POLICY

Prevention and countering of money laundering and terrorism financing

TABLE OF CONTENTS

DOCUMENT MANAGEMENT METHOD

Issuing company	doValue Group S.p.A.
Recipient company/companies	All Group Companies
Title	Policy on prevention and countering of money laundering and terrorism financing
Issue Date	30/07/2024
Start Date	30/07/2024
Classification	INTERNAL
Document identification code	PLG08-2024-R01
Hierarchical level of the Integrated Norm System	III Hierarchical Level
Type of document	Policy
Group Directive	YES
Drafted by (Owner)	Group AML
Validated by	-
Approved by (Accountable) on	doValue Board of Directors on 18/07/2024
Repealed or replaced norms	PLG01-2022-R01
Revision History	R01-First draft

GLOSSARY

Parent Company	doValue S.p.A.
Subsidiaries	– doValue Spain S.p.A. – doValue Cyprus LTD – doValue Greece Loans and Credits Claim Management S.A. – doNext Spa
Money Laundering	The following actions, if performed on purpose, represent money laundering: • The conversion or transfer of property, knowing that such property is derived from criminal activity or from an act of participation in such activity, for the purpose of concealing or disguising the illicit origin of the property or of assisting any person who is involved in the commission of such activity to evade the legal consequences of his action. • The concealment or disguise of the true nature, source, location, disposition, movement, rights with respect to, or ownership of property, knowing that such property is derived from criminal activity or from an act of participation in such activity. • The acquisition, possession or use of property, knowing, at the time of receipt, that such property was derived from criminal activity or from an act of participation in such activity. • Participation in, association to commit, attempts to commit and aiding, abetting, facilitating, and counselling the commission of any of the actions mentioned in the foregoing points.
Terrorism Financing	Securing or collecting funds, in any manner, directly or indirectly, with intention or knowledge that it shall be utilised, completely or partially, for performing terrorist acts by individual terrorists and/or terrorist organizations. b. Financing of terrorist activities also means encouraging and assistance in securing and gathering of property, regardless of whether the terrorist act was committed and whether the property was utilised for performing a terrorist act.
Money-Laundering risk	The risk arising from the breaching of legal, regulatory, and self-regulatory provisions, functional to the prevention of the use of the financial system for money laundering purposes, terrorism financing or financing of programmes for the development of weapons of mass destruction, as well as the risk for, involvement in money laundering and financing of terrorism episodes or financing of programmes for the development of weapons of mass destruction.
Customer	For the purposes of AML regulation, "customer" can have the following meanings: • The subject that pays amounts to a company of the Group due to a debt position or that underwrites financial products issued by a SPV for which a recipient company acts as a *servicer* in a securitisation transaction. • A subject that establishes an ongoing business relationship with a recipient company of the Group.

Identification data of the Customer, related actual Beneficial Owner and Representative	Name, surname, place and date of birth, the registered residence and domicile if different from the registered residence, the details of the identifying document and, where assigned, the tax code of the Customer, and where assignation is provided, also the related Beneficial Owner and Representative. In the event of subjects other than the natural person, the name, the registered office, the enrolment number in the register of companies or in the register of legal persons, where required.
Identification data of the Beneficiary, related actual Beneficial Owner and Representative	Name, surname, place, and date of birth. In the event of subjects other than the natural person, the name, the registered office, the enrolment number in the register of companies or in the register of legal persons, where required. In both cases, at the time of the provision of the service, also the place of residence and, if different, the domicile, the details of the identification document, the tax code of the Beneficiary and, if such assignment is required, also of the related Beneficial Owner and Representative.
Suspicious Activity Report (SAR)	The report regarding suspicious activities (including a suspicious transaction) submitted to the FIU.
Anti-Money Laundering Function	An integral part of the level two internal control system, in charge of preventing and combating the execution of money laundering or terrorism financing. The Function supervises the activities related to the prevention and management of the money laundering and terrorism financing risk, through the ongoing monitoring of the appropriateness of relevant internal procedures.
Occasional transaction	A transaction which cannot be referred to an existing ongoing business relationship.
Ongoing business relationship	A long-lasting contractual relationship referred to institutional activities carried on by recipients that can result in several transfers or movements of funds and that does not end with a single transaction.

Politically Exposed Persons (PEP)	The natural persons indicated in article 1, paragraph 2, letter dd) of the Anti-Money Laundering Decree, or the "natural persons who hold or have ceased to hold, for less than one-year, important public positions, as well as their family members and those who have a close relationship with these subjects, as hereinafter described and as described by the national legislation of each Legal entity of doValue Group: 1) Natural persons who hold or held important public offices are those who hold or held the office of: 1.1 President of the Republic, Prime Minister, Minister, Deputy Minister and Undersecretary, President of the Region, Regional Councillor, Mayor of the Provincial capital or metropolitan city, Mayor of a Municipality with a population of not less than 15,000 inhabitants, or similar offices in foreign countries. 1.2 Deputy, senator, European parliament member, regional councillor or similar offices in foreign countries. 1.3 Members of central governing bodies of political parties. 1.4 Judges of the Constitutional Court, judge of the Court of Cassation or the Court of Auditors, councillor of State or other members of the Council of Administrative Justice for the Sicily Region or similar offices in foreign countries. 1.5 Member of the governing bodies of central banks or independent authorities. 1.6 Ambassador, chargé d'affaires or equivalent offices in foreign countries, top official in the armed forces or similar offices in foreign countries. 1.7 Member of the board of directors, management or control of companies controlled, including indirectly, by the Italian State or by a foreign country or with investments, to a substantial or total extent, by the Regions, main Provincial municipalities or metropolitan cities or municipalities with a population of not less than 15,000 inhabitants. 1.8 General director of ASL or hospitals, university hospitals or other national healthcare service entities. 1.9 Manager, deputy manager or member of the governing body or party carrying out equivalent functions in international organizations; 2) The following are family-members of politically exposed persons: parents, spouse or the person in a civil partnership or de facto co-habitant or similar situations of the politically exposed person, the children and their spouses or persons in civil partnerships or de facto co-habitants or similar situations with the children. 3) The following are persons with whom the politically exposed persons are known to have close ties: 3.1 natural persons linked to the politically exposed person due to the joint beneficial ownership of legal entities (including trusts and relevant legal arrangements) or other close business relationships; 3.2 natural persons who only formally hold total control of an entity which is known to have been established, on a de facto basis, for the interest and benefit of a politically exposed person.

Beneficial Owner	The natural person(s) who ultimately owns or controls the customer and/or the natural person (s) of whose behalf a transaction or activity is being conducted. The beneficial owner shall at least include: a) in the case of corporate entities: • the natural person(s) who ultimately owns or controls a legal entity through direct or indirect ownership or control over a sufficient percentage of the shares or voting rights in that legal entity, including through bearer share holdings, other than a company listed in a regulated market that is subject to disclosure • requirements consistent with Community legislation or subject to equivalent international standards; a percentage of 25% plus one share shall be deemed sufficient to meet this criterion; • the natural person(s) who otherwise exercises control over the management of a legal entity; b) in the case of legal entities, such as foundations, and legal arrangements, such as trusts, which administer and distribute funds: • where the future beneficiaries have already been determined, the natural person(s) who is the beneficiary of 25% or more of the property of a legal arrangement or entity; • where the individuals that benefit from the legal arrangement or entity have yet to be determined, the class of persons in whose main interest the legal arrangement or entity is set up or operates; • the natural person(s) who exercises control over 25% or more of the property of a legal arrangement or entity.
Financial Intelligence Unit (FIU)	The Authority[1] which collects, investigates and evaluates suspicious transaction reports filed with the FIU by obligated persons, as well as information transmitted to the Authority by other public or private agencies or brought to the Authority's attention through the mass media, the internet or any other source, concerning business or professional transactions or activities potentially linked to money laundering or terrorism financing.
Financial Action Task Force (GAFI)	The global money laundering and terrorism financing watchdog. The inter-governmental body sets international standards that aim to prevent these illegal activities and the harm they cause to society. As a policy-making body, the FATF works to generate the necessary political will to bring about national legislative and regulatory reforms in these areas.
Financial Sanctions Unit (FSU)	The Unit which collects and evaluates any information forwarded to it by the police and public prosecutors or coming to the Authority's attention in any other way, concerning the commission of the offences related to terrorist acts.
Source of Funds Investigation Unit (SFIU)	The Unit which receives the source of funds declarations of natural persons required to disclose the origin of their assets and property.

[1] The Unit for Combating Money Laundering in Cyprus is the MOKAS. doValue Cyprus is not an obliged entity therefore it has no obligation to report any suspicious transaction.

1. INTRODUCTION

The Board of Directors of doValue S.p.A. (hereinafter, "**doValue**" or the **"Parent Company**") has approved this AML Group Policy (the "**Policy**") in compliance with European, Italian and foreign regulation.

This Policy is part of a broader system of internal controls aimed at ensuring compliance with prevailing law and constitutes the base document for the entire anti-money laundering and anti-terrorism control system of the Group.

Following the approval by the Board of Directors of the Parent Company, the Policy and its subsequent amendments shall be implemented by the relevant Management Bodies of the Subsidiaries. The contents of this Policy are in the responsibility of the Board of Directors of the Parent Company.

The Chief Executive Officer of the Parent Company, with the support of the Anti-Money Laundering Officer and the Member of the Board of Directors responsible for AML/CFT of doValue, evaluates and submits for approval to the Board of Directors the amendments. In addition, the Anti-Money Laundering Officer of doValue is responsible for ensuring the dissemination of the Policy and for ascertaining its adoption by all the subsidiaries, which are subject to the relevant obligations according to the local applicable regulations.

The doValue Group adopted this Policy which considers the uniqueness of the different components of the Group as well as of the risks inherent in the activities carried out, consistent with the principle of proportionality and with the actual exposure to money-laundering risks.

In drafting the document, the Group has also considered the outcomes of the annual process for the self-assessment of money laundering risk. According to the same approach also future updates of the Policy shall reflect the outcomes of this annual self-assessment exercise.

With reference to the Group's foreign companies subject to the specific requirements of the host country's legislation, they are required to implement the provisions of this Policy informing the Parent Company, adapting them to their own organisational context for the purposes of assigning roles and responsibilities and submitting them to the standard internal regulations' approval process.

2. APPLICABLE CONTEXT AND REGULATORY FRAMEWORK

This Policy has been adopted in accordance with the regulatory framework existing at the date of its approval, by the Board of Directors and is subject to subsequent amendments and additions that will become necessary as result of both primary and secondary regulatory interventions.

The AML Policy is compliant with the provisions of the Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorism financing, amending the Directive 2009/138/EC and 2013/36/EU and following the EBA guidelines EBA/GL/2022/05 of the 14 June 2022.

Since the Parent Company is based in Italy, the document is drawn up in accordance with the provisions of the Bank of Italy Decree issued on 30 March 2019, amended by the Provision issued on 1st August 2023, concerning provisions on organisation, procedures, and internal controls to prevent the money laundering and terrorism financing risks. The decree provides that the Parent Company shall define and approve:

- a group methodology for the assessment of money laundering risks;
- a set of formalised procedures for the coordination and sharing of relevant information between the companies belonging to the Group;
- the general standards for customer due diligence, data retention, detection and reporting of suspicious transactions.

The Regulations apply to the companies belonging to the Group with registered offices in Italy subject to the anti-money laundering provisions of Italian Legislative Decree No. 231/07 and to the other companies that belong the Group, despite these not being subject to the provisions on prevention of money laundering and terrorist financing of Italian Legislative Decree No. 231/07. with registered offices abroad, in compliance and compatibly with current local laws and regulations, to strengthen the organisational controls in the prevention of money laundering and terrorist financing and to allow the assessment of the specific risk exposure, also during the Group's internal assessment.

2.1 Scope of the document

The main goal of this Policy is to define:

- the measures to be adopted in terms of organisational structures, procedures and internal controls, proper data auditing and storage;
- the governance rules, roles and responsibilities for combating the risks of money laundering and terrorism financing to be adopted by the Group;

- the group guidelines for combating the risks of money laundering and terrorism financing, as well as the principles for the management of relationships with the customers classified as high risk.

The principles stated in this Policy are reflected in the internal documentation (e.g. AML Local Policy, AML Manual and specific operating procedures, etc.) where the operational and the control tasks are defined in compliance with the principles and regulations applicable to the monitoring of money-laundering and anti-terrorism financing risks.

2.2 Risk assessment criteria

Each company shall develop systems to assess the risk of money laundering by applying the criteria identified by the regulatory authorities responsible for the referenced area. In particular, the following main risk factors categories must be considered:

- risk factors relating to the client, the executor, the beneficial owner.
- risk factors relating to the services and the operations.
- geographical risk factors.

A money laundering risk rating must be assigned to each customer based on the above-mentioned factors. According to a risk-based approach, each risk class will be subject to different requirements in terms of customer due diligence.

Local entities adopt different profiling systems: one of the goals for the Group is to progressively harmonise the risk profiling standards to ensure uniformity in the treatment of the main risk factors. In this context the Anti-Money Laundering Function is responsible for:

- assessing the level of homogeneity, while reflecting the operational peculiarities of the respective activities.
- identifying, based on the self-assessment of money laundering risks, any risk factors not adequately considered and defining their level of priority.
- envisaging (after consultation with the Parent Company AML function) stricter risk rating criteria, according to the results of the self-assessment exercise of the money laundering risks to which the company is exposed.

The customer profile must be updated every time there is a significant change in the status (e.g. acquisition of the PEP position, bad news and prejudicial to the customer, transfer of the residence in a high-risk country).

When a customer is client in various local legal entities, these must align the respective risk rating to the highest one assigned across the Group.

Local AML procedures may provide for the possibility of reviewing the risk profile automatically assigned by the system after documenting the reason of proposed changes.

2.3 Anti-Money Laundering model governance

The AML model governance aims to implement all the necessary measures to ensure compliance with rules, procedures and organisational structures that can ensure the prevention and management of the risks.

The model provides that the primary responsibility in terms of monitoring the risks of money laundering and terrorism financing is assigned to the Corporate Bodies of each legal entity of the Group, according to their respective duties, and in compliance with the directives of the Parent Company. The distribution of tasks and responsibilities among the corporate bodies and the functions must be clearly defined in each company.

In line with the authorised corporate governance standards, the model acknowledges for each company of the Group the centrality of the Board of Directors with respect to the risk governance policies. In this context the Board is responsible for the approval of the anti-money laundering policy (in line with the principles of this Policy) and for the adoption of an operational and control framework that is suitable to the characteristics of the company. To this end, the framework is organised so as to be able to address any issues concerning money laundering and terrorism financing risks as carefully as possible and with the necessary level of detail.

The Management Body is responsible for ensuring the implementation of the strategic guidelines and governance policies applied to the risk of money-laundering, approved by the Board of Directors, as well as for adopting all the measures necessary to ensure the effectiveness of the organisation and the anti-money laundering controls.

The Board of Statutory Auditors, within the scope of its responsibility of overseeing the completeness, suitability, functionality, and reliability of the internal control system, is also constantly in contact with the Anti-Money Laundering Function.

In compliance with the proportionality principle and if provided for in the specific applicable regulations, each company of the Group must set up a specific Anti-Money Laundering Function aimed at preventing and combating the execution of money-laundering activities.

The companies of the Group appoint their own manager entrusted with the Anti-Money Laundering Function, and their own Delegate Manager in charge of Suspicious Transactions reporting (known as "STR Delegate"), in line with the principles established in this Policy (as defined below).

The legal entity doValue – Parent Company of the Group – sets up its own Anti-Money Laundering Function, appoints an AML Officer and a Delegate Manager in charge of suspicious transaction reporting. doValue approves its own policy that defines the actual measures adopted in terms of organisational structures, procedures and internal controls, proper data auditing and storage, in line with the principles contained in this Policy and consistent with the regulatory provisions

specific of the sector to which it belongs.

The Parent Company ensures that the Corporate Bodies and the other companies belonging to the Group implement, in their own local environment, the strategies and policies of the Group. Local subsidiaries adopt a policy consistent with the principles and the guidelines described in the Group Policy, according to a principle of proportionality and based on the activities carried out.

The Anti-Money Laundering Function of doValue identifies additional categories of information that may be shared where there are relationships between the Parent Company and the individual subsidiaries (or among the latter) because of respective business activities. The Parent Company adopts appropriate technical and organisational measures to guarantee that the data contained in the shared information database is handled in compliance with the applicable national laws on personal data protection.

The Anti-Money Laundering Functions of subsidiaries activate appropriate regular information flows toward the Parent Company regarding the main performed activities, the outcome of the controls and the status of remedial actions defined to address any weakness identified as result of these activities.

2.4 Internal information flows: top-down and bottom-up

The doValue Group has developed a decentralised model to prevent AML risks. Therefore, the Anti-Money Laundering Function of subsidiaries functionally report to the Parent or other group company (in the case of doValue Cyprus to doValue Greece) and informs it about the results of the control activities carried out. In addition, the Local AML Officer, reports to and informs the AML Officer of the Parent Company about every relevant information, the objectives set and the result of the AML activities.

Within doValue Group, the strategic guidelines for money laundering risk management and anti-money laundering controls are adopted by the corporate bodies of the Parent company. The Parent Company ensures that the corporate bodies of the other companies belonging to the Group implement group strategies and policies in their business environment. In addition, it has to identify the appropriate organisational solutions to ensure compliance with provisions applicable to the different geographical and business areas of operation and, at the same time, ensure that risk management takes into account all the assessment and elements in each company inside the Group.

In accordance with the regulatory provisions, strategic decisions at group level regarding the management of sanctions, the risk of money laundering and terrorism financing fall into the responsibility of the corporate bodies of the Parent Company.

2.5 Board of Directors

The Board of Directors of the Parent Company approves and periodically reviews the strategic guidelines and policies for managing money laundering risks. In compliance with the risk-based approach, it ensures that these policies are appropriate to the extent and type of risks to which the Group's activities are concretely exposed, as detailed in the annual report which summarizes the results of the AML risk self-assessment exercise.

2.6 Chief Executive Officer

The Chief Executive Officer of each recipient Company is responsible for implementing the strategic money laundering risk guidelines and policies defined by the Parent Company, as outlined in the documents implementing the Policy approved by their respective Boards of Directors.

The Chief Executive Officer is also responsible for adopting all necessary measures to ensure the effectiveness of the anti-money laundering control system and organization. To this end, the Chief Executive Officer reviews the proposals for organizational and procedural interventions presented by the AML function and formally justifies any decision not to accept them.

2.7 Board of Statutory Auditors

The Board of Statutory Auditors, acting as a supervisory body, oversees the compliance with laws and regulations and ensures the control systems' completeness, functionality, and adequacy for preventing money laundering and terrorist financing. In executing its duties, the Board of Statutory Auditors utilizes internal structures for conducting necessary checks and verifications, and leverages on information from other corporate bodies, the Head of the Anti-Money Laundering function, and other relevant units.

In this role, the Board of Statutory Auditors:

- evaluates the effectiveness of procedures for customer due diligence, information retention, and the reporting of suspicious transactions.
- investigates the causes of deficiencies, anomalies, and irregularities detected, and promotes the implementation of appropriate corrective actions.
- is consulted during the processes for appointing and dismissing the Group Anti-Money Laundering Manager and the Manager responsible for suspicious transaction reporting, as well as during the development of the overall system architecture for managing and controlling the risks of money laundering and terrorist financing.

The Members of the Board of Statutory Auditors are required to promptly inform the Supervisory Authority about any facts they discover in the course of their duties that may constitute serious, repeated, systematic, or multiple violations of applicable laws and related regulations.

3. ANTI-MONEY LAUNDERING FUNCTION

The Anti-Money Laundering Function is a specialised second level control function and falls under the category of the company's Control Functions. It is an independent function, and its resources are able to carry out their duties from a qualitative and quantitative standpoint. For this reason, it should consist of enough human resources with the necessary technical-professional skills, to be kept constantly up to date through the provision of continuous training programs. The Function has unlimited access to all the information that are relevant to carry out its duties to fulfil its analysis on the business activities.

The staff of the Anti-Money Laundering Function must be in an independent position to express its assessment, give its opinions and provide recommendations on an impartial basis; regardless of its hierarchical position within the organisation and it must not have any conflicts of interest. The AML Function can outsource some of their activities and the AML Officer as well as the Member of the Board of Directors responsible for AML/CFT update the Board of Directors on the progress of the outsourced activities.

Under a group perspective, the AML Function of the Parent Company is responsible for:

- defining and regularly reviewing common methodology standards at group level to manage the risk of money laundering and combating terrorism financing, reflecting these standards in appropriate group guidelines and overseeing their adoption across the Group.
- collecting and reviewing the information flows from the AML functions of the other Group legal entities.

Although the doValue Group does not adopt a centralised model to manage the risks of money laundering, a global approach is developed to ensure the coordination and the standardisation of activities across the Group. To this end, the AML Function of the Parent Company defines and approves:

a) a group methodology for the assessment of money laundering risks.
b) formalised procedures for the coordination and sharing of relevant information between the companies belonging to the Group.
c) general customer due diligence standards.

Furthermore, due to the organizational complexity of the doValue Group, different Managers in charge of Suspicious Transactions Reporting are designated in each region. The AML Officer of doValue, as Delegate of the Parent Company and Group AML Officer, can collect information from the companies of the Group, to recognize anomalous operations and relationships in a group perspective, and provide the other Managers of the group companies with all the relevant information regarding the shared customers. Moreover, the Parent Company should ensure that the group companies allow the Group AML Officer the full access to the information concerning

the suspicious transactions reported to the FIU as well as to all additional cases not transmitted as deemed to be unfounded together with the rationale of the decision.

3.1 Anti-Money Laundering Officer

The Function Manager (hereinafter also referred to as the AML Officer) is appointed by the Board of Directors, in agreement with the Board of Statutory Auditors (or any other Control Body where present), when applicable under national rules.
The AML Officer must meet the independence, authority, professionalism, and integrity requirements set in this policy.

The Anti-Money Laundering Officer is placed in the appropriate hierarchical and functional position to guarantee the necessary independence and authority, without neither direct responsibilities for any operational areas nor any hierarchical reporting line into the managers of these same areas. The Anti-Money Laundering Officer must demonstrate the following characteristics:

- in-depth knowledge of the legal and regulatory provisions in the areas of anti-money laundering and anti-terrorism and/or former experience in risk management or control functions.
- in-depth knowledge of the banking-financial industry.
- ability of managing the relationships with the Supervisory Authorities, the Investigating Authorities and the Corporate Bodies.

The AML Officer ensures an effective information flow and closely collaborates for the implementation of anti-money laundering policies and procedures.

Within doValue Group a local AML Officer is appointed in each subsidiary directly reporting to the Board of Directors of the company and functionally to the Group AML Officer.

Organizational measures are in place to ensure the operational continuity of the Anti-Money Laundering Function even in the absence or temporary impediment of the Anti-Money Laundering Officer. In the event of the absence or temporary impediment of the Anti-Money Laundering Officer, the Member of the Board of Directors responsible for AML/CFT interfaces with the members of the Function. If the absence of the Anti-Money Laundering Officer extends beyond three months, the Board of Directors proceeds with the replacement or appointment of a temporary Anti-Money Laundering Officer.

3.2 Delegated Manager in charge of Suspicious Transactions Reporting

This Manager is responsible for evaluating suspicious transaction reports submitted by the business departments and forwarding any reports deemed to warrant attention to the Financial Intelligence Unit (FIU). Usually, the AML Officer is appointed for this role, but the Company may choose a different Manager. Within the doValue Group, in order to ensure the proper independence of the reporting function and the compliance with professional and integrity standards, the role of Delegate for Reporting Suspicious Transactions is assigned to the Anti-Money Laundering Officer.

Each company within the doValue Group appoints its own Delegate for Suspicious Activity Reporting, who reports suspicious transactions to the national Financial Intelligence Unit (FIU). The role and responsibilities of the Delegate must be properly formalized and communicated within the company structure.

3.3 Member of the Board of Directors responsible for AML/CFT

The Board of Directors is required to appoint one of its members as responsible for AML/CFT. This role plays a crucial role within the organization as he/she collaborates closely with the Anti-Money Laundering Officer to ensure the effective management of money laundering and terrorism financing risks. The person in charge of this role must have expertise, independence, and knowledge of national and international anti-money laundering regulations. Additionally, he must be familiar with internal control systems and have a high reputation and integrity. The Board of Directors avoids any conflict of interest in the choice of the Member responsible for AML/CFT.

In his/her role he/she coordinates various activities within the organization to ensure effective oversight of money laundering and terrorism financing risks. These tasks include:

- **Surveillance and Monitoring**: Constantly monitors the adequacy of anti-money laundering policies, procedures, and internal controls.
- **Collaboration with the Board of Directors:** Actively engages with the Board of Directors, providing periodic reports on the effectiveness of anti-money laundering measures adopted and contributing to strategic risk management assessments.
- **Supporting the AML Officer**: ensuring that the AML officer has direct access to all the information necessary to perform his/her tasks, has sufficient human, economic and technical resources, and tools to be able to adequately perform the tasks assigned to them.

In coordination with the Anti-Money Laundering Officer and the staff of the AML Function, the Member of the Board of Directors responsible for AML/CFT performs the following tasks:

- **Internal Communication:** ensures effective flow of information among various business units, ensuring that Board members and other corporate bodies are adequately informed about risks and measures taken to mitigate them.
- **Risk Assessment:** actively contributes to the assessment of money laundering and terrorism financing risks, identifying potential vulnerabilities and suggesting appropriate mitigation measures. Promotes awareness and training of staff on the importance of money laundering and terrorism financing prevention.
- **Reporting activity:** ensures that the activities carried out by the AML function are regularly reported to the management body which is then provided with sufficiently comprehensive and timely information and data on AML risks.

Each company of the Group appoints a Member of the Board of Directors responsible for AML/CFT. Please refer to local policies for more details about the Member of the BoD responsible for AML/CFT.

4. AML REQUIREMENTS

The AML legislation outlines key requirements for monitoring AML processes. Each company within the doValue Group implements specific procedures to comply with regulatory requirements and manage the risk of money laundering regarding the main topics described below.

4.1 Customer Due Diligence

The doValue Group companies put in place customer due diligence process when:

- a continuous relationship is established.
- a single occasional transaction or multiple linked transactions are executed for an amount equal to or above the applicable designated threshold.
- there is a suspicion of money laundering or terrorism financing, regardless of any derogation, exemption or designated threshold that may apply.
- there are doubts about the authenticity or the reliability of previously obtained customer identity information.

Customer's identity information to be collected as part of the customer due diligence process may change depending on the type of customers (i.e. private individuals or legal entities).

All required information is included within a questionnaire and is supported by attached documents. The authenticity of customers' information collected in the due diligence process must be verified based on documents and data obtained from reliable and independent sources, in accordance with the applicable regulations. The fulfilment of due diligence obligations includes checking whether customers are on any Aml watchlist.

The impossibility to comply with due diligence requirements implies the obligation to refrain from processing the transaction/opening the continuous relationship or to terminate the relationship if it is already in place.

As a general provision, the information collected during the customer due diligence process must be updated:

- in the event of a change in beneficial ownership for the companies for which such information is available.
- based on a different frequency depending on the level of AML risk assigned to the customer; in any case no later than 10 years in Italy, Spain and Cyprus, 5 years in Greece.

The update of the customer's information is required whenever it becomes evident that the information already available for the due diligence are no longer up to date as well as the customers acquires a specific qualification (e.g. PEP) or is included in blacklists (e.g. Crime, Terrorism lists).

4.1.1 Enhanced Due Diligence

The enhanced due diligence requirements apply to customers with the highest levels of money laundering risk. The model in place envisages the collection of a due diligence questionnaire, which provides a set of information different from those collected in the ordinary due diligence process. Summing up, the enhanced due diligence process consists of obtaining more information by extending the scope and frequency of related obligations.
In "high-risk" scenarios, such as transactions or relationships involving Politically Exposed Persons (PEPs), as well as transactions or relationships suspected of money laundering or potentially related to criminal activities, the NPL Management Unit Manager or an Asset Manager, along with their supervisors, must seek authorization from the AML Function to establish the relationship.
For transactions or relationships involving PEPs, authorization will be granted exclusively by the AML Manager. In the event of established risks of money laundering or criminal activity, the Delegate Manager in charge of Suspicious Transaction Reporting may decide to report the transaction to the FIU, stop the relationship, inform the Managing Director, or take other appropriate measures.
The Delegate's decision will be formalized and communicated to the proposing department via e-mail.
In case of a negative opinion from the AML, the person in charge must implement the risk mitigation measures indicated by the Delegate.

The Parent Company is empowered, through its Anti-Money Laundering Function, to provide guidelines about raising the risk profile of economic activities that, due to their specific features, may be considered at high risk of money laundering. In particular:

- specific categories of transactions.
- subjects belonging to high-risk countries or involved in operations referable to such countries.

Moreover, further information relevant for the risk assessment of the customer should be collected on:

- the source of funds used in the relationship or to execute a transaction.
- the economic (e.g. sources of income) and financial situation (e.g. balance sheets, VAT and income tax returns, documents and declarations from the employer, financial intermediaries or other parties) of the customer.

The enhanced due diligence measures must be taken in the event of:

- Politically Exposed Persons (PEPs): when the client or the beneficial owner falls within the definition of PEP, the establishment or continuation of a relationship or the execution of an

occasional transaction shall be preventively authorised by the Head of the Anti-Money Laundering Function.

- Trusts: appropriate investigations shall be carried out to understand the reasonableness and the soundness of the entity and intercept any cases of improper use of the trust to achieve undeclared purposes (e.g. the subtraction of assets to creditors and tax authorities).
- Cross-border correspondent relationships with a Financial Institution based in a third country: the opening of such relationships must be subject, in addition to other law provisions, to the preventive authorisation of the Head of the Anti-Money Laundering Function.

In the light of above, as provided by the VI European Directive, business relationships or transactions involving high-risk countries should be limited when significant weaknesses in the AML/CFT regime of these countries are identified, unless adequate additional mitigating measures are adopted.

4.1.2 Simplified Due Diligence

Simplified due diligence measures can be applied to those customers classified as low risk, such as public administrations, institutions, or other entities performing public functions in accordance with European Union regulations.

Each Company that belongs to doValue Group identifies, in accordance with its own Regulation, further categories of entities to which simplified due diligence standards can apply, provided that low risk classification criteria are consistent with those ones identified by the law as well as with the suggestions of the EU competent supervisory authorities.
The adoption of simplified due diligence standards shall be motivated, validated by the Anti-Money Laundering Function of the Parent Company and approved by the Board of Directors.
The simplified due diligence measures require aa limited set of documents and a lower frequency in reviewing the collected information.

The simplified due diligence standards do not apply when:

- there are doubts, uncertainties or inconsistencies in relation to the data and the information collected during the identification of the customer, the executor or the beneficial owner.
- the conditions for the application of simplified measures based on the risk scoring assigned to the customer by the profiling systems no longer apply.
- the monitoring activities on the customer's overall operations and the information acquired during the relationship lead to exclude the low-risk classification.

- there are any elements to suspect the exposure to money laundering or terrorism financing risks.

4.1.3 Obligations to abstain

If the company is unable to perform a customer due diligence, it cannot start, continue, or pursue any relationship or transactions with the affected customer (known as the obligation to abstain) and, if necessary, must terminate the business relationship already in place and decide about the submission of a suspicious transaction report to the Financial Intelligence Unit (FIU). Before making the suspicious transaction report to the FIU, and to exercise any right to terminate, the obliged entity may not carry out any transactions suspected to be in connection with money laundering or with terrorism financing.

If the obligation to abstain cannot be fulfilled since there is a legal commitment to receive the documentation or the execution of the transaction may not be postponed due to its nature or the act of abstaining could hinder the investigations, a suspicious transaction report must be immediately sent to the FIU.

The doValue Group companies abstain from offering products/services or carrying out transactions that may facilitate the anonymity or the concealment of the customer's and the beneficial owner's identity, as well as from establishing business relationships or remotely carrying out occasional transactions, not assisted by adequate recognition mechanisms and procedures.

4.1.4 Customer profiling

The doValue Group adopts suitable procedures to calculate the money laundering and terrorism financing risk profile to be assigned to each customer, based on the information collected and the analyses carried out these procedures consider all the risks related to the Customer, the legal Representative, the Beneficial Owner, products, services, transactions, and also geographic area.

This approach is an application of the broader principle of proportionality, set forth by prevailing regulatory provisions, with the purpose of maximising the efficiency of the company controls.

The different profiling systems allow – based on the processing of the data and the information collected when initiating a business relationship, executing occasional transactions, or continuously monitoring the operations - the determination of a "score" which reflects the level of risk of money laundering or terrorism financing and then the classification of the Customers into different risk classes. This ensures that the scores assigned by the system are consistent with the information available.

The risk classes are defined by each legal entity of the Group according to the limits set by the national law as well as to the criteria provided by the AML IT system in force at each company. The customer analysis shall be carried out in accordance with the approved AML international standards and with the regular reports issued by the European Commission, pursuant to Article 6 of the EU AML Directive, where the main developments in the risks of money laundering and terrorism financing on the European market are identified, analysed, and assessed.
In the light of the above, the customer risk classification carried by the doValue Group considers the following factors,

a) in relation to the customer:

- the legal nature.
- the main activity carried out.
- his/her behaviour during the execution of the occasional transaction or the establishment of the ongoing relationship.
- the geographical area of residence or establishment of the customer or the counterparty.

b) in relation to the features of the transaction or the ongoing relationship:

- the type of transaction or the continuous relationship put in place.
- the procedures for carrying out the transaction and the ongoing relationship.
- the amount of the transaction.
- the frequency and volume of transactions and the length of the ongoing relationship.
- the coherence of the transaction or the continuous relationship, related to the activity carried out by the customer and the extent of its economic and financial resources.
- the geographical area of destination and the object of the transaction, the ongoing relationship, or the professional performance.

These factors shall be complemented by the criteria listed in the previous paragraphs 4.1, 4.1.1 and 4.1.2 and following, regarding the customer due diligence processes.

Based on all the collected information, whenever the employee deems the customer's behaviour to be anomalous or a transaction to be unreasonable, he/she shall promptly send a suspicious transaction report to the Anti-Money Laundering Function. The Delegate Manager in charge of Suspicious Transactions reporting, as result of its own assessment, takes any action needed, including the upgrade or the downgrade of the Customer's risk profile and the reporting of the transaction to the FIU. Appropriate evidence of all the assessments conducted must be kept.

The Group Companies will monitor and regularly update the criteria and the system functionality supporting the risk profiling process. These updates include the main developments in the AML area and the leading practices in the market.

In case of customers in common among different companies of the Group, they are graded by all the companies with the highest risk profile assigned to them across the Group.

4.2 Data Recording and Retention

The Companies shall keep the documents collected during the customer due diligence and the records relating to the transactions executed in a way that allows them to be unchangeable and easily retrievable.

The retained documentation shall allow, at least, to identify:

- the date of establishment of the ongoing relationship.
- the identification data regarding the customer, the beneficial owner and the executor, and information on the purpose and nature of the relationship.
- the date, amount, and reason for the transaction.
- the means of payment used.

The documents, data and information collected are retained for a period set forth by the national laws in force[2] which starts at the termination date of the ongoing relationship or the execution date of the occasional transaction.

4.3 Suspicious Activity Reporting

The Companies of doValue Group will promptly send to the Financial Intelligence Unit (FIU) a suspicious transaction report in all cases where they know, suspect, or have reasonable grounds to suspect that money laundering or terrorism financing transactions are taking place or were carried out or attempted, and whenever the funds used to execute those transactions, regardless of the amount, derive from criminal activities[3].

The employees who are in contact with the Customers are therefore responsible for continuously monitoring the progression of the relationship and the transactions put in place They promptly send a suspicious transaction report to the Anti-Money Laundering Function, in accordance with the internal procedures, before executing the transaction.

This is without any prejudice to the cases where:

a) the transaction must be carried out since there is a legal obligation to receive the documentation and the transaction cannot be postponed.

b) the postponement of the transaction could hinder the investigations.

2 The retention period, for AML information/documents in Italy and Spain is 10 years, in Greece is 5 years.
3 When doValue Cyprus observes suspicious transactions or, knows or has reasonable suspicion that monetary sums constitute proceeds of illegal activities or relate to terrorism financing, all of which ought to be reported to the Cyprus anti-money laundering unit (MOKAS) by obliged entities, doValue Cyprus has no 'official' communication channel with MOKAS because it is not an obliged entity. It would therefore have to communicate any suspicious activity to MOKAS as any other non-obliged entity or individual and not through the submission of suspicious activity reports (SARs) usually prepared and submitted by the money laundering compliance officers. Although doValue Cyprus has appointed a compliance officer, as a non-obliged entity, such compliance officer is not one appointed within the meaning of the AML Law. What could doValue Cyprus do is to report the transaction to its customer since the transaction relates to the clients of doValue Cyprus customer.

To facilitate the identification of suspicious transactions by the internal staff, the Group refers to the risk indicators issued and periodically updated by the Financial Intelligence Unit (FIU), preparing appropriate guidelines and training.

If, after receiving a SAR from the business units, the AML Officer deems that the transaction must be sent to the Financial Intelligence Unit (FIU), he/she will proceed with the transmission by omitting the name of the subject who sent the report.
Group companies shall take appropriate measures to prevent the disclosure of information on the identity of the reporting person; their names may be disclosed only when the Judicial Authority, issuing a reasoned decree to that effect, deems it essential to assess the crimes to be prosecuted. The reporting subject must not inform anybody about the decision to proceed with a suspicious transaction report.

4.3.1 Internal violation reporting system

The anti-money laundering regulation establishes the adoption of internal procedures for employees to report, either potential or actual, violations of provisions related to the prevention of money laundering and terrorist financing. These procedures must ensure:

- the confidentiality of the reporter's identity as well as of the alleged perpetrator of the violation.
- the protection of the reporter against possible retaliatory actions.
- the development of a specific reporting channel that is anonymous and independent, the complexity of which is proportionate to the nature and size of the obligated entity.

Each group company must identify its own channel and communicate it to employees.
For some doValue Group companies, the channel used is whistleblowing.

4.3.2 Forbidden Relationships

All companies within the Group are prohibited from entering any business relationship with legal entities, or individuals and entities associated with them, if there is a belief or reasonably grounded suspicion that they may be involved in criminal activities, be members of a criminal or terrorist organization, or politically support or finance such an organization.
Furthermore, the entire Group is forbidden from entering a business relationship with individuals known to have been convicted of or prosecuted for criminal offenses such as drug trafficking, abuse of public funds, money laundering, terrorism, or terrorist financing.
The Company is prohibited from entering or maintaining a business relationship with financial institutions that do not have a physical presence or staff in the country in which they are registered (shell banks), unless they are subsidiaries of banking or financial groups that are adequately supervised on a continuous basis.

The Group is prohibited from entering or maintaining a business relationship or executing occasional transactions involving, directly or indirectly, trusts or corporations based in high-risk third countries.

Finally, it is not permitted to enter or maintain any business relationship with legal entities active in the armaments industry if this relationship is related to the manufacturing, trade, import/export, distribution, or financing of armaments, or with individuals associated with them.

4.3.3 Reporting obligations on transfers of cash and bearer securities

The doValue Group ensures centralized reporting to the Authorities of any breaches of restrictions on cash and bearer securities that come to its attention, in accordance with the time limits and procedures specified in relevant laws and regulations.

5. COMBATING TERRORISM FINANCING REQUIREMENTS

To effectively combat terrorism and deprive terrorists of necessary financial resources, it is crucial to adopt measures to prevent the use of the financial system for such purposes. These measures include freezing funds held by individuals or entities designated by United Nations Security Council (UNSC) or European Union (EU) resolutions.

Close monitoring of cash flows and significant financial transactions is essential to ensure they do not match lists of suspected individuals or entities. The Companies belonging to doValue Group are required to report any suspicious transactions to the Financial Intelligence Unit of reference and comply with reporting obligations under Anti-Money Laundering laws.

Embargo provisions can originate from both the EU and the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC), affecting individuals, entities, or countries subject to trade or financial restrictions. Procedures focus on names listed in relevant databases, such as those of the EU and OFAC, with the Ministry of Economy and Finance responsible for ordering the freezing of funds held by individuals or entities involved in terrorist activities or threats to international security.

The Financial Intelligence Unit disseminates lists and any exemptions, while financial intermediaries conduct checks to ensure compliance with sanctions and embargoes. All Group companies, in accordance with legal provisions and directives from competent authorities, implement measures to avoid involvement in transactions that violate anti-terrorism laws or international embargoes.

Information regarding sanctioned individuals is treated with maximus confidentiality and cannot be disclosed directly or indirectly to the affected parties.

6. EXCHANGE OF INFORMATION WITHIN THE GROUP

Companies are required to share the following information with other companies in the Group:

- the risk profile assigned to the client.
- the names of the persons subject to suspicious transaction reporting.
- any other information that is necessary to the Manager in charge for Reporting of Suspicious Transactions or to the Anti-Money Laundering Officer of the Parent Company for the purpose of carrying out in-depth analysis of the shared customers.

Within the boundaries established by the requirements of the AML legislation about data protection and confidentiality obligations, the Group Companies are allowed to exchange the information collected during the due diligence process with the main purpose of avoiding duplications in the fulfilment of due diligence obligations as well as in the submission of information requests to customers.

6.1 Methodology for Group Self-Assessment

Group companies annually perform a self-assessment of the money laundering risk to which they are exposed. The self-assessment activity is based on a methodology defined by the Anti-Money Laundering Function of the Parent Company and comprises the following macro-activities:

- **identification of the inherent risk:** the companies identify the current and potential risks they are exposed to, also considering the elements provided by external sources.
- **vulnerability analysis:** the Companies analyse the adequacy of the organisational structure as well as of the prevention and monitoring measures with respect to the risks previously identified to detect any vulnerability.
- **determination of the residual risk:** the Companies assess the level of risk to which they are exposed based on the level of inherent risk and the effectiveness of mitigating measures.
- **remedial actions:** the Companies implement appropriate corrective actions against any existing critical issues and to adopt appropriate measures to prevent and mitigate the risk of money laundering.

The self-assessment process shall be conducted by the Parent Company supported by the subsidiaries in compliance with the guidelines provided by the Bank of Italy, as reference legislation of doValue. The Anti-Money Laundering Function of the Parent Company coordinates the self-assessment activities and conducts a group-wide self-assessment, based on the required data and information provided by each subsidiary.

Remedial actions are proposed by each local AML Officer in accordance with the AML Officer of the Parent Company and approved by the Board of Directors. The adjustment measures are

implemented by the Management Body, acting through the Anti-Money Laundering Function.

The self-assessment is conducted annually and is submitted to the doValue Board of Directors by the 30th of April of the year following the year of the assessment.

The exercise shall also be performed when new lines of business are opened and it shall be promptly updated when new significant risks emerge or significant changes in existing risks, operations, organisational or corporate structure occur.

6.2 Cross Sectional Processes and Information Flows

The strong cross relevance of the process of managing the risk of money laundering, terrorism financing and related sanctions, requires the establishment of cross-sectional processes as well as an adequate model of relations and the effective activation of timely information flows between all the affected organisational structures.

The information flows can be summarised in:

- information flows within the company.
- information flows between Group companies and the Parent Company.

In general, a detailed description of the information flows supporting the management of risks of money laundering and terrorism financing is provided in the Regulation of the AML Function. The attached sheet summarizes the top-down and bottom-up information flows established between the Parent Company and the other subsidiaries of the doValue Group.

doValue_Intercomp
any Information Flo

7. REVIEWING AND UPDATING THE POLICY

The AML/CTF Function reviews and updates this policy on regular basis and submits the revised version to the Chief Executive Officer for the Board of Directors' approval. Any amendments to the Policy are subsequently disclosed to all subsidiaries (Italian and foreign) to ensure their implementation in the local framework of policies and procedures.