Our approach to Anti-Money Laundering and Countering Financing of Terrorism

Based on the AML/CTF Policy, version 2.2
approved by the Board of Directors on 18 February 2019

INTRODUCTION

The Ageas[1] policy on Combating Money Laundering (AML) and Financing of Terrorism and Proliferation (CTF), and Limitation of Cash usage (AML - CTF Policy) describes:

- The definitions of Money Laundering, Terrorist Financing and Proliferation;
- The Ageas **Anti-Money Laundering principles**;
- The standards to comply with, and the prohibited relationships;
- The input for setting up an **Anti-Money Laundering program**, based upon a risk-based approach, customer identification and acceptance principles, customer follow-up and ongoing monitoring (of customers and transactions), investigating and notifying to the competent authorities, record keeping, administrative organization and training…in the operational companies;
- **Practical examples on signals and alerts, and on how to deal with them**; and
- Requests for Management oversight and control.

The policy sets out the anti-money laundering (AML) principles and minimum standards for the prevention, contribution to detection and reporting of money laundering and terrorist financing. All references to money laundering and AML in the policy include terrorist financing (CFT), even when the latter is not specifically mentioned.

Tax crimes, criminal activities and corruption, countering the financing of the proliferation of weapons of mass destruction, and complying with (supra)national financial embargoes are included in the EU Directive / the Belgian Law as predicate offence as well, and are thus in scope of the policy, even if not specifically mentioned.

N.B.:
For the legibility of this document, “AML” will refer to all above mentioned offences.

The policy creates a framework for structuring the processes, procedures, controls and systems deemed by Ageas entities to be appropriate for applying the policy’s principles and standards. It is aimed at protecting against the reputation risks and legal risks to which Ageas might be exposed as a result of money laundering and terrorist financing.

SCOPE OF THE POLICY

The policy applies to ageas SA/NV and its Subsidiaries, and on a best effort basis in the Affiliates.

In case of discrepancy or deviation from the principles set out in the policy, it must be notified to the Group Director Compliance.

The policy is applicable to all Ageas employees, agents and contractors working for or on behalf of Ageas.

1 “Ageas” designates the conglomerate of companies forming a group of which ageas SA/NV is the top holding. It encompasses the mother company, all its subsidiaries and affiliates. Subsidiary means an entity in which ageas SA/NV, directly or indirectly, has a majority shareholding and holds operational control, and Affiliate means any entity in which ageas SA/NV, directly or indirectly, has a minority shareholding and holds no operational control.

DEFINITION

The definitions take into account the topics mentioned in the EU directive.

AML

In essence, money laundering is the process of making dirty money look clean. Money launderers conceal or disguise the existence, illegal source, movement, destination, or illegal application of illicitly derived property or funds to make them appear legitimate.
Money laundering typically involves three stages:

- the placement of illegally derived funds or assets, such as cash, securities or precious metals, into the legitimate financial system;
- the layering of transactions: the illegally derived funds or assets are moved through a bank, a securities account, a series of accounts, or to a third party to disguise their source, ownership and location; and
- the integration of the funds into society in the form of holdings that appear legitimate.

The criminal offences that lead to money laundering are determined by local legislation and regulations on anti-money laundering.

Fraud against the financial interest of the European Union, as well as serious fraud tax, organized or not, and social fraud fall in scope as well.

CTF

Terrorist financing means the provision or collection of funds, by any means, directly or indirectly, with the intention that they should be used or in the knowledge that they are to be used, in full or in part, in order to carry out an act of terrorism.

AML/CTF may be linked to criminal activities in the sense of article 4, 23° of the Belgian Act of 18 September 2017, as any type of participation in the commission of such related offense can lead to money laundering.

PRINCIPLES

Ageas conducts business only with customers and beneficial owners whose identity and source of income and wealth have been established in accordance with local legislation and regulations.

Ageas wants to limit business relationship and transactions involving high-risk third countries.

Ageas subjects customer relationships and transactions that it deems to present an increased money laundering risk to higher scrutiny through enhanced due diligence and increased monitoring procedures.

Ageas monitors and, where appropriate, investigates customer transactions to prevent and contribute to the detection of unusual or suspicious activity or behaviour; to this end, Ageas implements appropriate monitoring procedures and systems in its offices.

Ageas notifies suspicious activity or behaviour to the competent Authorities in accordance with local legislation and regulations.

Pursuant to these principles and to its statutory and regulatory obligations, Ageas

- does not accept assets and transactions that are known or suspected to be the proceeds of a criminal offence that qualifies as money laundering;
- does not conduct business relationships, directly or indirectly, with money launderers, terrorists or their financiers;
- does not enter into or maintain business relationships with people or entities that require Ageas to open an anonymous account or an account under a fictitious name
- does not enter into or maintain business relationships with people or entities that it could not identify properly;
- does not enter into or maintain business relationships with shell banks or with banks that are known to permit their accounts to be used by shell banks; and,
- will not keep anonymous accounts (or similar products).

AML PROGRAMME

Each Ageas entity must implement an AML program to ensure that its organisation is in full compliance with the relevant local legislation and regulations. This program must refer specifically to the processes, procedures, controls and systems that are necessary to mitigate the risks associated with customers who may be involved in laundering money or financing terrorism. It is based essentially and primarily on preventive measures.

The AML program must include at least the following processes:

- Internal policies;
- Risk-based approach; controls and procedures; model risk management practices;
- Customer identification and acceptance, due diligence;
- Customer follow-up (on-going monitoring and regular reviews);
- Investigating and notifying to the Competent Authorities;
- Record keeping;
- Administrative organisation and training;
- Screening procedures to ensure high standards when hiring employees;
- Internal control; Compliance management and Independent audit function to test the AML program and system.

COMPLEMENTARY ROLE OF LOCAL AML POLICIES AND PROCEDURES

Ageas AML Standards set out in the policy must be supplemented by appropriate local procedures, based on local legislation and regulations and on local requirements.

RISK-BASED APPROACH: THE ENTERPRISE-WIDE RISK ASSESSMENT (EWRA)

The principle underlying the risk-based approach is that resources should be directed on the basis of priority so that the greatest risks receive the greatest attention. It permits less stringent preventive measures if the AML/CFT risks are low but stipulates tougher measures if those risks are high.

The approach consists of a comprehensive exercise that begins with identification of potential money laundering risks organisationally at the level of the entity as a whole, including all relevant business lines. This high-level analysis is translated into more detailed procedures applying to individual customers and their transactions. This

makes it possible to focus on those customers and transactions that potentially pose the greatest risk of money laundering. Risk identification, gap-analysis and action plan are the cornerstones of the EWRA.

Each Ageas entity must develop, implement, and document an enterprise wide risk-based approach to managing money laundering and terrorist financing risks.

However, where particular individuals, organisations, other entities or countries are the subject of financial embargoes or terrorist finance sanctions issued by the United Nations, the European Union, the OFAC or other competent or local authorities, the obligations are absolute and are not subject to a risk evaluation. Nor is a risk-based approach permitted for notification of activities identified as suspicious.

With regard to estimation of the risk posed by a particular customer or transaction, the risk-based approach must also take into account any risk variables specific to that particular customer or transaction, such as the value of the assets deposited or the size of transactions undertaken.

The outcome of the risk assessment will have a knock-on effect on internal monitoring activities, such as customer identification, acceptance and follow-up procedures and their related controls, e.g. management clearance for major international fund transfers for high-risk customers.

The performed EWRA is to be validated by the Executive Committee, embedded in a clear methodology (in writing) and results must be documented and reviewed regularly; and made available to all relevant stakeholders.

CUSTOMER IDENTIFICATION & ACCEPTANCE, MONITORING AND FOLLOW-UP

Ageas wants to understand and, as appropriate, obtain information on the purpose and intended nature of the business relationship.

Therefore, each Ageas entity must have written customer identification and acceptance policies and procedures.

These must identify the customer due diligence requirements appropriate to each situation and commensurate with the AML risk profile, with particular attention being paid to high risk customers. They must set out how to proceed in general and for specific cases.

When enhanced due diligence is required, reasonable measures to establish the source of wealth and source of funds, and a senior management approval for establishing (or continuing, for existing customers) such business relationship have to be obtained; if (the beneficial owner of) the beneficiary is a PEP[2], senior management must be informed before pay-out of policy procedures.

The acceptance procedures always include “filtering” (via automatic or manual means) the new customers, agents, and beneficial owners against watch lists of particular individuals, organisations, other entities or countries that are the subject of financial embargoes or terrorist finance sanctions, issued by the United Nations, the European Union, the OFAC or other competent or local authorities (e.g. UN Resolutions 1267, 1373 and 1988). Based on all the information obtained, the customer must be allocated a risk category and adequate measures to mitigate the risk must be taken.

2 Politically Exposed Person.

Each Ageas entity must have written customer follow-up policies and procedures. They must indicate clearly that all existing customers must be followed-up on the basis either of an ongoing monitoring process or of a regular review. They must also specify how this must be done.

ON-GOING MONITORING

On-going monitoring of existing customers means:

- Keeping the existing customer identification files complete and up-to-date.
- Filtering the existing customer base to ensure that customers' names do not appear on the relevant watch lists.

On-going monitoring of customers transactions means:

- Monitoring the customer's transactions by applying a risk-based approach to ensure that they are consistent with Ageas' knowledge of the customer, the business and risk profile and, if necessary, identifying the source and destination of funds, thereby aiming at detecting atypical and unusual transactions.
- Filtering the customer's transactions to ensure that the beneficiaries and other parties in the transaction do not appear on the relevant watch lists.
- Other forms of ongoing monitoring, such as ensuring, by appropriate means, compliance with EU Regulation 2015/847 on payer data accompanying fund transfers, designed to implement the seventh special recommendation of the FATF, and including the full traceability of transfers of funds, and information on payers and payees.

REVIEW OF THE CUSTOMER RELATIONSHIP

Review consists of a regular evaluation of the customer relationship from the point of view of compliance in order to be able to confirm or change the risk profile and determine whether the relationship can be continued or must be terminated. This regular review is done in addition to and separately from the updating of the customer's identification data and the detection of atypical transactions. The review must be done for all high-risk customers at the very least.

INVESTIGATING AND NOTIFYING COMPETENT AUTHORITIES, AND RECORD KEEPING

Unusual or atypical transactions or attempts to undertake such transactions must be investigated as soon as they are identified, regardless of the means of identification. Each Ageas entity must establish a unit devoted to this task. This unit must determine whether the activity is suspicious after undertaking any investigations that it deems appropriate. It must document all investigations.

When the name of a person is found to match a name on a black list, this must be notified immediately to the Compliance Officer who must examine whether it is relevant; where this is the case, the assets of the person concerned must be frozen.

The Compliance Officer, or his delegate for these matters, is responsible for filing reports on suspicious activities and/or blacklisted persons with the competent authorities (for example the local Financial Intelligence Unit, the Ministry of Finance or the Police) in accordance with prevailing legislation and regulations. All suspicious transactions, including attempted transactions, shall be reported to the relevant control authority.

Ageas employees are prohibited from disclosing to a customer or third party their suspicions, the existence of an investigation or the filing of a report.

Unless prohibited by local legislation or regulations, local Compliance must report immediately to Group Compliance any issue that may pose substantial legal, regulatory or reputation risks for Ageas or one of its subsidiaries.

Each Ageas entity must store the documents to be collated for compliance with customer due diligence obligations in a way which makes them easy to recover. Unless longer retention periods are set by local legislation or regulations, each Ageas entity must hold those documents for a period of at least ten years from the date on which the business relationship with the customer comes to an end, or after the date of the occasional transaction.

ADMINISTRATIVE ORGANISATION, STAFF SCREENING AND TRAINING

In order to implement the Ageas AML Principles and Standards set out above,

- each Ageas entity must put in place an adequate administrative organisation and appropriate internal control procedures. More specifically, the Compliance function is responsible for monitoring to ensure that all obligations arising from the policy are met and it has the final say on AML-related issues that it deems to be critical, including customer acceptance and review; and
- each Ageas entity must develop AML awareness by providing relevant staff with appropriate and regularly updated AML training consistent with the policy and prevailing local AML legislation and regulations. Training must teach Ageas personnel how to recognize unusual or atypical customers or operations, and how to proceed in such cases.

Each Ageas entity must include in its recruitment procedure for staff and authorized agents an appropriate verification of their trustworthiness, according to and in the limits of the local prevalent laws and regulations.

LOCAL AML RULES

Each Ageas entity must comply with specific local AML rules. Consequently, each Ageas entity must adapt these Group AML Standards to the specific constraints imposed by local legislation, regulations or market circumstances. In the event that one or more Ageas entities established in different countries serve the same customer, the customer due diligence procedures put in place must comply with obligations of all the jurisdictions concerned.

THE ULTIMATE BENEFICIAL OWNER (UBO) REGISTER

Companies and other legal entities are obliged to collect and report information on their ultimate beneficial owners (UBO) which is to be stored in a central register per European Member State. This register is mandatory and is intended to allow entities to identify their beneficial owner(s). An UBO is any individual who ultimately owns or controls the company. To qualify as an UBO an individual must hold voting or ownership rights of more than 25% in the legal entity (directly or indirectly), or controls the legal entity via other means (e.g. through shareholders agreement). If no UBO can be identified, or if there is any doubt that the persons identified are the effective beneficial owners, then the natural person(s) holding the position of senior managing official will be registered as the UBO.

PROTECTION MECHANISM

Privacy

All personal data to be processed within the framework of the policy, e.g. data to be included in the UBO register will be processed lawfully, fairly and in a transparent manner.

Laws on the protection of individuals with regard to processing of personal data and on the free movement of such data will be complied with. This includes data protection and privacy-related rules and regulations, such as the General Data Protection Regulation, and relevant Ageas policies.

On implementation of the 5th EU Directive, processing of personal data shall be considered a matter of public interest under the (EU) General Data Protection Regulation.
It shall not prevent disclosure between entities belonging to the same group, provided that they fully comply with this group-wide policy.

PROTECTION AGAINST RETALIATION

No staff member who in good faith reports a wrongful situation or an incident shall suffer harassment, retaliation or adverse employment consequence (e.g. termination of employment or any other improper deviation from the employment contract, negative appraisal, mutation, blocking career perspectives…), as a consequence of his report; he should be protected against any threat or hostile act, and in particular any prejudicial or discriminatory employment actions.

GOVERNANCE

Senior management and line management are responsible and accountable for ensuring that the employees under their supervision are complying with the Ageas AML Policy, in accordance with the supervisory requirements in their locations.

To this end, Ageas vigorously complies with the anti-money laundering and anti-terrorist financing legislation of each jurisdiction in which it conducts its operations and all Ageas entities provide full assistance in enforcement of the applicable laws and regulations.

Consistent with these commitments, Ageas and its employees are prohibited from engaging in or facilitating, in any manner whatsoever, money laundering or terrorist financing. They are also required to exercise the appropriate level of care and diligence when dealing with customers in order to identify suspicious behaviour and transactions, and to avoid any involvement in money laundering or terrorist financing.

Senior Management will take into account that when reliance on third parties is permitted, the ultimate responsibility for AML/CFT measures remains with the entity relying on the third party.

Senior Management will prohibit any person or entity they are responsible for to make available any funds or other assets, economic resources, or financial or other related services, directly or indirectly, wholly or jointly, for the benefit of persons and entities (owned or controlled, or acting on behalf of designated persons) with whom dealing prohibitions have been issued.

As Ageas is required to implement group-wide policies and procedures for sharing information for money-laundering and terrorist financing purposes, Group Compliance will give reasonable assurance that, at least, majority owned subsidiaries apply AML/CFT measures consistent with the policy.

Each Operational Company (through the Board of Directors of ageas SA/NV, and the Boards of the respective subsidiaries) shall designate a responsible AML/CFT officer (subject to the Fit & Proper rules), reporting directly to a member of the Management Committee. He/she will issue, at least once a year, a activity report to the Management Committee, copying the Group Compliance Officer. This report shall allow the Management to form

itself a judgement concerning the scope of the traced attempts of money-laundering or financing of terrorism, concerning the appropriate character of the developed administrative organisation and internal control and concerning the collaboration of the services of the venture to the prevention.

In addition a person at senior management level shall be designated, generally responsible for ensuring compliance of the entity with AML rules.