in order to ensure the identification of missing or incomplete information on the payer and/or the payee

		under Regulation (EU) 2023/1113 and in accordance with EBA Guidelines on travel rules, under Article 36 of Regulation (EU) 2023/1113. (e) limitation of business relationships or transactions involving high-risk third countries, in terms of nature, volume or means of payment, following a thorough assessment of the residual risk posed by the correspondent relationship.
Transactions or business relationship with high-risk third countries	50.	(1) With regard to business relationships or transactions involving high-risk third countries as defined in Article 2 of the Law, countries allegedly associated with terrorist financing and high-risk countries with significant strategic weaknesses in the area of money laundering and terrorist financing that have been announced by the Financial Action Task Force (FATF), and for which specific actions are required, obliged entities must ensure that they apply, at least, the enhanced due diligence measures provided for in Article 64(1)(a) of the Law, and, where applicable, the measures provided for in Article 59(13) of the Law. (2) Obliged entities must apply the measures referred to in the above paragraph and adjust the extent of the measures according to the level of risk.
		(3) A business relationship or transaction shall be deemed to be related to a high-risk third country if at least one of the following applies: (a) the funds were generated in a high-risk third country; (b) the funds are received from a high-risk third country; (c) the destination of the funds is a high-risk third country; (d) the obliged entity deals with a natural person or legal entity resident or established in a high-risk third country; (e) the undertaking deals with a trustee established in a high-risk third country or with a trustee arrangement governed by the law of a high-risk third country. (4) Increased due diligence measures, as provided for in Article 64(1)(a) of the Law and, where applicable, Article 59(13) of the Law, shall apply where the obliged entity considers that: (a) the transaction is executed through a high-risk third country, e.g. because the intermediary payment service provider has an establishment in such a country; or (b) the beneficial owner of the customer resides in a high-risk third country. (5) Without prejudice to the requirements of subparagraphs (1), (2) and (4) above, obliged entities shall carefully assess the risk associated with business relationships and transactions in which: (a) the customer is known to have close personal or professional links with a high-risk third country; or (b) the beneficial owner(s) is known to have close personal or professional links with a high-risk third country. In such cases, obliged entities must decide, on a risk-sensitive basis, whether or not to apply the measures provided for in Article 64(1)(a) of the Law, i.e. enhanced due diligence measures or standard due diligence measures.
Crypto-asset service providers not regulated and supervised under Regulation (EU) 2023/1114	51.	(1) Where a business relationship is established and maintained with a customer that is a crypto-asset service provider and is not regulated or supervised under Regulation (EU) 2023/1114, obliged entities may be exposed to increased risk. Therefore, they are required to carry out the money laundering and terrorist financing risk assessment related to that customer before entering into a business relationship. In doing so, obliged entities shall also take into account the money laundering and terrorist financing risk associated with the type of crypto-assets provided or serviced by that provider. As a minimum, obliged entities shall apply the following enhanced measures and procedures, in addition to the due diligence measures and procedures for identifying customers and final beneficiaries set out in the Law and in this Directive: (a) hold a discussion with the customer in order to understand the nature of the business and the money laundering and terrorist financing risks to which they are exposed; (b) in addition to verifying the identity of the customer's beneficial owners, apply due diligence measures towards senior management to the extent that they differ, including consideration of any negative information; (c) understand the extent to which that customer applies its own due diligence measures to its clients either on the basis of a legal obligation or on a voluntary basis; (d) determine whether the customer is registered or authorised in an EU/EEA Member State, or in a third country, and, in the case of a third country, examine the adequacy of the regulatory and supervisory regime to prevent money

		laundering and terrorist financing of the third country in accordance with paragraph 2.11 of the EBA Risk Factor Guidelines ; (e) determine whether the services provided by the customer fall within the scope of the customer's registration or authorisation; (f) determine whether the customer provides services other than those for which it is registered or authorised as a credit or financial institution; (g) where the customer's business involves issuing crypto-assets to raise funds, such as Initial Coin Offerings (ICOs), obliged entities shall determine whether that business is conducted in accordance with applicable legal requirements and, where applicable, whether it is regulated for the purposes of preventing money laundering and terrorist financing in accordance with internationally agreed standards, such as those published by the Financial Action Task Force (FATF).
Monitoring the business relationship, accounts and transactions	52.	(1) Subject to the provisions of Article 61(1)(d) of the Law, obliged entities must apply customer due diligence measures, including continuous monitoring of the business relationship. This includes, but is not limited to: (a) scrutinizing the transactions carried out in the course of the business relationship to ensure that the transactions executed are consistent with the customer's data and information held by the obliged entity, his/her economic profile, risk profile, and where necessary, on the origin of funds, in order to detect unusual or suspicious transactions; and (b) updating the documents, data or information available to the obliged entity, in accordance with the requirements of paragraph (25) of this Directive, in order to understand whether the risk associated with the business relationship has changed and to verify whether the information underlying the ongoing monitoring is accurate. (2) Identification procedures and customer due diligence measures are in place when negative information about the customer, his/her transactions or activities has been detected in the press or online or requests for information have been made by a competent authority or MOKAS or the Police, or another financial institution. In such a case, the obliged entity must carry out an investigation and assessment as soon as possible and take appropriate measures. The results of the survey must be archived and if any findings are deemed significant, then the Central Bank of Cyprus shall be informed.
		(3) As a minimum, an effective system for monitoring the business relationships of the obliged entity, including transactions, shall achieve the following: (a) the periodic audit of the customer database to identify politically exposed persons and other higher-risk accounts or business relationships. Therefore, the management information systems of obliged entities must be able to produce detailed statements for each group of high-risk customers in order to assist them in monitoring their accounts and transactions; (b) the detection of complex or unusually large transactions, or unusual patterns of transactions carried out with no apparent economic or clear legitimate reason or suspicious transactions incompatible with customer's economic profile for the purposes of further investigation; (c) the identification of transactions that may be linked to terrorist financing; (d) the creation of alerts/alerts for suspicious or unusual transactions, according to the parameters and scenarios set; (e) investigation of unusual or suspicious transactions by relevant members of staff assigned to this task. The results of the investigations must be recorded in a separate note and be readily available for inspection; (f) taking all necessary measures and actions on the basis of the findings of the investigation, including internal reporting of suspicious transactions/activities to the Anti-Money Laundering Compliance Officer; (g) the identification of the source and origin of funds credited to accounts in relation to the customer's economic profile; (h) the verification of the obliged entity's clientele and transactions against the lists of persons or entities subject to restrictive measures adopted on the basis of relevant European Union Regulations and United Nations Security Council Resolutions. The audit is carried out in real time at the beginning of the business relationship or during the execution of the transaction, always in accordance with the requirements of the CBC Directive on Compliance with the Provisions of the UN Security Council Resolutions and the Decisions and Regulations of the Council of the European Union;

Central Bank of Cyprus Directive on Compliance with the Provisions of the UN Security Council Resolutions and the Decisions and Regulations of the Council of the European Union 31/03/2020		(i) the periodic review of the obliged entity's clientele to identify any negative information about their customers or other persons associated with them. (4) Obliged entities must ensure that their transaction monitoring approach and procedures are appropriate, effective and meet the requirements of Regulation (EU) 2016/679. (5) The choice of appropriate measures shall depend on the nature, size and complexity of the business of the obliged entity and the risk to which it is exposed. Obliged entities are required to adjust the intensity and frequency of monitoring in line with the risk-based approach. In all cases, obliged entities shall determine: (a) which transactions will be monitored in real time, as well as which transactions will be monitored retrospectively. In doing so, obliged entities are required to determine: (i) which high-risk factors, or which combination of high-risk factors, always trigger real-time monitoring; and (ii) which transactions associated with a higher risk of money laundering and terrorist financing are monitored in real time, in particular where the risk associated with the business relationship is already increased. (b) whether to monitor transactions manually or use an automated transaction monitoring system. Obliged entities processing large volumes of transactions, or high-frequency transactions, shall implement an automated transaction monitoring system. It is understood that the use of automated monitoring methods does not eliminate the need for an obliged entity to remain vigilant, since factors such as staff intuition/crisis, direct contact with a customer and the ability, through experience, to identify transactions and activities that do not appear to be meaningful cannot be fully automated; (c) the frequency of the monitoring of transactions, taking into account the requirements of this Directive; and (d) whether it is necessary to use advanced analytical tools, such as distributed ledger or blockchain analytics, based on the money laundering and terrorist financing risk associated with the business of the undertaking and the individual transactions of the obliged entity's customers. (6) In addition to real-time monitoring and ex-post monitoring of transactions, and regardless of the level of automation used, obliged entities shall regularly carry out ex-post sample checks on already processed transactions in order to identify trends that they could use in the risk assessment process, perform checks and, if necessary, subsequently improve the reliability and appropriateness of the transaction monitoring system. Obliged entities shall also use the information obtained under paragraphs 19(16) and 19(17) of this Directive to monitor and improve the transaction monitoring system. (7) An effective transaction monitoring system, based on up-to-date customer information, must enable the obliged entity to identify transactions that are outside the usual form of account movement, or that are complex or unusual transactions, or that are carried out without an obvious economic purpose or a clear legitimate reason. Obliged entities must ensure that they have procedures in place to investigate such transactions without undue delay.
		(8) Transaction monitoring can be done by reference to specific types of transactions, the customer's economic profile, the customer's usual turnover/activities, and by comparing at regular intervals the movement of the account or transactional behavior with the expected movement, as declared at the beginning of the business relationship as well as with the movement of the account and the nature of the transactions carried out by other customers active in the same field of business. Significant discrepancies must be further investigated and the findings must be recorded electronically or in a separate note, which is recorded in the customer's file. It is understood that the obliged entity, for cases registered electronically, must be able to identify/produce at any time customer lists for all cases investigated for the specific customer, fully ensuring the audit trail. (9) Transaction monitoring systems must be able to aggregate the balances and movements of all connected accounts on a consolidated basis and detect unusual or suspicious types of transactions and activities. This can be done by setting limits for a specific type or category of accounts (e.g. high-risk accounts) or transactions (e.g. cash deposits or withdrawals, incoming and outgoing remittances above a predetermined threshold, etc.), taking into account the customer's economic profile, country of origin, source and destination of the money, counterparties, type of transaction or other risk factors. Particular attention must be paid to transactions

		above predefined thresholds. If accounts are not maintained, transactions are tracked based on an identity card/passport or a separate identification number for each customer.
		(10) Furthermore, monitoring procedures shall cover customers who do not have direct contact with the obliged entity, dormant accounts that suddenly move, or dormant customers who suddenly want to resume a business relationship, unusual transactions carried out through cash machines, etc. It is also necessary to monitor cash transactions whether they are carried out in a single transaction or in several linked transactions. (11) Electronic management information and management systems must also be used to extract information in relation to missing elements of the customer's identification and economic profiling documents, account opening documents, and overall information on the customer's business relationship with the obliged entity. (12) The monitoring system put in place by each obliged entity must, inter alia, be capable of producing information, statistical and exemption reports, both for each individual customer and for categories of customers with common characteristics. Such data must be used to identify, analyse and effectively monitor the trading behaviour of customers and/or their accounts and transactions, on the basis of their calculated risk of involvement in money laundering and terrorist financing. (13) Obliged entities must monitor those statistics at regular intervals, on a risk-sensitive basis, and apply additional due diligence measures where necessary.
		(14) In accordance with the principle of proportionality, the obliged entity shall ensure that an effective monitoring system is in place that meets its needs and is capable of detecting unusual activity. The effectiveness of this system depends on the appropriateness of the parameters and criteria set by the obliged entity for generating warning messages (alerts), as well as on the ability of its staff to properly understand and assess these messages and to take appropriate action where and when required. It is important to have a balance in the number of warning messages. A large number of "false positive" messages may require disproportionate resources to investigate, while a small number of messages may entail an increased risk of undetected suspicious transactions. In any case, the obliged entity must set out in writing the parameters, criteria and any limits it has set for the production of the warning messages. (15) Notwithstanding the above, the determination of parameters, criteria, and thresholds for the generation of warning messages must be based on the assessment of money laundering and terrorist financing risks of the obliged entity and the specific risks faced by the obliged entity. Furthermore, they must be updated periodically to reflect any changes in laws and directives, as well as to take into account any other information the obliged entity deems relevant. (16) The obliged entity shall ensure that its staff responsible for monitoring and investigating warning messages receive appropriate and adequate training to that end. (17) For warning messages that cannot be justified, the procedure laid down in Part 12 of this Directive must be followed. (18) Account and transaction monitoring procedures shall include, inter alia, measures to monitor (e.g. audit trail) warning messages and ensure that they are properly managed. (19) In order to ensure the correct and effective application of the procedures for the examination and investigation of warning messages, obliged entities, depending on the size and nature of their operations, shall apply the 'four eyes principle'. (20) By way of derogation from the above obligation, obliged entities must adopt the following internal control measures in the event of non-application of the principle of control by a second person: (a) use of technological solutions; (b) categorisation of warning messages into high-risk and low-risk; (c) spot checks by a second person; (d) a documented risk assessment supporting the processes that an obliged entity intends to implement. (21) The management of warning messages must be subject to control by the Anti-Money Laundering Compliance Officer and the Internal Audit function. (22) Obliged entities shall ensure that the data stored in their computerised systems or databases are accurate and valid to ensure that the data flowing through the

		electronic systems for the purposes of monitoring accounts and transactions are complete and accurate. (23) The obliged entity shall assess the transaction and account monitoring system at least every year or earlier if it deems it appropriate. The assessment shall include, inter alia, checking the correctness of sources of information, management and management supervision, policy, procedures and controls, its effectiveness in identifying money laundering and terrorist financing risks. (24) Obliged entities shall ensure that their resources, both in terms of human resources and technology, are sufficient for the proper and timely examination and investigation of warning messages.
		PART 8 CASH TRANSACTIONS
General requirements	53.	(1) Subject to the provisions of Article 58(d) of the Law, obliged entities shall apply appropriate procedures and controls for cash transactions for amounts equal to or greater than EUR 10.000 or their equivalent in foreign currency. In particular, obliged entities shall, depending on the calculated risk, exercise control to establish: • the source and origin of the cash; • the purpose and destination of the money; and • whether the amount and nature of the transaction is consistent with the customer's activities/tasks and economic profile. (2) Furthermore, and subject to the limits and controls set by the obliged entity, appropriate documentary evidence and evidence of the economic, commercial or other purpose of the cash transaction shall be obtained and, where necessary, authorisation to execute the transaction shall be obtained from an appropriate higher authority of the obliged entity. (3) Similar checks must be carried out for cash transactions below EUR 10.000 or the equivalent in foreign currency where there are suspicions that the transaction is related to money laundering or terrorist financing.
Requirements to execute a cash transaction imported from abroad	54.	(1) Obliged entities shall be prohibited from accepting cash of a value of EUR 10.000 or more or the equivalent in foreign currency imported from abroad where: a) they are not accompanied by the relevant import declaration to the Customs and Excise Department ("Declaration of cash") pursuant to Regulation (EU) 2018/1672 and Law (Law 63(I) of 2022); or b) the import declaration contains incomplete, false or untrue information.
		(2) For the transactions referred to in subparagraph (1) above, the obliged entities shall receive and file with the transaction the original of the relevant import declaration. (3) Obliged entities must immediately inform the Customs and Excise Department of all cases in which they have refused a transaction for the reasons set out in subparagraph (1) above.
Cash transactions in foreign currency of EUR 100.000 or more	55.	(1) An individual cash transaction in foreign currency imported into Cyprus from abroad, by any person, with a value equal to or greater than the equivalent of EUR 100.000, is accepted only with the written approval of the Anti-Money Laundering Compliance Officer of the obliged entity.
		(2) Furthermore, the execution of foreign currency cash transactions on a continuous and regular basis, which cumulatively exceed or are expected to exceed the equivalent of EUR 100.000, within the same calendar year, by any person, shall be accepted only with the written approval of the Anti-Money Laundering Compliance Officer of the obliged entity. (3) Depending on the level of risk posed by the transaction or business relationship, the obliged entity shall assess the existence of connected persons and, where necessary, apply appropriate due diligence measures.
		(4) Applications for acceptance of foreign currency cash transactions referred to in subparagraphs (1) and (2) above must be submitted in writing to the Anti-Money Laundering Compliance Officer by the competent officials of the obliged entity who will execute the transaction and shall be accompanied by: • full details of the customer, • its activities; • the nature and purpose of the transaction; and • the source of the cash.

		For customers intending to carry out such transactions on a continuous and regular basis, copies of their most recent annual audited accounts or management accounts shall be submitted in addition to the above, where there is no obligation to prepare annual audited accounts.
		(5) After examining the transaction and the relevant information submitted, the Anti-Money Laundering Compliance Officer approves or rejects the transaction. The Anti-Money Laundering Compliance Officer shall keep a separate file with the above requests, the accompanying data and documents and his/her decision. The above are also kept in the customer's file.
		(6) The Anti-Money Laundering Compliance Officer must ensure, before giving his written approval, that the transaction is consistent with the financial situation and cash flow of the customer's business and other activities. Furthermore, the Anti-Money Laundering Compliance Officer shall ensure that the customer due diligence and identification procedures, as provided for in Part 7 of this Directive, have been fully implemented and that the cash does not originate from illegal activities.
		(7) The Anti-Money Laundering Compliance Officer must keep separate registers for customers involved in: (i) individual cash transactions, and (ii) cash transactions on a continuous and regular basis.
		(8) The Anti-Money Laundering Compliance Officer monitors, at least on a monthly basis, the volume of foreign currency cash transactions carried out by customers for whom he has given written approval. In this context, the Anti-Money Laundering Compliance Officer prepares a monthly analytical statement with data on customers carrying out foreign currency cash transactions during the reference month, as well as accumulated deposits, for the period from the beginning of the year to the end of the reference month.
Exempted cash transactions	56.	The provisions of paragraphs 53, 54 and 55 above shall not apply in the following cases: (i) Deposits of foreign currencies in cash by the Government of the Republic. (ii) Cash deposits of foreign currencies by semi-governmental oganisations in Cyprus. (iii) Cash deposits of foreign currencies from other credit institutions operating in Cyprus.
		PART 9 CENTRAL CONTACT POINT
General requirements	57.	(1) Subject to the provisions of Article 70A of the Law, electronic money issuers and payment service providers whose head office is in another Member State of the European Union and which are established in Cyprus and operate through a representative shall designate a central contact point on the basis of the criteria laid down in Article 3 of Commission Delegated Regulation (EU) 2018/1108. (2) The central contact point shall be responsible for ensuring, on behalf of the electronic money issuer and/or the payment service provider, compliance with the provisions of the Law and the relevant instructions issued by the Central Bank of Cyprus to prevent money laundering and terrorist financing and for facilitating supervision by the Central Bank of Cyprus, including by providing documents and information at its request. (3) In addition to the obligations arising from Articles 4 and 5 of Commission Delegated Regulation (EU) 2018/1108, the central contact point must apply the provisions of Article 6 of the above-mentioned Delegated Regulation and keep a record of the suspicious transaction or activity reports it sends to MOKAS, in accordance with the requirements of Part 12 of this Directive. (4) In any case, e-money issuers and payment service providers whose head office is located in another Member State remain responsible for their compliance with the Cypriot legal and regulatory framework. (5) Taking into account the principle of proportionality, electronic money issuers and payment service providers which have their head office in another Member State and are established in the Republic and operate through an agent may determine the form of the central contact point, and shall demonstrate to the Central Bank of Cyprus that: (a) their resources in both human resources and technology are sufficient to enable the central contact point to fulfil its tasks, taking into account the extent of the network, the number and volume of transactions carried out in Cyprus, the level and risk factors in relation to money laundering and terrorist financing related to the activities carried out in Cyprus; and (b) the format of the central contact point is appropriate to manage the above-

		mentioned resources in an adequate and consistent manner. (6) The central contact point must have the capacity, knowledge and expertise to prevent money laundering and terrorist financing.
		PART 10 RELATIONSHIP WITH AGENTS
General requirements	58.	(1) An obliged entity licensed in Cyprus, which enters into agreements with other parties acting as its agents, shall establish and maintain appropriate anti-money laundering and countering terrorist financing policies and procedures to address the risks that the agents undertake or may undertake. (2) Obliged entities must implement procedures for the assessment of agents prior to entering into a business relationship, taking into account at least the following: (a) the agent applies internal measures and controls to ensure compliance with the Law and EU Regulation 2023/1113; (b) there are no indications that money laundering or terrorist financing is being or has been attempted or committed in connection with the intended engagement. (3) The obliged entity shall apply identification and due diligence measures to agents with whom it will enter into an agreement, as well as to the person owned or controlled by the agent, where the agent is a legal person, in order to ensure that the obliged entity does not increase the risk of money laundering and terrorist financing to which the obliged entity is exposed by cooperating with that agent. (4) The obliged entity shall obtain appropriate information, data, and documents in order to be satisfied as to the suitability and integrity of the directors and other persons responsible for the management of the agent, including by examining the honesty, integrity and reputation of those persons. In order to establish the above, the investigation carried out by the obliged entity must be proportionate to the nature, complexity and scale of the risk inherent in the services provided by the agent and for which the agent applies due diligence procedures as set out in the obliged entity's procedures and policies. (5) The obliged entity shall empower the agent to act on its behalf and shall remain responsible for the agent's actions. The above, however, does not exempt the agent from his legal obligations to comply with the Law. (6) The obliged entity shall enter into a contract with the agent setting out the roles and responsibilities of each party. The agreement shall make explicit reference to the policies and procedures relating to the legal and regulatory framework for the prevention of money laundering and terrorist financing. (7) The obliged entity shall keep an up-to-date register of representatives in which, inter alia, it shall record details of: • the shareholder structure of the agent; • members of its management body; • the address of the administrative offices; and • the addresses from which it provides products and services of the obliged entity. (8) The obliged entity must: (a) implement continuous and appropriate monitoring of customers and agent transactions. These include on-site visits to the agent's offices/facilities, where the obliged entity assesses the agent's level of compliance with the obliged entity's policies and procedures, as set out in the contract between them, as referred to in subparagraph (6) above; (b) ensure that the internal controls carried out by the agent in relation to the prevention of money laundering and terrorist financing are appropriate and remain appropriate throughout the duration of the agency relationship; (c) examine the nature and volume of transactions carried out by the agent and its location in order to identify cases where the agent is exposed to higher risk. In such cases, the obliged entity shall carry out more frequent on-site visits and carry out more intensive monitoring and record them in a register; (d) ensure that the agent understands the importance of identifying and reporting suspicious transactions and activities to the obliged entity's Anti-Money Laundering Compliance Officer; (e) ensure that the agent understands the risks involved in the use of cash and that cash transactions can be carried out to launder money and/or finance

		terrorism. They shall also ensure that cash transactions are properly managed; (f) ensure that the agent promptly takes corrective action to address any deficiencies identified by the obliged entity. The obliged entity itself may take corrective measures or even terminate the contract with the agent, terminating the cooperation between them. (9) The obliged entity shall provide anti-money laundering and counter-terrorist financing training and education to delegates to ensure that delegates have an adequate understanding of the associated risks, and perform quality controls to prevent money laundering and counter terrorist financing, in accordance with the obliged entity's policies and procedures and requirements.
		PART 11 RECORD KEEPING PROCEDURES
Certification and language of documents 50/1972 6(III)/2005	59.	(1) Obliged entities shall obtain and keep documents and identification of the customer and beneficial owner in one of the following formats, when initiating a business relationship or executing an individual transaction: (a) originals, or (b) a true copy of the original, where the certification is made by the official or representative of the obliged entity carrying out the identification, after the original has been presented to him. Such certification must bear the name and signature of the person certifying the document and the date of certification; or (c) a true copy of the original, where the certification is made by a third person, on which the institution relies for the purposes of customer identification pursuant to Article 67 of the Law and the provisions of paragraph 29 of this Directive. The certification must be dated, signed and stamped by the third person on whom the obliged entity relies for customer identification purposes, or (d) in the case of non-Cypriot citizens and/or legal persons or entities incorporated outside Cyprus, original documents bearing the "Apostille" stamp, in accordance with the Convention on the Abolition of the Obligation to Legalise Foreign Public Documents (Hague Convention), bearing the distinguishing serial number assigned by the central authority in the country of issue. The obliged entity, after having seen the original documents, may keep true copies of those documents in the customer's file. Such copies must be certified by an official of the obliged entity and bear the name and signature of the official of the obliged entity certifying the documents as well as the date of certification; or (e) a true copy of the original, where the certification has been made by a government department or an independent authority competent to provide such a service; or (f) copies of documents retrieved from the obliged entity itself or through a commercial provider, from the website of the Registrar of Companies or equivalent competent authority of the European Economic Area or a third country assessed by the obliged entity as low-risk taking into account the EBA Risk Factors Guidelines and Annex II to the Law. In such a case, information shall be kept on the source, date and person who has retrieved that information, or is responsible for its authentication, whether or not that person is a member of staff of the obliged entity; or (g) in the case of a remote customer, the obliged entity complies with the EBA Guidelines on the use of remote customer identification solutions. (2) Where an update of the identity information is carried out, the obliged entity shall decide, depending on the money laundering and terrorist financing risk of each individual business relationship, whether the updated information or documents shall be in one of the formats referred to in subparagraph (1) or whether they shall be copies of the originals, taking into account that there are no other risk factors that require the presentation of the original or a true copy. Where a copy of a document is obtained, the obliged entity must assess whether it is necessary to implement additional risk-appropriate control measures and procedures in order to ensure the accuracy and validity of the updated information and to limit the risk of money laundering and terrorist financing. (3) Documents and particulars received by the obliged entity in accordance with subparagraphs (1) and (2) above, which are in a language other than Greek or English, must be accompanied by a document in Greek or English stating that it is a faithful translation of the original. This document must be dated and signed by the duly authorised person (e.g. a certified translator or staff of the obliged entity with appropriate training, or a mother tongue or university degree in that language) who

		carried out the translation.
Data format	60.	(1) Records, including the data and documents referred to in this Directive, to the extent that they concern personal data in compliance with the requirements of Regulation (EU) 2016/679 may be kept in paper or electronic form, provided that they can be retrieved in a timely manner and without delay and the obliged entity is able to provide the above information at any time to the Central Bank of Cyprus or MOKAS, at their request. (2) The documents may be kept in electronic form, provided that the obliged entity uses an electronic system which complies with the following: (a) automatically records data allowing the obliged entity to identify the person who has scanned the document; (b) automatically record the date and time of scanning of the document; and (c) it has appropriate safeguards which make it impossible to modify or alter the document or information referred to in points (a) and (b) above. (3) The obliged entity shall establish policies and procedures for keeping records and documents, taking into account the requirements of the Law, this Directive and Regulation (EU) 2016/679.
Submission of information to MOKAS	61.	Subject to the provisions of Articles 68 and 68B of the Law, obliged entities shall ensure that, within the framework of an investigation into a suspicious transaction or the activities of a client, they are able to provide, in a timely manner and without delay, information and copies of the following: (a) the identity of the customer or the person who carries out the transaction; (b) the identity of the beneficial owners of the customer in case of a legal entity; (c) the identity of the beneficial owners for whose benefit the transaction is carried out and the identities of the persons acting on behalf of or entitled to act on behalf of those persons; (d) details of the volume and amount of transactions entered into by the persons referred to in points (a), (b) and (c) above; (e) any connected accounts; (f) in relation to specific transactions and where applicable: (i) the date of the transaction; (ii) the source of funds; (iii) the currency and amount of the transaction; (iv) how the money has been transferred, deposited or withdrawn, i.e. cash, cheques, electronic transfers, etc.; (v) the destination of funds; (vi) the nature of the instructions and authorisation given; and (vii) the type and number of the transaction account or the cheque or card number, etc. g) any other information or document deemed necessary or requested by MOKAS.
Electronic transfers of funds Regulation (EU) 2023/1113	62.	(1) Obliged entities are required to comply with the EBA Guidelines on travel rules under Article 36 of Regulation (EU) 2023/1113 when implementing their obligations under that Regulation and this Directive. In this context, obliged entities shall implement the necessary measures to identify missing or incomplete information on the payer or the payee as well as appropriate procedures for the management of transfers of funds that are not accompanied by the required information. (2) The obliged entity, acting (a) as payment provider of the payee in accordance with Article 8(2) of Regulation (EU) 2023/1113; or (b) as an intermediary payment service provider in accordance with Article 12(2) of the above-mentioned Regulation. it must report to the Central Bank of Cyprus the cases where the payment service provider repeatedly fails to provide any of the required information on the payer or the payee, as well as the measures taken in accordance with the requirements of Regulation (EU) 2023/1113 and the above-mentioned EBA Guidelines.

		PART 12 RECOGNITION AND REPORTING OF SUSPICIOUS TRANSACTIONS/ACTIVITIES
Identification and reporting of suspicious transactions and activities	63.	(1) Obliged entities shall, at all times, ensure that they are in possession of sufficient information, that they have built up a substantial economic profile and that they are aware of the activities of their customers to enable them to identify in a timely manner that a transaction or series of transactions, or activity, is unusual or suspicious.
		(2) Obliged entities, in addition to identifying suspicious transactions related to money laundering, shall ensure that they have in place appropriate procedures, controls and infrastructure to detect transactions that may be related to terrorist financing.
		(3) Obliged entities shall ensure that they have adequate and up-to-date information about their customers and their economic activities, as well as appropriate procedures in place to enable them to identify transactions that may be linked to terrorist financing. As such transactions often involve small amounts that are not easy to detect in a timely manner, obliged entities must be able to identify cases where a single transaction, a series of connected transactions or unusual trading behaviour may be related to terrorist financing. In addition, they must take into account that terrorist financing is mainly linked to the final destination of the funds, since their source of funds and origin may originate from legitimate activities.
Examples of suspicious transactions and activities Annex III	64.	(1) Obliged entities must consult the Third Annex to this Directive, which provides indicative examples of suspicious transactions/activities that could be linked to money laundering and terrorist financing.
		(2) The list in Annex III is not exhaustive, nor does it contain all types of transactions likely to be used by persons seeking money laundering and terrorist financing. Obliged entities need to adapt to situations and identify possible new ways that can be used by these persons. (3) Any identification of similar transactions to those provided in Annex III shall be the subject of further investigation and the cause of seeking additional information and/or explanations as to the source and origin of the money, the nature and economic/commercial purpose of the transaction, and the events associated with the specific activity.
Internal reporting of suspicious transactions and activities First Annex Second Annex	65.	(1) Subject to the provisions of Articles 26 and 58(c) of the Law, obliged entities shall ensure that all members of their staff are aware and know their legal obligations, as well as the person, i.e. the Anti-Money Laundering Compliance Officer, to whom they will report their knowledge or suspicion of persons who appear to be involved in money laundering or terrorist financing offences, and the information that came to their attention in the course of their employment or profession. (2) The submission of an Internal Suspicion Report must be made on a special form, which is easily accessible to the staff of the obliged entity. An indicative internal reporting form is set out in Annex I to this Directive ("Internal Report on Suspicion of Money Laundering and Terrorist Financing"). (3) All "Internal Suspicion Reports on Money Laundering and Terrorist Financing" shall be archived and kept in a separate file, under the safe custody of the Anti-Money Laundering Compliance Officer. Provided that where such reports are kept in electronic form, obliged entities must have a system in place to enable them to produce such suspicion reports in paper form for control purposes. (4) As part of the assessment of the report, among other things, other connected accounts or relationships of the reported customer are considered. These relationships may concern either commercial transactions or partnerships/relationships with other natural persons, such as professional intermediaries, shareholders, authorized signatories, directors, etc. (5) From the moment the Internal Suspicion Report is submitted, all subsequent transactions of the reporting customer, his/her other connected accounts and relationships, as referred to in paragraph (4) above, shall be monitored by the Anti-Money Laundering Compliance Officer. (6) If, as a result of the assessment referred to in subparagraphs above, the Anti-Money Laundering Compliance Officer decides not to disclose the relevant information to MOKAS, then he/she should fully explain the reasons for his/her decision in the "Internal Reporting Assessment of suspicion of money laundering and terrorist financing", which must also be filed in the relevant file. An indicative form of the Internal Suspicion Report Assessment is set out in Annex II.

Suspicion Reports to MOKAS	66.	(1) Subject to the provisions of Article 69 of the Law, the Anti-Money Laundering Compliance Officer shall include in the 'Report of Suspicion to MOKAS' all relevant information concerning the customer, transactions or activities, according to the data in his/her possession.
		(2) All "Reports of Suspicion to MOKAS" must be submitted in accordance with the relevant instructions of MOKAS within a reasonable time. Obliged entities must have a system in place to enable them to produce such suspicion reports on paper for audit purposes.
		(3) Following the submission of the 'Report of Suspicion to MOKAS', the obliged entity may wish to terminate the relationship with the customer in order to avoid any risks arising from the continuation of the business relationship. Subject to the provisions of Article 48 of the Law, obliged entities must exercise particular care and not disclose to the customer that a suspicion report has been submitted against him/her to MOKAS. Therefore, close contact, communication and cooperation with MOKAS is needed to avoid creating any obstacles or difficulties in the conduct of investigations.
		(4) After submitting the 'Report of Suspicion to MOKAS', obliged entities must follow any instructions from MOKAS, in particular as regards the execution or non-execution of a specific transaction, or the maintenance of that account or business relationship.
		(5) Furthermore, following the submission of a 'Report of Suspicion to MOKAS', the business relationship in question, the customer's accounts and any other linked accounts are placed under the close monitoring of the Anti-Money Laundering Compliance Officer.
		PART 13 STAFF TRAINING AND AWARENESS
Staff training and education	67.	(1) Subject to the provisions of Article 58(f) and (h) of the Law, the obliged entity shall implement an appropriate and adequate training and awareness-raising programme for staff who are: (a) relevant to the obliged entity and its business; (b) tailor-made to staff training needs and duties. The staff training and awareness-raising programme shall be updated on a regular basis. (2) The awareness and training of staff must be well thought out, planned and targeted and must take into account the nature and size of the obliged entity's activities, as well as the nature and extent of the money laundering and terrorist financing risks to which it is exposed. Therefore, programmes with a one-size-fits-all or random approach to education are considered not to meet the above-mentioned criteria. (3) In this context, the Anti-Money Laundering Compliance Officer shall oversee the preparation and implementation of a continuous training and education programme to prevent money laundering and terrorist financing. In this regard, in cooperation with other competent departments of the obliged entity (e.g. Human Resources and Training Department, etc.), training and education needs are identified and then an annual training and education programme is prepared and recorded, as appropriate, for members of the management body, staff and their representatives. (4) The Anti-Money Laundering Compliance Officer shall duly inform staff of: (a) the money laundering and terrorist financing risks to which the obliged entity is exposed, including methods, trends, and typologies, as well as the calculated risk approach applied by the obliged entity to mitigate those risks; (b) adopted policies and procedures to prevent money laundering and terrorist financing; (c) how to use automated systems, including advanced analytical tools, to monitor transactions and business relationships, and how to interpret the results generated by such systems and tools; (d) how to identify suspicious and unusual transactions and activities taking into account the specific nature of their products and services, and how to deal with such cases; (e) internal procedures for reporting suspicious transactions or activities; (f) the person acting as Anti-Money Laundering Compliance Officer and his/her responsibilities;

		(g) general policies and procedures regarding whistleblowing; (h) their own individual obligations and responsibilities arising from the Law and this Directive. It is understood that the duties and responsibilities of staff must be recorded in an easily accessible place so that staff can refer to them throughout their employment.
		(5) In addition to the general training, for the purposes of Article 58(f) and (h) of the Law, as well as the above-mentioned requirements, the Anti-Money Laundering Compliance Officer shall assess the training needs within the obliged entity and ensure that adequate theoretical and practical training is provided to the persons most directly involved in dealing with the risks or for whom there is a need for further specialisation, such as: (a) persons working in the Department/Unit/Section of the Anti-Money Laundering Compliance Officer; (b) persons in contact with customers or in charge of carrying out their transactions (e.g. employees, agents, distributors); (c) staff of departments involved in offering specialised services/products; (d) new staff or staff who have been transferred from one department to another. (6) The duration, frequency and content of the training provided to persons with different levels of exposure to money laundering and terrorist financing risks shall be adapted to: (a) on a risk-sensitive basis; (b) according to the needs of the persons/staff and/or representative concerned; (c) any changes and amendments to the relevant legal and/or regulatory framework; (d) changes in the financial system of the country.
		(7) Where the obliged entity adopts a training and awareness-raising programme developed abroad, e.g. by its parent company, the Anti-Money Laundering Compliance Officer shall ensure that this programme is adapted to the Cypriot legal and regulatory framework, as well as to the typologies related to money laundering and terrorist financing, and to the activities of the obliged entity. (8) Where certain training activities are outsourced to a service provider, the Anti-Money Laundering Compliance Officer shall ensure that: (a) the service provider has the necessary knowledge to prevent money laundering and terrorist financing to guarantee the quality of the training provided; (b) the conditions governing such outsourcing shall be determined by means of a written agreement between the two parties; (c) the terms of the above agreement are complied with; and (d) the content of that training shall be adapted to the specific characteristics of the obliged entity itself.
		(9) The Anti-Money Laundering Compliance Officer shall establish evaluation indicators to monitor the effectiveness of the training and education programme and, if he/she identifies weaknesses in its implementation, shall inform the management body and the senior executive management. (10) The Anti-Money Laundering Compliance Officer shall ensure that the obliged entity keeps a record of the training seminars/programmes relating to the prevention of money laundering and terrorist financing which have been attended by the staff and representatives of the obliged entity. The file shall contain, as a minimum, the following information: (a) name of employee/representative per establishment, per position (managerial staff, officials, new entrants, etc.). The list must include all employees/representatives of the obliged entity even if one of them did not attend any seminar; (b) date of participation, title, duration and names of the trainers of the seminar; (c) whether the lecture/seminar was prepared by the obliged entity or by an external organisation or consultants; and (d) summary information on the programme/content of the lectures/seminars.

		PART 14 APPLICATION OF THE DIRECTIVE TO BRANCHES AND SUBSIDIARIES OF OBLIGED ENTITIES
General principles	68.	(1) The obliged entity is required to adapt its internal control framework in line with its activities, its complexity and the associated risks, taking into account the group context. (2) The obliged entity shall ensure that, where the parent company is a credit or financial institution, it has sufficient data and information and is able to assess the group-wide money laundering and terrorist financing risk profile. (3) An obliged entity, which is the parent of a group, shall ensure that: each management body, business area and internal unit, including each internal audit function, shall have the information necessary to carry out its functions. In particular, it must ensure the exchange of adequate information between the business lines and the department/unit/section responsible for preventing money laundering and terrorist financing, as well as the compliance unit, where these are different departments, at group level. Furthermore, it must ensure the exchange of adequate information between the heads of internal control functions at group level and the management body of the obliged entity. (4) An obliged entity which is the parent of a group shall be able to inform the supervisory authorities, on request, of: (a) the process for assessing and managing money laundering and terrorist financing risks; (b) consolidated policies and procedures to prevent money laundering and terrorist financing; and (c) the arrangements of the group for the exchange of information as provided for in subparagraph (3) above.
Role of the management body at group level	69.	(1) The management body of an obliged entity, which is the parent company of a group, shall perform the following tasks: (a) ensure that group entities conduct their own money laundering and terrorist financing risk assessments in a coordinated manner and based on a common methodology in order to have a mapping of the money laundering and terrorist financing risks to which each group entity is exposed. These assessments must reflect the specificities of each of the group entities, and take into account Article 58A of the Law and Part 6 of this Directive; (b) where they are informed by members of the group management body or the member of the management body responsible for preventing money laundering and terrorist financing or directly by the group Anti-Money Laundering Compliance Officer about supervisory activities carried out in the group entities by a competent authority, or deficiencies identified in the course of those supervisory activities, they shall ensure that the remedial actions are completed by the subsidiary or branch in a timely and effective manner.
Organisational requirements at group level	70.	(1) Subject to the provisions of Section 68A of the Law, conflicting interests, i.e. activities that create money laundering and terrorist financing risks, such as commercial operation, between the parent obliged entity and its subsidiaries or branches must not jeopardise compliance with anti-money laundering and terrorist financing requirements and must be mitigated.
		(2) The parent obliged entity must: (a) appoint the member of the management body responsible for preventing money laundering and terrorist financing at the level of the parent undertaking and the group-level Anti-Money Laundering Compliance Officer; (b) establish an organisational and operational coordination structure at group level, with sufficient decision-making powers, in order for the group's management, responsible for anti-money laundering and countering the financing of terrorism matters, to make this position effective in managing and preventing money laundering and terrorist financing risks, in accordance with the principle of proportionality and the Law; (c) approve the internal group-wide money laundering and terrorist financing policies and procedures and ensure that they are consistent with the group structure, size and characteristics of obliged entities belonging to it; (d) set up internal control mechanisms to prevent money laundering and terrorist financing at group level;

		(e) regularly assess the effectiveness of anti-money laundering and countering the financing of terrorism policies and procedures at group level; and (f) for the obliged entity operating branches or subsidiaries in the Republic of Cyprus, or in another Member State or in a third country, appoint the Group Anti-Money Laundering Compliance Officer as coordinator to ensure the implementation of the group policy by all group entities carrying out financial activities, as well as the appropriate and appropriate systems and procedures for the effective prevention of money laundering and terrorist financing.
		(3) The Group Anti-Money Laundering Compliance Officer must fully cooperate with the Anti-Money Laundering Compliance Officer of each group entity.
		(4) The Group Anti-Money Laundering Compliance Officer must perform at least the following tasks: (a) coordinate the undertaking-wide assessment of money laundering and terrorist financing risks carried out locally by group entities and organise the aggregation of their results in order to have a thorough understanding of the nature, intensity and location of the money laundering and terrorist financing risks to which the group as a whole is exposed; (b) assess the potential risks arising from the activity reported by its branches and subsidiaries and, where necessary, assess the risks to the group presented by a particular customer or category of customers. The policies and procedures should enable it to verify whether other branches or subsidiaries have accounts for the same customer (including any related or related parties). The obliged entity shall also have in place policies and procedures governing the relationships of accounts at group level that are considered to be higher risk or that have been associated with potential suspicious activities, including escalation procedures and guidance on limiting the activities of accounts, including the closure of accounts if necessary. The head office of an obliged entity should be able to require all its branches and subsidiaries to search its records against specific lists or lists of persons or organisations suspected of assisting and contributing to money laundering or terrorist financing or the circumvention of financial sanctions, and to report any correspondence; (c) prepare a group-wide money laundering and terrorist financing risk assessment. In this context, the parent company of the group should take into account, in its system for managing money laundering and terrorist financing risks at group level, both the individual risks of the different entities of the group and their possible interactions that could have a significant impact on the risk exposure at group level. In this context, particular attention shall be paid to the risks to which branches and/or subsidiaries of the group established in third countries are exposed, in particular if countries pose a high risk of money laundering and terrorist financing; (d) set standards to prevent money laundering and terrorist financing at group level and ensure that the policies and procedures of each group entity comply with the anti-money laundering and terrorist financing legislation and regulations applicable to each group entity individually and are aligned with the defined group standards; (e) coordinate the activities of the different local Anti-Money Laundering Compliance Officers in the group's operational entities in order to ensure that they operate consistently; (f) monitor the compliance of branches and subsidiaries located in third countries with the provisions of the Cypriot legal and regulatory framework for the prevention of money laundering and terrorist financing, in particular where the requirements for the prevention of money laundering and terrorist financing are less stringent than those set out in the Cypriot legal and regulatory framework and the relevant instructions of the Central Bank of Cyprus. In this regard, it should be ensured that the provisions of Delegated Regulation (EU) 2019/758 are applied; (g) establish group-wide policies, procedures and measures relating, in particular, to data protection and the exchange of information within the group, for the purposes of preventing money laundering and terrorist financing, in accordance with national legal provisions; (h) ensure that group entities have appropriate procedures in place to report suspicious transactions and properly exchange relevant information, including information that a suspicious transaction report has been submitted, without prejudice to national confidentiality rules, where available.

		(5) When preparing and submitting to the management body its Annual Reports in accordance with the requirements of Parts 5 and 6 of this Directive, the Anti-Money Laundering Compliance Officer shall also include matters relating to the group's compliance with regard to the prevention of money laundering and terrorist financing. The Group Anti-Money Laundering Compliance Officer must include in the relevant Annual Reports, at least the following additional information, which he/she receives from the Anti-Money Laundering Compliance Officers of the Group's branches and subsidiaries: (a) consolidated statistics at group level, in particular on risk exposure and suspicious activities; (b) monitoring the inherent risks that have arisen in subsidiaries or branches and the impact on other subsidiaries and branches, and analysing the impact of residual risks; (c) information on supervisory controls, internal or external audits of subsidiaries or branches of the obliged entity, including any significant weaknesses identified in policies and procedures to prevent money laundering and terrorist financing and actions or recommendations for remedial measures; and (d) information on guidance and supervision of subsidiaries and branches, in particular for subsidiaries and branches located in high-risk countries. (e) a brief description of the governance system and the anti-money laundering and countering the financing of terrorism policies and procedures applied at group level. (6) The Anti-Money Laundering Compliance Officer of a subsidiary or branch must have a direct reporting channel with the Group Anti-Money Laundering Compliance Officer. (7) Subject to proportionality criteria, obliged entities should, where appropriate, establish committees in the management body, including the compliance committee.
		PART 15 REPORTING OF DATA, STATEMENT, INFORMATION AND DOCUMENTS TO THE CENTRAL BANK OF CYPRUS
General requirements	71.	(1) Obliged entities are required to submit data and statements when requested by the Central Bank of Cyprus. (2) Provided that obliged entities are required to adapt their automated/electronic systems to enable the reporting of correct, accurate and complete information in those statements and to improve the ability of institutions to identify and monitor transactions and/or business relationships that are considered to pose a higher risk of being interconnected with money laundering and terrorist financing activities.
		(3) The Anti-Money Laundering Compliance Officer must confirm the accuracy of the information sent to the Central Bank of Cyprus, assess it and, where necessary, investigate any trends that may indicate risks of involvement in money laundering or terrorist financing transactions or activities and ensure that he or she is ready to answer questions from the Central Bank of Cyprus.
		PART 16 FINAL AND TRANSITIONAL PROVISIONS
Transitional provisions	72.	Pending procedures or actions or acts initiated pursuant to the Central Bank of Cyprus Directive of February 2019 to credit institutions in accordance with Article 59(4) of the Prevention and Suppression of Money Laundering Activities Laws of 2007 to 2024 and its subsequent amendments, but not completed at the time of entry into force of this Directive, shall be governed by the provisions of the Directive of February 2019 until their completion.
Termination of validity of previous Directives	73.	(1) From the date of entry into force of this Directive, the following Directives shall be repealed: - The Central Bank of Cyprus Directive of February 2019 to credit institutions in accordance with Article 59(4) of the Prevention and Suppression of Money Laundering Activities Laws of 2007 to 2024. - The Central Bank of Cyprus Directive of 2009 on Money Transfer Business of 2009.
Power to issue Directives	74.	(1) In order to achieve the objectives and a better implementation of the provisions of this Directive, the Central Bank of Cyprus may issue general or specific directives to obliged entities, as a whole or individually, which it shall communicate in any way it may specify.

		(2) In particular, and without prejudice to the generality of paragraph (1), the Central Bank of Cyprus may issue directives with a view to adapting the application of specific provisions of the Directive with regard to certain obliged entities, in view of the nature of their activities.
Entry into force	75.	This Directive shall enter into force one month after the date of its publication in the Government Gazette of the Republic.

FIRST ANNEX

INTERNAL SUSPICION REPORT FOR MONEY LAUNDERING OR TERRORIST FINANCING

EMPLOYEE DETAILS

Name: .....Telephone:.....

Branch/Department:.....Fax (if applicable): .....

Title/tasks:.....

CUSTOMER DETAILS

Name: ....

Address:..... .....

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

Telephone:.....Profession:

Fax:.....Employer details: .....

.....

Email:.....

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

Identity number: .....Other identification details: .....

.....

INFORMATION/SUSPECTIONS

Brief description of events/transaction: ....

....

....

Reasons for suspicion:..... .....

....

Signature of employee Date

....

FOR USE BY THE CONFORMITY OPERATOR

Date Download: .....Time of download: ..... Ref. .....

MOKAS briefing: Yes/No .....Information day:..... Ref. .....

SECOND ANNEX

INTERNAL ASSESSMENT OF SUSPICION REPORT FOR MONEY LAUNDERING OR TERRORIST FINANCING =

Reference: ..... Customer details: .....

Official:..... Branch/Department: .....

INVESTIGATIONS CARRIED OUT (Brief description)

.....

.....

.....

ATTACHED DATA AND DOCUMENTS RECEIVED:

.....

.....

.....

ANTI-MONEY LAUNDERING COMPLIANCE OFFICER'S DECISION

.....

.....

.....

DOCUMENT NO.....

ANTI-MONEY LAUNDERING COMPLIANCE OFFICER'S SIGNATURE DATE

....

THIRD ANNEX

EXAMPLES OF SUSPICIOUS TRANSACTIONS/MONEY LAUNDERING AND FINANCING OF TERRORISM

A) MONEY LAUNDERING

(1) Customers who provide insufficient or suspicious information:

a) A customer who is reluctant to provide complete information at the commencement of the business relationship regarding the nature and purpose of his/her business activities, the intended account movement, previous business relationships with institutions, names of directors and advisors, or information about the commercial address of the business. The customer usually provides minimal or misleading information that is difficult or costly for the obliged entity to ascertain.

b) A customer who provides unusual identity documents, the authenticity of which cannot be directly ascertained or which gives rise to suspicion.

c) A customer whose mobile phone number, home or work phone line is disconnected.

d) A customer who carries out frequent or high value transactions, without the existence of any evidence/document for his/her previous or current professional experience or knowledge.

(2) Activities incompatible with the economic profile:

a) The transaction appears to be outside the customer's usual type of transactions and/or the business sector in which the customer operates.

b) Unnecessarily complex transaction in relation to its commercial purpose.

c) The activities of the customer are incompatible with the declared tasks.

d) Sudden change in the nature of the customer's transactions, incompatible with the customer's usual transactions

e) A large volume of bank cheques, payment orders and/or money remittances are credited or transferred from an account and the nature of the customer's business does not justify such activity.

f) A retailer that has a significantly different type of cash deposits from similar businesses in the same region.

(3) Characteristics of customers and their business activities, unusual behavior:

a) Shared address of persons involved in cash transactions, in particular where the address is a commercial location and/or does not appear to be linked to a specific professional activity (e.g. student, unemployed, self-employed, etc.).

b) The declared address appears to be a simple mailing address and not the address at which the undertaking operates.

c) The customer’s declared profession is inconsistent with the amount or type of transactions (e.g. student or unemployed person receiving or sending a large number of remittances or withdrawing cash daily from various locations in a wider geographical area).

d) A safe-deposit box used by a commercial undertaking whose operations are not known or the nature of its operations does not appear to justify the use of a safe-deposit box.

e) Financial transactions by non-profit or charitable organizations for which there is no reasonable economic purpose or connection with the activity of the organization and the other parties to the transaction.

f) Unexplained inconsistencies are found when verifying the identity of the customer (e.g. previous or existing country of residence, country of passport issuance, countries visited according to the passport, documents issued to confirm the name, address and date of birth, etc.)

g) There is unusual nervousness in customer behavior during a transaction.

h) Accounts shall be closed within a very short period of time after they have been opened, in particular after the obliged entity has required the submission of supporting documents.

i) The customer chooses to close the accounts or terminate the business relationship due to negative reports.

j) The customer is accompanied by others, who maintain a low profile.

k) The customer reads a note that apparently he did not write himself.

l) The customer receives instructions from others.

m) The customer does not seem to give convincing information when asked for clarification.

n) The customer requests that the mail be sent to another person's address.

(4) Transactions relating to the acceptance of payment transactions by merchants (merchant acquiring)

a) The declared address appears to be a simple mailing address or another address which is not linked to the commercial activity.

b) The volume of transactions/refunds/return of charges that were declared/carried out are inconsistent with the actual results or with the results of other traders with the same activities and sizes.

c) Products/services of merchants which in some countries/regions are prohibited.

d) Unusual or changing trends in transaction volume and value since the start of the business relationship (e.g. average transaction amount, sales volume, chargebacks and refund rates).

e) Off-standard or excessive volume of cash advances or credit refunds.

f) Lack of activity on an account (e.g. monitoring inactive accounts for possible fraudulent diversions).

g) Fee refund mismatch with transaction types/volumes.

h) Unusual volume of activity, change of address immediately after opening the account or activity other than that declared when opening the account.

i) Indications that a trader's premises are used by third parties.

(5) Cash or other transactions

a) Large cash transactions, which are not justified by the nature and amount of the customer's business.

b) Loans secured by a large cash deposit.

c) Large cash withdrawals from a dormant account or from an account that had recently been credited with a large transfer from abroad.

d) Large cash withdrawal, which is immediately redeposited to another account.

e) Large cash transactions with rounded amounts.

f) Unusually large cash deposits by an individual or company whose business transactions could be carried out by electronic remittances and/or the use of other similar means.

g) Significant increases in cash deposits of any individual or business without reasonable cause, especially the amounts deposited, are subsequently and shortly transferred to another account and/or destination which, prima facie, does not appear to be related to the customer.

h) Customers who deposit cash using numerous deposit slips in such a way that each deposit individually is not significant, but the total of the above deposits is significant.

i) Accounts of companies where almost all transactions, both deposits and withdrawals, are made in cash instead of in the form normally used for similar transactions and/or by companies with similar commercial activities (e.g. use of an e-remittance account, etc.).

j) Branches with a much higher than expected/average number and amount of cash transactions (e.g. statistics held by the Headquarters of an obliged entity should be used to detect such large cash transactions).

k) Deposits of counterfeit banknotes or transactions with counterfeit means of payment.

l) Customers who transfer large amounts to or from abroad, with further instructions for paying other persons in cash.

m) Numerous deposits of small amounts in several establishments of the obliged entity or by a group of persons entering the same establishment at the same time. These amounts may then be transferred to another account, usually in another country.

n) Customers who require large quantities of low-value banknotes to be exchanged for other high-value banknotes.

o) Frequent cash conversions from one currency to another.

p) Low-value cash that's dirty. Stained or mold-smelling banknotes that have been negligently packaged. Cases where when counting the actual amount differs significantly (either upwards or downwards) from the amount declared by the bearer.

q) Purchase of banknotes in a currency that is not in line with the customer's activities.

(6) Transactions through accounts

a) Use of accounts in the name of proxies, trusts or customer accounts in the name of professionals, without showing or needing to do so or keeping up with the activities of the account holder.

b) Claims for a refund, on the grounds that they have been sent to the wrong account.

c) Multiple transactions that take place on the same day in a specific store but with an obvious effort to be made by different service officers.

d) Customers who hold multiple accounts and make separate cash deposits in each of them, with a large total of these deposits.

e) Any person or company whose account does not show any particular movement for personal or professional activities, but is only used to collect or pay large sums which have no apparent purpose or relationship with the account owner and/or its business (e.g. a significant or unusual increase in account movement).

f) Customers that hold accounts with several institutions in the same geographical area, in particular where the obliged entity is aware that account balances are consolidated prior to any order to transfer funds.

g) Payments obviously arising from deposits made in cash the same day or the day before.

h) High value deposits of cheques of third parties, incompatible with the movement of the account.

i) Accounts in which deposits are made on a periodic basis and remain inactive in other periods.

j) Large cash withdrawals from an account that usually does not move or remains inactive or from an account that has recently been credited with an unexpectedly large transfer from abroad.

k) Unusually increased use of safekeeping services by a group of customers. Use of sealed packages which are deposited and withdrawn in safe deposit boxes.

l) Representatives of companies who appear to avoid direct contact with the obliged entity.

m) A large number of people depositing funds in the same account without a satisfactory explanation.

n) An account for which there is authorization to handle various persons, but who do not appear to have any relationship with each other (either family or commercial relationship).

(7) Money remittances/international transactions

a) Customers making regular and large payments, including electronic remittances, which cannot be identified as being made in good faith or where customers regularly receive large sums from countries related to the production or processing or trafficking of drugs.

b) Creation of large credit balances in an account, where this is not in line with the normal turnover of the business, and these balances are then transferred to accounts abroad.

c) Electronic inflows and at the same time outflows of funds carried out by customers without these transactions being carried out through a specific account.

d) Frequent requests for foreign currency cheques or other negotiable means of payment.

e) Frequent deposits of foreign currency cheques originating from abroad.

f) Numerous incoming electronic transfers to a specific account, with each transfer below the reporting threshold applicable in the sender's country.

g) Transfers to/from a high-risk country, without any obvious business reason or when the transaction is incompatible with the customer's business activities.

h) Remittances originating from businesses operating in high-risk countries, e.g. countries that do not or insufficiently implement the FATF recommendations on anti-money laundering and countering the financing of terrorism.

i) Remittances where there is no information on the originator or the person on whose behalf the transaction is carried out.

j) Multiple incoming remittances for small amounts, all or most of which are almost immediately remitted to another country with this being incompatible with normal business operations or the current transactional picture of a particular customer.

k) Large transfers from a customer who resides abroad, for no apparent reason.

l) Electronic remittances with no apparent reason to make, repetitive or showing unusual signs. Payments or receipts with no apparent link to legitimate contracts, products or services.

m) A series of transactions, the amount of which is slightly below the threshold for which due diligence measures are applied.

n) A transaction is split into smaller amounts or two or more shops or cashiers are used on the same day to avoid scrutiny.

o) Transactions carried out by the customer on behalf of third parties, without any apparent business relationship or commercial purpose.

(8) Real Estate Sales and Purchases

a) Transfer of property at a price unusually higher than its value.

b) The purchase price of a property is paid, with money coming from a third party account.

c) The purchase price of a property is paid with money from a third party's account, which is not related to the buyer, as shown in the purchase contract.

(9) New payment methods

a) A customer carries out high value transactions with a prepaid card, taking advantage of the possibility of loading it without a physical presence in the bank, e.g. via ATM, internet banking.

b) A customer purchases a large number of prepaid cards from the same obliged entity and/or from different distributors.

c) Unusually high value in relation to volume.

d) Unusually high activity.

e) Use of the card in unexpected or high-risk countries.

f) Loading cards from many different sources.

g) Loading cards/accounts from many different accounts held with institutions operating in different countries.

h) Loading of cards/accounts by third parties.

i) Loading cards/accounts with amounts below the control threshold for which due diligence measures are in place.

j) Multiple loading of cards/accounts and their immediate transfer or withdrawal from ATMs.

k) Making payments of high balances of debit or credit cards in cash, without knowing the origin of the funds.

l) A customer credits his or her account with substantial amounts almost exclusively through an ATM, which may indicate an intention to avoid a physical presence in the obliged entity.

(10) Correspondent accounts

a) Large-value electronic remittances, where the correspondent account has not previously been used for such remittances.

b) The channelling of transactions by the obliged entity holding the correspondent account to different countries and/or financial institutions before or after crediting the account without any apparent purpose other than to conceal the nature, source, ownership or control of the money.

c) Frequent or numerous remittances to or from the correspondent account originating in or destined for a country that insufficiently or not at all implements the FATF recommendations on anti-money laundering and countering the financing of terrorism.

(11) Investment-related transactions

a) Purchases of securities on behalf of a customer, which are then held by the obliged entity for safe custody, where such an arrangement does not appear to be the most appropriate for that client.

b) Deposits/loans from/to subsidiaries or captives of foreign financial institutions in countries or geographical areas that insufficiently or not at all implement FATF recommendations in the fight against money laundering and terrorist financing.

c) Customer requests for portfolio management (either foreign currency or securities) where the source of the money is unclear or where the request is inconsistent with the nature of the customer’s business and more generally the customer’s needs as known to the obliged entity.

d) Large or unusual settlements of securities transactions in cash.

e) Buying and selling securities without a clear purpose or under conditions that seem unusual.

(12) Borrowing with or without collateral

a) Customers who unexpectedly repay bad loans.

b) Requests for lending against assets owned by third parties (i.e. collateral or guarantee), where the original origin of the assets is not known or where these assets are inconsistent with the known economic displacement of their alleged owners.

c) A request from a customer for securing or arranging financing where the source of the customer's own involvement is not clear, in particular when it concerns immovable property.

(13) Trade-based transactions

a) The goods are shipped to (or from) a country or jurisdiction designated as "high risk" for money laundering and terrorist financing activities.

b) The type of commodity has been classified as "higher risk" in relation to money laundering and terrorist financing activities.

c) Significant discrepancies appear between the description of the good in the bill of lading and/or its description in the invoice in relation to the good itself.

d) There are significant discrepancies between the invoiced value of the goods and their fair market value. Obvious over- or under-pricing of goods and services.

e) The size of the consignment appears incompatible with the size of the exporter or importer or their normal business operations.

f) The type of goods appears not to be in line with the normal business activities of the importer or exporter.

g) The transaction involves receiving cash (or other payments) from a third party or entity that does not appear to be clearly related to the transaction.

h) The transaction involves the use of repeatedly modified or frequently extended letters of credit.

i) The transaction is done through shell companies.

j) The goods are transhipped in one or more countries or jurisdictions for no apparent economic reason.

(14) Transactions by employees or agents or trustees

a) Changes in the lifestyle of employees, e.g. luxurious lifestyle or avoiding absence from the office for holidays.

b) Changes in employee performance/behavior.

c) Transactions with agents, where the identity of the beneficial owner or trader remains unknown, as opposed to the standard procedure for this type of activity.

d) Registration of false customer information by the agent.

e) A dealer's activity pattern is very different from other dealers.

f) High percentage of customers who carry out high value transactions. High percentage of high-risk customers.

g) A large number of references to MOKAS compared to other representatives.

h) Transactions before or after business hours.

i) Customers who always insist on dealing with the same staff member/employee even for routine transactions or who stop dealing with the obliged entity during a period of absence of a specific employee/employee.

j) Complex network of trusts and/or proxies.

k) Corporate structures established or operated in an unnecessarily commercial manner, e.g. companies issuing non-nominal shares for which the bearer is considered a shareholder or issuing other financial instruments owned by the bearer or using a post office box.

l) Reluctance by the trustee to provide information required for the proper performance of his duties.

m) Use of general powers of attorney by third parties, thus limiting the control exercised by the Company's Board of Directors.

Financing of Terrorism

(1) Sources and methods

The funding of terrorist organisations comes from both legal and illegal sources. Proceeds include kidnapping (requiring ransom), extortion (requiring money for "protection"), smuggling, theft, burglary and drug trafficking. Legitimate methods for earning revenue used by terrorist organisations include:

- Collection of subscriptions
- Sale of books and other printed matter
- Cultural and social events
- Donations

- Carrying out fundraisers to raise money from the community.

Revenues from illegal sources are laundered by terrorist organisations using exactly the same methods as those used by criminal organisations. These include illicit cash trafficking and sending, standardised deposits or withdrawals from bank accounts, the purchase of financial instruments (e.g. bank cheques), crypto-asset transactions using credit and debit cards, electronic money transfers using "strawmen" or fake identities or companies without physical presence or nominees from their close family, friends and associates.

(2) Non-profit organisations

(a) Terrorist groups use non-profit and charitable organisations as a means of collecting money and/or as a cover for moving money to aid terrorist acts. The potential misuse of non-profit and charitable organisations can be done in a variety of ways such as:

- Establishment of a non-profit organisation with a specific charitable purpose, which is used to channel money to a terrorist group.
- Infiltration of a non-profit organisation with an entirely humanitarian or charitable mission, diverting money collected for an obvious legitimate purpose to financially support a terrorist group.
- The non-profit organisation acts as an intermediary or to cover money movements on an international basis.
- The non-profit organisation provides administrative support to the activities of terrorist groups.

(b) Unusual characteristics of non-profit organisations that indicate that they are likely to be used for an illegal purpose include the following:

- Inconsistency between obvious sources and amounts collected and handled.
- Inconsistency between the type and amount of financial transactions and the declared mission of the non-profit organisation.
- Sudden increase in the frequency and amount of financial transactions of the non-profit organisation.
- Large unexplained cash transactions.
- Absence of contributions from donors residing in the country of operation of the non-profit organisation.

ANNEX IV

REPUBLIC OF CYPRUS

ASYLUM SERVICE

Confirmation of Submission of an Application for International Protection

Family File No:

File number:

Submission Date:

Arc No:

Applicant Information

Name:	**Surname:**
Father's Name:	Mother's Name:
Nationality:	ID/Passport No:
Date of Birth: 07/07/1999	Place of Birth:
Residence Address:	

This is to confirm that the above applicant has lodged an application for International Protection in accordance with Article 11 of the Refugee Law. Article 8 of the same Law provides that the applicant is entitled to stay in the areas controlled by the Government of the Republic, merely for the purpose of the examination of his/her application for international protection until a final decision is reached regarding his/her claim according to the Refugee Law. This document secures the access of its holder to the rights and benefits provided for in the above mentioned Law.

Applicant Signature _____ Date: 27/11/2024

Issuing Authority

Officers Name: _____ Issuing Authority: _____

Signature: _____ Date: 27/11/2024 Stamp:

IMPORTANT

Note 1: The holder of this confirmation letter is obliged to proceed for **MEDICAL EXAMINATIONS** to the Outpatient District Hospital of his/her place of residence. The examination is free of charge.

Note 2: At the time of lodging the application, the FINGERPRINTS of the applicant, as well as of his/her dependants, in case there are any, should be taken according to Article 11A of the Refugee Law and Article 9 of the Regulation (EU) No 603/2013 of the European Parliament and of the Council, of 26 June 2013. The fingerprints are taken by applicants who are 14 years old or older. They are transmitted to a fingerprint database 'Eurodac' to identify if the applicant has ever applied before for asylum in any other member state of the European Union or has previously been fingerprinted at a border of the EU. The fingerprint data are stored by Eurodac for 10 years.

Note 3: In case of change of address, the holder of this confirmation letter is obliged to inform within three days the competend local Aliens and Immigration Departments of the Police, according to Article 8(2) of the Refugees Law.

Applicant Signature _____ Date: 27/11/2024

IMPORTANT NOTE

You should present yourself to ..... at ..... in order to proceed with all the necessary arrangements for your application for international protection.

Stamp:

FIFTH ANNEX

μπροστινή όψη

ΒΕΒΑΙΩΣΗ ΑΝΑΓΝΩΡΙΣΗΣ ΘΥΜΑΤΟΣ ΕΜΠΟΡΙΑΣ ΠΡΟΣΩΠΩΝ, ΝΟΜΟΣ 60(Ι)/2014

Όνομα:
Επίθετο:
Ημ. Γενν.:
Διαβ.:
Ταυτότητα:
ΔΕΑ:
Χώρα Καταγωγής:
Ημερ. έκδοσης:
Date of issue:
00100114

Σφραγίδα/Υπογραφή

πίσω όψη

Βεβαιώνεται ότι το πιο πάνω άτομο βρίσκεται νόμιμα στο έδαφος της Κυπριακής Δημοκρατίας και έχει πρόσβαση στα δικαιώματα που παρέχει ο Νόμος 60(Ι)/2014, συμπεριλαμβανομένης της πρόσβασης στην αγορά εργασίας.

Σημείωση: Το παρόν δελτίο εκδίδεται με βάση το άρθρο 46(4) του Ν. 60(Ι)/2014 και ως εκ τούτου αποτελεί επίσημο έγγραφο. Η αντιγραφή, παραποίηση ή κατοχή από μη εξουσιοδοτημένο άτομο αποτελεί αδίκημα (άρθρο 337, Κεφ.154)

Η παρούσα βεβαίωση ισχύει για ένα μήνα από την ημέρα έκδοσης της.
Valid for one month.