Group Policy

Policy on prevention and countering of money laundering and terrorism financing

TABLE OF CONTENTS

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 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.

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 a result of both primary and secondary regulatory interventions.

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 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;
- formalised procedures for the coordination and sharing of relevant information between the companies belonging to the Group;
- general standards for customer due diligence, data retention, detection and reporting of suspicious transactions.

Moreover, the policy sets forth the doValue Group's global anti-money laundering and counter-terrorism financing Policy and is applied to all subsidiaries.

The contents of this Policy are in the responsibility of the Board of Directors of the Parent Company, having consulted the Risk & Transactions with Related Parties Committee and the Board of Statutory Auditors.

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

1. APPLICABLE CONTEXT

This Policy forms part of a broader system of internal controls aimed to ensuring compliance with prevailing law and constitutes the base document for the entire anti-money laundering and anti-terrorism control system of the Group. Standards set in this Policy must be considered complementary and applicable in so far as they are not in conflict with the provisions issued by

the local Authorities.

The Policy considers the peculiarities and the complexities of the business operations carried out by the Parent Company and the other Group legal entities, the services provided, the types of customers, the type of business and the developments expected in these areas.

The Anti-Money Laundering (AML) and Counter Terrorism Financing (CTF) regulatory framework is based on a comprehensive set of national, EU and international regulatory sources.
The EU guidelines on preventing the use of the financial system for money laundering and terrorism financing are contained in EU Directive 2015/849 of the European Parliament and of the Council of 20 May 2015 (Fourth Anti-Money Laundering Directive), implemented by EU Directive 2018/843 (Fifth Anti-Money Laundering Directive).

At a national level, prevention and fight against money laundering and terrorism financing are regulated by the following primary laws:

ITALY

- Legislative Decree no. 231 of 21 November 2007, as amended by Legislative Decree no. of 25 October 2019 (hereinafter also "Anti-Money Laundering Decree")

GREECE

- Law 4557/30.07.2018, as amended by Laws 4734/08.10.2020 and 4816/2021, is the basis of the applicable Greek institutional framework on preventing and combatting money laundering and terrorism financing and incorporates the provisions of Directive (EU) 2015/849, 2018/843 and 2018/1673 of the European Parliament and of the Council.

SPAIN

- Law 10/2010 of 28 April on anti-money laundering and financing of terrorism and in accordance with the Order EHA/2444/2007 of 31 July.

PORTUGAL

- Law 83/2017 of 18 August (transposition of directive 2015/849/EU) updated by the law 58/2020 of 31 August (transposition of directive 2018/842/EU); Regulation 276/2019 of 26 March of IMPIC (regulates law 83/2017) and regulation 603/2021 of 2 July of IMPIC[2].

CYPRUS

- Prevention and Suppression of Money Laundering Activities Laws of 2007 (188(I)/2007).

The Group has 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.

[2] IMPIC stands for Instituto dos mercados públicos do imobiliário e da construção and it's the housing market regulator

In drafting the document, the Group has considered also 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.

The Parent Company doValue issues this Policy to be complied with by all the Group subsidiaries, both Italian and foreign, which are subject to sanctions and money laundering risk prevention, obligations. In this context AAM Cyprus and doValue Cyprus are an exception as they are currently not obliged entities as per the Cypriotan Law[3].

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 accordingly, 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.

1.1 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 and the roles and responsibilities for combatting the risks of money laundering and terrorism financing to be adopted by the Group;
- the group guidelines for combatting the risks of money laundering and terrorism financing, as well as the principles for the management of relationships with the customers who are classified as high risk.

The principles stated in this Policy are reflected in the internal detailed documentation (e.g. AML Manual and specific operating procedures, etc.) where the operational and the control tasks are disciplined in compliance with the principles and regulations applicable to the monitoring of money-laundering and anti-terrorism risks. Please refer, in particular, to the "Anti-Money Laundering Manual[4]" issued by the AML function of the Italian Legal Entities, and regularly updated by the Anti-Money Laundering Function, which overall defines in detail the responsibilities, the operational tasks and the methodology applied to the management of money-laundering risk with regard to due diligence, reporting of suspicious transactions and

[3] Section 2A(1) of the Cypriotan AML Law lists the categories of 'obliged entities' which are subject to supervision by regulating Supervisory Authorities (as defined herein). The company does not fall under any of the categories and as such, is not classified as an 'obliged entity' pursuant to the AML Law. In particular, the company does not fall into the category of 'estate agents' because pursuant to Section 33(1)(d) of the Estate Agents Law, it does not qualify as an estate agent.

[4] The internal manual issued in June 2021 by the AML functions of dovalue and Italfondiario. The document is in force for all the Italian companies, since that describes the operational guidelines to follow in carrying out the anti-money laundering activities. Every single legal entity of doValue Group should have an internal document that sets the AML guidelines, taking into account the business, the IT systems and the national legislation in force.

second level controls carried out by the Anti-Money Laundering Function.

1.2 Risk assessment criteria

Each company shall have systems in place to assess the risk of money laundering by applying the criteria identified by the regulatory authorities responsible for the sector in which they operate. In particular, the following main categories of risk factors, also identified as relevant by the Italian and European Authorities, 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.

Based on the above-mentioned factors, a money laundering risk must be assigned to each customer. According to a risk-based approach, each level of the adopted rating scale will be subject to different requirements for customer due diligence.

Different profiling system are currently in place in the various Group legal entities. However, a plan has been developed at group level to progressively harmonise the risk profiling standards in order 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) more stringent risk rating criteria, according to the results of the self-assessment of the money laundering risks to which the company is exposed, whether this is deemed as necessary and/or appropriate.

The updating of customer profiling and other available AML relevant information must be carried out whenever events occur which are likely to lead to a change in customer status (e.g. acquisition of the PEP position, bad news and prejudicial to the customer, transfer of residence in a high-risk country) and, according to a risk-based approach, different frequencies may be defined according to the assigned risk profile.

In case of customers shared by various Group subsidiaries, they must be conservatively profiled by each company with the highest risk rating assigned across the Group.

Local AML procedures may provide for the possibility of reviewing the risk profile automatically assigned by the system by clearly and comprehensively documenting the rationale of proposed changes.

1.3 Anti-Money Laundering model governance

This model to combat money laundering and terrorism financing is managed, at group level, through a specific process aimed at implementing and ensuring the maintenance by all Group companies of rules, procedures and organisational structures that can ensure the prevention and management of the risks in question.

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 company of the Group, according to their respective duties, and in compliance with the directives of the Parent Company. The distribution of tasks and responsibilities in the area of compliance by the corporate bodies and 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 Control Body, within the scope of its responsibility to oversee 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 reference regulations, each company of the Group must set up a specific Anti-Money Laundering Function aimed at preventing and combatting 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 responsible for Reporting of Suspicious Transactions, 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 and appoints a Manager of this Function and a Delegate responsible for Reporting of Suspicious Transactions. 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.

Within the scope of the group guidance and coordination activities, the Corporate Bodies of the Parent Company adopt the approved strategic guidance in the area of money laundering risk and anti-money laundering controls. The Parent Company ensures that the Corporate Bodies and the other companies belonging to the Group implement, in their own corporate environment, the strategies and policies of the Group.

In order to pursue a full and concrete implementation of the group model, the consolidated subsidiaries adopt a policy consistent with the principles and the guidelines described in this Policy, according to a principle of proportionality and based on the specific character of their activities.

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) as a result of respective business activities. The Parent Company adopts appropriate technical and organisational measures in order 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 the subsidiaries activate appropriate regular information flows toward the Parent Company regarding the main performed activities, the outcome of the carried-out controls and the status of corrective actions defined to promptly and effectively address any criticalities identified as a result of these activities and controls.

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

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.

The doValue Group does not use a centralised model, therefore the Anti-Money Laundering Function of subsidiaries refers in a complete and timely manner to the Parent or other group company (in the case of AAM Portugal to AAM Spain and doValue Cyprus to doValue Greece) about the results of the control activities carried out. In addition, the AML Local 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.

2. GUIDANCE AND COORDINATION OF GROUP COMPANIES

In accordance with the relevant 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. With reference to the management of money laundering risk, the Group Companies, in agreement with the Parent Company, may organise in compliance with the guidelines described below.

3. ANTI-MONEY LAUNDERING FUNCTION

According to a risk-based approach, the Anti-Money Laundering Function is responsible for monitoring the risk of money laundering and terrorism financing and for adjusting the processes in accordance with developments in the applicable regulatory and procedural environment.

It checks that the company procedures are consistent with the objective of preventing and fighting infringement of external (regulatory laws and rules) and internal regulations about money laundering and terrorism financing.

It pays attention particularly to the adequacy of the internal systems and procedures with the purposes of adequately assessing the customers and their risk profile, recording any AML relevant information as well as of detecting, assessing and reporting suspicious transactions.

The Anti-Money Laundering Function is a specialised second level control function and falls under the category of the company's Control Functions. This Function is independent, 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 programmes. In order to fulfil its analysis on the business activities the Function has unlimited access to all the information that are relevant to carry out its duties. AML Function reports directly to the Board of Directors, the Board of Statutory Auditors or the Chief Executive Officer, in accordance with the specific requirements of the national laws.

The staff of the Anti-Money Laundering Function must be in an independent position to be able to express their assessment, give their opinions and provide recommendations on an impartial basis; regardless of their hierarchical position within the organisation, they must not have any conflicts of interest, arising from professional or personal relationships, monetary or any other type of interest, that may jeopardise the duties to be fulfilled. Additionally, they must be protected from undue interference that could limit or change their scope of action or the performance of their tasks, or that could significantly affect or influence their opinions or the content of their work.

More specifically, the Anti-Money Laundering Function, if applicable under national law:

- identifies the applicable regulations about monitoring the risk of money laundering and combatting terrorism financing, evaluates their impact on the internal processes and procedures, prepares/validates and updates the internal regulations, the policies and procedures on anti-money laundering and anti-terrorism;
- provides advisory and support activities to the Corporate Bodies, Senior Management and the organisational units of doValue Group, regarding issues under its competence;
- cooperates in the definition of the internal control system, the procedures and the controls aimed at preventing and combatting money-laundering risk;
- cooperates in the definition of the governance of money-laundering risk policies and of the various steps composing the process for managing this risk;
- checks the suitability of the process for managing the money-laundering risk and the suitability of the internal control system and procedures, and proposes organisational and procedural changes needed or advisable to ensure adequate coverage of the risks;
- ensures the definition and maintenance of the control system aimed at guaranteeing compliance with the obligations relating to the Customer Due Diligence, according to a risk-based approach which provides for an adjustment of such obligations according to the money-laundering risk profile attributed to the Customer;
- may carry out an enhanced due diligence process only in those cases when – for objective, environmental and subjective circumstances – the money-laundering risk is quite significant;
- verifies the reliability of the information system for the fulfilment of the obligations related to the Customer Due Diligence, the storage of data and the reporting of suspicious transactions;
- verifies the correct functioning of the information system for the fulfilment of the obligations regarding the forwarding of objective communications;
- analyses and investigates the internal and external reports received on alleged suspicious transactions to be submitted to the Delegate responsible for Reporting of Suspicious Transactions, with the purpose of evaluating any necessary reporting to the FIU;
- examines the evidence generated by any detection systems (automated or not) available for the Anti-Money Laundering Function and, when relevant, submits the results to the "Delegate responsible for Reporting of Suspicious Transactions" with the purpose of assessing whether to send the reports to the Financial Intelligence Unit (FIU);
- supports the Delegate responsible for Reporting of Suspicious Transactions in transmitting suspicious transactions reports to the Financial Intelligence Unit (FIU);
- cooperates with the Delegate responsible for Reporting of Suspicious Transactions to evaluate the effectiveness of detection and reporting systems and the accuracy of first evaluations about the nature of customers' operations carried out by company's staff;

- monitors the monthly transmission to the Financial Intelligence Unit (FIU) of the aggregated data registered in the Anti-Money Laundering database;
- forwards to FIU, based on the instructions issued thereby, the objective communications;
- cooperates with the Authorities to manage any anti-money laundering relevant issues and follows up on the received requests for information;
- ensures, in cooperation with the other corporate functions, competent in the area of staff training, the setup of an effective training programme aimed at achieving the continuous strengthening of staff awareness about anti-money laundering risks;
- at least once a year prepares a Report on the initiatives undertaken, the deficiencies identified and the relevant corrective actions identified as well as on staff training activities, to be submitted to the Board of Directors, the Risk & Transactions with Related Parties Committee, the Board of Statutory Auditors and the Chief Executive Officer;
- carries out, in cooperation with the other involved corporate functions and according to the methodology and the time frame defined by the Bank of Italy, a self-assessment of the group exposure to the money laundering and financing of terrorism risks and consolidates the results in the above described annual Report;
- promptly informs the Corporate Bodies about relevant breaches or deficiencies identified in the execution of its tasks;
- prepares proper information flows for the Corporate Bodies;
- performs on behalf of some business partners and in compliance with the contractual obligations undertaken with them, specific activities aimed at combatting the money-laundering risk according to the methodology and the scope defined in said agreements
- .

In this context, 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 combatting terrorism financing, reflecting these standards in appropriate group guidelines and overseeing their adoption across the Group;
- collecting and reviewing the information flows coming 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, various Delegates responsible for Reporting of Suspicious Transactions are designated in each region. The Group AML Officer, as Delegate of the Parent Company, can collect information from the companies of the Group, in order to recognize anomalous operations and relationships in a group perspective, and provide the other Delegates 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 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 AML Officer

The Manager of the Function (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 Anti-Money Laundering Officer must meet the independence, authority, professionalism and integrity requirements set in this policy.

In order to guarantee the necessary independence and authority, the Anti-Money Laundering Officer is placed in the appropriate hierarchical and functional position, without neither direct responsibilities for any operational areas nor any hierarchical reporting line into the managers of these same areas. As regards professionalism requirements, 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 sector;
- capacity of managing the relationships with the Supervisory Authorities, the Investigating Authorities and the Corporate Bodies.

The Board of Directors assesses the characteristics of the candidate and, upon consultation with the Board of Statutory Auditors (or any other Control Body where present), approves its appointment. The Anti-Money Laundering Officer:

- participates, if required, in the meetings of the Corporate Bodies and reports directly to them, with no restrictions or intermediations;
- can access all the necessary corporate documentation in order to perform the tasks set out in the Supervisory regulations;

- verifies the effectiveness of procedures, organisational structures and systems, providing support and advice for Management decisions;
- represents the reference contact of FIU for all issues concerning the transmission of objective communications and the follow up on requests of information.

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.

3.2 Delegate Responsible for Reporting of Suspicious Transactions

The AML Officer is in charge of assessing the suspicious transaction reports received from company's departments and transmitting to the Financial Intelligence Unit (FIU) any reports that is considered to warrant attention.

In order to guarantee the appropriate independence of the reporting function and the fulfilment of the professionalism and integrity requirements, the role of Delegate responsible for Reporting of Suspicious Transactions is assigned to the Anti-Money Laundering Officer; this approach further allows for leveraging on the specific competences of this manager in the area of anti-money laundering, as well as his/her knowledge of the procedures for an effective Customers Due Diligence and AML risk profiling adopted by the company.

The role and responsibilities of the Delegate must be properly formalised and made public within the structure of the company.

The Delegate responsible for Reporting of Suspicious Transactions:

- has free access to the information flows for the Corporate Bodies and to the facilities involved in combatting money laundering and terrorism financing (e.g. requests arrived from the Judicial Authority and the Investigating Bodies);
- may permit, with the required confidentiality precautions and without disclosing the name of the subject which originated the reporting, the Managers of the impacted departments to know the identity of Customers that have been reported, also by means of suitable information reports, whenever the said information could be relevant for the acceptance of new Customers or the assessment of pre-existing Customers operations.
- manages, to the extent of his/her authority, relations with the Financial Intelligence Unit (FIU) and promptly follow up on any requests for further information;
- gives advice to the company's operating departments about the procedures to adopt in order to report any suspicious transactions or to abstain from executing the transactions;
- reviews, based on all available information, the reports on suspicious transactions received from the company's operating departments, the communications received from the Board of Statutory Auditors, the Supervisory Body and/or the Internal Audit Function as well as those that have been brought to his/her attention within the scope of his/her activities;

- forwards to FIU the reports deemed as well-founded, omitting the names of the subjects that have reported the transaction;
- files the reports not considered to require further investigation by accurately documenting the rationale of the decision;
- also makes use, as part of the assessment process, of any elements that may be retrieved from public information sources;
- communicates, by applying organisational methods suitable to ensure compliance with the confidentiality obligations set forth in the Anti-Money Laundering Decree, the outcome of the assessments to the subject who has originally reported the transaction;
- helps identify, for the Board of Directors approval, the measures needed to ensure the confidentiality in the handling and the storage of data, information and documentation relating to the reported transactions.

The Delegate, when assessing the suspicious transactions, may be supported by the staff of the Anti-Money Laundering Function.

The Delegate may authorise the Anti-Money Laundering Function staff to operate, under its responsibility and supervision, within the system in use to report suspicious transactions (Infostat-FIU) in accordance with the instructions given by the Financial Intelligence Unit (FIU) as well as within the profiling system in order to upgrade/downgrade the profile assigned to the analysed customers, as decided thereby.

According to the overall Group approach, in doValue Greece and in AAM Spain, the AML Officer is also appointed as Delegate responsible for Reporting of Suspicious Transactions. However, the doValue Greece AML Officer in specific cases may ask the advisory support of an independent committee whereas in AAM Spain the ultimate decision about the transmission of a SAR is usually taken by the OCI[5]. Finally, in AAM Portugal the AML Officer autonomously takes the decision about the communications to FIU and informs the BoD accordingly. In all the other companies of the doValue Group the decision about SAR is an exclusive responsibility of the AML Officer.

AAM Cyprus is not an obliged entity according to the local AML regulation, therefore the company is not required to report any suspicious transaction to the Unit for Combatting Money Laundering (i.e. MOKAS).

4. CUSTOMER DUE DILIGENCE

The doValue Group companies undertake customer due diligence process when:

- a continuous relationship is established;
- a single transaction or multiple linked transactions are occasionally executed by customers,

[5]The OCI is the internal control body of Altamira asset management

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). As a minimum standard, the following updated information/documentation has to be obtained

from private individuals

- personal details
- kind of profession
- identity card
- tax code
- financial sources
- beneficial owner and related personal details

from legal entities:

- company details
- kind of activity
- tax code
- vat code
- nace code
- legal representative and related personal details
- financial sources
- beneficial owner and related personal details

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 impossibility to comply with due diligence requirements entails 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, Portugal, 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 Enhanced Due Diligence

The enhanced due diligence requirements apply to customers with the highest levels of money laundering risk. Regardless of the specific criteria identified to conduct the customer profiling process, the following factors shall always be considered as high risk:

- customers based in high-risk third countries;
- cross-border correspondent banking relationships involving a credit or correspondent financial institution based in a third country;
- continuous relationships or transactions with customers and their beneficial owners who are politically exposed persons (PEP);
- customers who carry out transactions characterised by unusually high amounts or whose the purpose is not clear;
- continuous relationships established with trusts, trust companies, foundations;
- customers operating in the following sectors: gold dealers, gambling, provision of services related to the use of virtual money, currency exchange;
- customer transactions potentially in conflict with sanctions issued by international bodies;
- individuals subject to criminal investigations/proceedings and reported to the FIU.

Within the scope of criteria used for customer profiling, at least the following ones must be considered as relevant risk factors:

- continuous relationships established in unusual circumstances;
- customers and beneficial owners based in high-risk geographical areas;
- adverse reputational factors relating to the customer, the beneficial owner and the transaction's executor; in this context, connections with subjects involved in suspicious transaction reports or criminal proceedings must also be considered;
- company structures qualifying as asset interposition vehicles, such as foundations;

- companies that have issued bearer shares or are held by trustees;
- customers operating in the following economic sectors: health care, construction, mining, waste collection and disposal, renewable energy production, public procurement, arms trading, defence, military industry;
- services with a high degree of customisation, offered to customers with significant assets;
- cash transactions, depending on amount and typology.

Regarding the assessment of the geographical risk, profiling systems must be able to evaluate the risk associated with each country, as determined and regularly updated by the Anti-Money Laundering Function, considering at least the following risk factors:

- countries that reliable and independent sources consider to be lacking in effective anti-money laundering measures;
- countries and geographical areas assessed by reliable and independent sources as having a high level of corruption or permeability to criminal activities;
- countries subject to sanctions, embargoes or comparable measures adopted by relevant national and international bodies;
- countries and geographical areas financing or supporting terrorist activities or where terrorist organisations operate;
- countries assessed by reliable and independent sources as lacking in compliance with international standards on transparency and exchange of information for tax purposes.

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 operations;
- subjects belonging to high risk countries or involved in operations referable to such countries.

In all cases where this is deemed necessary, even in derogation of this Policy and regardless of the assigned AML risk profile, the Anti-Money Laundering Function may require the originating unit to carry out an enhanced due diligence on a customer/transaction.

The enhanced due diligence process consists of obtaining more information than in the case of The "standard" due diligence. In particular, further information 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.

In addition to the provisions of the previous paragraph #4, considering the complexity, the risk of money laundering and terrorism financing as well as the reputational risks inherently associated with the management of certain relationships/categories of transactions, at least the following measures must be taken as part of an enhanced due diligence process:

- *Politically Exposed Persons (PEPs):* when the client or the beneficial owner falls within the definition of PEP, the establishment or continuation of a continuous relationship or the execution of an occasional transaction shall be preventively authorised by the Head of the Anti-Money Laundering Function. All information necessary to ascertain the origin of the PEPs' assets and funds specifically used in the relationship or to execute a transaction shall be obtained. To this end, in the case of a continuous relationships, a client attestation should be collected and, according to a risk-based approach, the reported information should be verified by means of reliable documents, either from independent sources, provided by the client or publicly available. The enhanced due diligence standards must be applied to a PEP for one year after having lost this qualification (if applicable under national law). Nevertheless, in the case of a high risk of money laundering, the enhanced provisions shall continue to apply even after this period;
- *Trusts:* appropriate investigations shall be carried out in order to understand the reasonableness and the soundness of the entity. To this end the purposes declared in the articles of association/company bylaws must be considered and cross-checked with the economic and financial profile of the settlor and with any additional information available about the settlor and the other figures in the trust. The ultimate objective is to intercept any cases of improper use of the trust to achieve undeclared purposes (e.g. the subtraction of assets to creditors and tax authorities). The documentation to collect shall include at least the articles of association of the trust and any subsequent amendments.
- *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[6].

In the light of above, as provided by the V 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.

[6] Not applicable for the Greek legal entities

4.2 Simplified Due Diligence

Simplified due diligence standards can be applied to those categories of customers classified as low risk. In particular, simplified requirements can be applied to these categories of customers:

- banking and financial intermediaries as defined in the AML regulation - except for stockbrokers, insurance intermediaries and trust companies - as well as other banking and financial intermediaries based in EU or in an extra EU country that has adopted an effective anti-money laundering and anti-terrorism financing regime;
- public administrations, institutions or bodies performing public functions in accordance with European Union regulations;
- companies listed on regulated markets and subject to disclosure requirements, including those aimed at ensuring adequate transparency on ultimate beneficial owners.

In consideration of the differentiated business and the regulatory framework of the countries where the Group operates, each Group company has the possibility to identify, 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.
As a general provision the application of simplified due diligence measures requires the acquisition of a more limited set of supporting documentation and a lower frequency of review of the collected information/documentation. For example, according to the Italian Law, simplified due diligence measures may be applied when a payment is received from the Court of Appeals. In this case customer's identification duties can be fulfilled through the verification of authentic documentation certified by a public official (e.g. notary).

In any case, 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).

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.

4.3 Obligations to abstain

If the company is concretely unable to perform a customer due diligence, it cannot start, continue or pursue any relationship, transactions or professional services 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)[7]. Before making the suspicious transaction report to the FIU, and in order 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 company will not initiate any relationships, execute any transactions or provide professional services or terminate any existing business relationships or professional services with:

- customers who reside or have registered offices in countries that are "under embargo" as identified by the company and made available, on a quarterly basis, to all the employees and the external partners;
- credit or financial institutions located in non-EU countries that do not impose equivalent obligations to those ones provided under the EU directives;
- shell banks in any locations;
- service providers of shell banks;
- subjects who are, directly or indirectly, taking part of fiduciaries, trusts or anonymous companies (or controlled through bearer shares) located in high risk countries;
- companies that have issued bearer shares or are owned by anonymous shareholders;
- trusts where the available information about the beneficial owners of the trust, its nature or scope, are inadequate, inaccurate or not updated or where subjective or objective indicators evoke the use of this corporate structure to hide anomalous behaviours, also taking into consideration the recommendations provided by the competent authorities;

[7] the expression "termination of a business relationship already in place" in Greece means that the AML Function re-evaluates the business relationship, decides whether to provide favorable modification solution or not, to make a suspicious transaction report to the Financial Intelligence Unit (FIU) or to take further legal measures.

- relationships held in the name of trusts where the information available is inadequate, inaccurate or not updated with respect to the beneficial owners of the trust, its nature or scope;
- payment service providers (agents and/or money transfer companies) who do not carry out financial activities on an exclusive basis;
- services providers of virtual money or digital portfolio services;
- companies involved in the manufacturing of weapons or munitions;
- companies who are directly or indirectly owned by one of the above-mentioned categories of subjects.

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.

4.4 Customer profiling

The doValue Group adopts suitable procedures to determine the money laundering and terrorism financing risk profile to be assigned to each customer, based on the information collected and the analyses carried out, taking into consideration all the risks related to the Customer, the Representative and the Beneficial Owner as well as the risks related to products, services or transactions, and also geographic risks.

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 controls made available to the Group by the AML platform 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 collective knowledge of the customer.

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.

In particular the customer analysis shall be carried out in accordance with the approved AML international standards and taking into consideration 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;
- the customer behaviour during the execution of the occasional transaction or the establishment of the ongoing relationship or professional performance;
- the geographical area of residence or establishment of the customer or the counterparty;

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

- the type of transaction, continuous relationship or professional performance put in place;
- the procedures for carrying out the transaction, the ongoing relationship or the professional service;
- the amount of the transaction;
- the frequency and volume of transactions and the duration of the ongoing relationship or professional performance;
- the reasonableness of the transaction, the continuous relationship or the professional performance, in relation 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 and 4.2, 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 in order to enable an in-depth analysis of the case and leave to the ultimate decision of the Delegate responsible for Reporting of Suspicious Transactions, as a result of its own assessment, any actions to take, including the upgrade or the downgrade of the Customer's risk profile. 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, also to reflect the main developments in the area of reference and the leading practices in the market.

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

.

In accordance with the V European Directive, the approach to determine the scope and the frequency of reviewing existing customers is risk-based. However, given the higher relevance of money laundering terrorism financing risks and associated offences, it is recognised that this approach might not always allow for the timely detection and assessment of risks. It is therefore important to ensure that certain categories of customers, such as PEPs or people under investigation by judicial and/or regulatory authorities, are also monitored on an ongoing basis.

5. DATA RETENTION

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

The retained documentation shall allow, at least, to trace back uniquely:

- the date of establishment of the ongoing relationship;
- the identification data of 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 of time set forth by the national laws in force[8] which starts at the termination date of the ongoing relationship or the execution date of the occasional transaction.

6. SUSPICIOUS ACTIVITY REPORT

The Companies of doValue Group will promptly send the Financial Intelligence Unit (FIU) a suspicious transaction report when they knows, suspect, or have reasonable grounds to suspect that money laundering or terrorism financing transactions are taking place or were carried out or attempted, or in any case that funds used to execute those transactions, regardless of the amount, derive from criminal activities[9].

The employees who are actually in charge of the management of relationships with the Customers are therefore responsible for continuously monitoring the progression of the

[8] The retention period, for AML information/documents in Italy and Spain is 10 years, in Portugal is 7 years, in Greece is 5 years

[9] When AAM 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, AAM 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 AAM 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 AAM do is to report the transaction to its customer since the transaction relates to the clients of AAM customer.

relationship and the transactions put in place, and promptly sending to the Anti-Money Laundering Function, in accordance with the internally established procedures, a suspicious transaction report before executing the transaction. This is without prejudice to the cases where

a) the transaction must be carried out since there is a legal obligation to receive the documentation, or

b) the transaction cannot be postponed taking account of the normal operations, or

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

In order to facilitate identification of the 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 function, the AML Officer deems that the transaction must be sent the Financial Intelligence Unit (FIU), he/she will proceed with the transmission by omitting the name of the subject who has originated the report.

The companies of the Group adopt measures suitable to ensure the confidentiality of the reporting subjects; their names may only be revealed when the Judicial Authority, by issuing a reasoned decree in this regard, deems it essential to assess the offences to be prosecuted.

It is also prohibited to the subjects required to report any suspicious transaction and anybody else informed about the decision to proceed to a suspicious transaction reporting, to communicate this circumstance to the involved Customer or to any third parties, to forward additional information requested by FIU or any other information about the initiated or the possible investigation on money-laundering or terrorism financing issues.

7. 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 Delegate responsible for Suspicious Transaction Reporting 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 the confidentiality obligations, the Group Companies are allowed to exchange the information collected during the due diligence process, in order to avoid duplications in the fulfilment of due diligence obligations and replication of the same information requests that may cause disservices to customers.

8. METHODOLOGY FOR GROUP SELF ASSESSMENT

Group companies perform a self-assessment of the money laundering risk to which they are exposed. The self-assessment is conducted 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 to which they are exposed, also taking into account the elements provided by external information 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, in order to identify 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;
- **remediation 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.

On his side, 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, considering the indications set out in the annual report of the Anti-Money Laundering Function, 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 31st of March and to the Bank of Italy 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.

9. 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

10. REVIEWING AND UPDATING THE POLICY

The AML/CTF Function reviews this policy at least annually, updates it if and where necessary and submits the revised version of the document 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) in order to ensure their promptly and accurate reflection in the local framework of policies and procedures.