# GLOBAL ANTI-MONEY LAUNDERING AND TERRORIST FINANCING POLICY

Applicable to:

Alkemya Luxembourg S.à r.l.

August 2025

| Date | Version | Changes made | Responsible | Approved by |
|---|---|---|---|---|
| 06 August 2025 | V1.0 | First version | Cristina Rubino | Carlo Guido Della Peruta |
| | | | | |

For internal use only

# Contents

## 1. OBJECT

The purpose of the present global anti-money laundering and counter-terrorist financing policy (the "**Policy**") is to describe the measures implemented by Alkemya Luxembourg S.à r.l. ("**Alkemya**") in order to (**i**) prevent being used for money laundering or terrorist financing ("**ML-TF**") purposes and to (**ii**) avoid criminal sanctions, fines, financial and reputational damage which can result from a breach to the anti-money laundering and terrorist financing ("**AML-CTF**") framework.

The objectives of this Policy are to identify, mitigate and manage AML-CTF risks and ensure that Alkemya properly implement AML-CTF measures. The Policy describes the principles of AML-CTF, Alkemya's obligations as well as the processes put in place for accepting and entering into a business relationship[1] with customers[2] or counterparties, the identification, evaluation and analysis of risks, the monitoring of business relationships, the procedure in the event of suspicion or indication of money laundering or terrorist financing ("**ML-TF**"), the procedure for staff training, record-keeping, cooperation with the competent authorities and sanctions' screening.

The Policy should support the employees of Alkemya in adhering to the business principles of the company when dealing with modes of behavior which could potentially be connected to ML-TF. Above all, these rules of conduct should help the employees not to act in breach of duty or even in a criminal manner. Therefore, in the first instance, these rules of conduct should further increase employees' awareness of risk, provide them with the means of appropriately dealing with the relevant risks and with decision making criteria when undertaking practical day-to-day business.

As stated above, the Policy covers and is applicable to all Alkemya's staff and can be accessed by all.

The Policy shall be updated regularly and, notably, in the event of relevant legislative or regulatory changes.

The Policy is approved by Mr. Carlo Guido Della Peruta.

## 2. LEGAL BASIS

[1] In line with Article 3 (13) of AML 4 the concept of "business relationship" refers to "*a business, professional or commercial relationship which is connected with the professional activities of an obliged entity and which is expected, at the time when the contact is established, to have an element of duration*".

[2] In line with Article 1 (1) of the CSSF Regulation 12-02, the concept of "customers" must be understood as referring to any natural or legal person with whom a business relationship exists or for whom an occasional transaction is carried out, including any person purporting to act on behalf of the customer.

The AML-CTF framework derives from the application of international, European and national legislation. The main applicable legislative and regulatory sources at international and European levels are described in more detail below.

### 2.1. International texts

- Recommendations from the Financial Action Task Force ("**FATF**");
- Publication from the FATF.

### 2.2. European texts

- **Directive (EU) 2014/42** of the European Parliament and of the Council of 3 April 2014 on the freezing and confiscation of instrumentalities and proceeds of crime in the European Union;

- **Directive 2015/849** of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No. 648/2012 of the European Parliament and of the Council and Commission Directive 2006/70/EC, as amended ("**AML 4**");

- **Commission delegated regulation 2016/1675** of 14 July 2016 supplementing Directive 2015/849 of the European Parliament and of the Council by identifying high-risk third countries with strategic deficiencies, as amended;

- **Directive (EU) 2017/541** of the European Parliament and of the Council of 15 March 2017 on combating terrorism;

- **Council Regulation (EU) 2018/1542** of 15 October 2018 on restrictive measures against the proliferation and use of chemical weapons, as amended;

- **Regulation (EU) 2018/1672** of the European Parliament and of the Council of 23 October 2018 on controls of cash entering or leaving the Union, as amended;

- **Directive (EU) 2018/1673** of the European Parliament and of the Council of 23 October 2018 on combating money laundering by criminal law ("**AML 5**");

- **Council Implementing Regulation 2019/84** of 21 January 2019 implementing Regulation 2018/1542 concerning restrictive measures against the proliferation and use of chemical weapons;

- **Commission Delegated Regulation 2019/758** of 31 January 2019 supplementing Directive (EU) 2015/849 of the European Parliament and of the Council with regard to regulatory technical standards for the minimum action and the type of additional measures credit and financial institutions must take to mitigate money laundering and terrorist financing risk in certain third countries;

- **Regulation (EU) 2019/452** of the European Parliament and of the Council of 19 March 2019 establishing a framework for the screening of foreign direct investments into the Union;

- **Directive (EU) 2019/1153** of the European Parliament and of the Council of 20 June 2019 laying down rules facilitating the use of financial and other information for the prevention, detection, investigation or prosecution of certain criminal offenses;

- **Joint guidelines issued by the three European supervisory authorities** (EBA / ESMA / EIOPA) on the risk factors of money laundering and terrorist financing;

- **Regulation (EU) 2023/1113** of the European Parliament and of the Council of 31 May 2023 on information accompanying transfers of funds and certain crypto-assets;

- **Directive (EU) 2024/1203** of the European Parliament and of the Council of 11 April 2024 on the protection of the environment through criminal law;

- **Directive (EU) 2024/1260** of the European Parliament and of the Council of 24 April 2024 on asset recovery and confiscation;

- **Council Implementing Regulation (EU) 2024/1778** of 24 June 2024 implementing Regulation (EU) 2019/796 concerning restrictive measures against cyberattacks threatening the Union or its Member States.

### 2.3. National texts

- **Criminal Code** (Articles 506-1 and following);

- **Law of 19 February 1973** on the selling of medicinal substances and the fight against drug addiction, as amended (the "**Law of 1973**");

- **Law of 5 April 1993** on the financial sector, as amended (the "**Law of 1993**");

- **Law of 12 November 2004** on the fight against money laundering and terrorist financing, as amended (the "**AML Law**");

- **Grand-Ducal Regulation of 1 February 2010** providing details on certain provisions of the AML Law, as amended (the "**Grand-Ducal Regulation of 2010**");

- **Law of 27 October 2010** strengthening the legal framework in the fight against money laundering and the terrorist financing, as amended;

- **CSSF Regulation n°12-02 of 14 December 2012** on the fight against money laundering and terrorist financing, as amended (the "**CSSF Regulation n °12-02**").

- **Law of 13 January 2019** establishing a register of beneficial owners, as amended;

- **Grand-Ducal Regulation of 15 February 2019** on registration modalities, administrative fees and access to the Register of Beneficial Owners;

- **Law of 25 March 2020** amending *i.a.* the AML Law;

- **Law of 10 July 2020** establishing a Register of *fiducies* and trusts, as amended;

- **Law of 19 December 2020** on the implementation of restrictive measures in financial matters, as amended.

- **Law of 16 July 2021** on the organisation of controls on the physical transport of cash entering, transiting or leaving the Grand Duchy of Luxembourg and implementation of Regulation (EU) 2018/1672 of the European Parliament and of the Council of 23 October 2018 on controls of cash entering or leaving the Union and repealing Regulation (EC) No 1889/2005.

## 2. MONEY LAUNDERING: DEFINITION

Money laundering is a technique consisting of transforming money from criminal and illegal activities into so-called "clean" money whose origin is no longer traceable.

Money laundering presupposes the existence of an underlying offence (or predicate offence) whose purpose and proceeds may give rise to a money laundering offence.

Money laundering consists of **3 stages**:
- placement: placing money from an illicit source in the financial or commercial sector;
- layering: multiplying operations to avoid detection and to create a diversion;
- integration: investing or using the money in the legal economy. This stage allows funds from an illicit activity to be given a licit origin.

At the end of the process, funds that originated from an illicit activity are laundered, *i.e.* these funds have taken on a licit appearance.

AML-CTF measures are not intended to prevent the illicit activities from which the funds originate but rather to prevent these funds from entering the financial/economic sector with a view to transforming their origin and use thereafter. Therefore, the AML-CTF measures focus on the first two steps (*i.e.* layering and integration).

## 3. LEGAL DEFINITION

Money laundering is defined under Article 506-1 of the Criminal Code and Article 8-1 of the 1973 Law.

**Article 506-1 of the Criminal Code reads as follows:**

"*Those who knowingly facilitate, by any means, the false justification of (…) the origin (…) of the goods forming the object or proceeds, directly or indirectly, [of one or more of the primary offences] or constituting any pecuniary advantage whatsoever from one or more of these offences.*

*Those who knowingly assisted in the placement, concealment, (...) or conversion (…) of the goods (…) forming the direct or indirect object or proceeds of the offences or constituting a pecuniary advantage derived from one or more of these offences.*

*Those who acquired, held or used the good (…) which was the object or direct or indirect proceeds of the [primary] offences or which constituted any pecuniary advantage derived from one or more of these offences, knowing, at the time of receipt, that it derived from one or more of the [primary] offences or from participation in one or more of these offences.*"

In this context, primary offences are listed in Article 506-1 (1) of the Criminal Code and also include all offences punishable by an imprisonment sentence of at least six (6) months.

**Article 8-1 of the 1973 Law reads as follows:**

"*The following shall be punished by an imprisonment of one to five years and a fine of 1,250 to 1,250,000 euros, or by one of these sentences only:*

1) *those who have knowingly facilitated by any means the false justification of the nature, origin, location, disposition, movement or ownership of goods or incomes derived from any of the offences mentioned under Article 8 (1), (a) and (b) [of the 1973 Law];*
2) *those who knowingly assisted in the placement, concealment, disguise, transfer or conversion of the direct or indirect proceeds of any of the offences referred to in Article 8 (1), (a) and (b) [of the 1973 Law];*
3) *those who have acquired, possessed or used the object or the direct or indirect proceeds of one of the offences referred to in Article 8 (1), (a) and (b) [of the 1973 Law], knowing, at the time they received it, that it was derived from one of these offences or from participation in one of these offences;*
4) *the offences referred to in point (1) to (3) are also punishable:*
    - *where the primary offence was committed abroad;*
    - *where the perpetrator is also the perpetrator or accomplice of the primary offence.*
5) *The offences referred to in points (1) to (3) shall be punishable independently of any prosecution or conviction for any of the offences referred to in Article 8 (1), (a) and (b) [of the 1973 Law];.*

*The same sentences shall be imposed on those who acquire, hold or use goods knowing, at the time they receive it, that they originated from one of the offences mentioned in Article 8 (1), (a) and (b) [of the 1973 Law] or from participation in one of those offences."*

Attempts and complicity are punishable by the same sentences as those mentioned above.

**Material element**

Money laundering consists in any act relating to the proceeds or goods derived from the primary offence, *i.e.* any benefit derived from the primary offence. The primary offences are listed under Annex A to this Policy.

**Moral element**

To commit a money laundering offence, the intentional element is decisive. The mere act of laundering is not sufficient to characterise the offence of money laundering, there must be knowledge of the illicit origin of the funds or property and the will to commit the act of laundering.

**Acts committed abroad**

The offence of money laundering is punishable in Luxembourg even where the primary offence to money laundering was committed abroad.

**Exception**: the primary offence must be punishable in the country where it was committed (except for offences where the law allows prosecution even if they are not punishable in the country where they were committed).

The offences referred to in the aforementioned Article 506-1 of the Criminal Code are also punishable when the perpetrator is also the perpetrator or accomplice of the primary offence.

## 4. TERRORIST FINANCING: DEFINITION

Terrorist financing refers to any financial support to terrorism or to those who support, plan or commit terrorism.

Terrorist financing is an opposite concept to money laundering as it involves the distribution of funds, which may be legal, to terrorists (in order to finance criminal activities).

**Article 135-5 of the Criminal Code**

" *(1) Constitutes an act of terrorist financing, the fact to provide or collect, by any means, directly or indirectly, unlawfully and intentionally, funds, securities or goods of any kind, with the intention that they should be used or in the knowledge that they are to be used, in whole or in part, for the purposes of committing or attempting to commit one or more of the in paragraph (2) of this article, even if they have not actually been used to commit or attempt to commit any of those offences, or if they are not related to one or more specific terrorist acts.*

*(2) Paragraph (1) of the present Article refers to the offences provided for by:*

- *Article 112-1, 135- 1 to 135-4, 135-9, 135-11 to 135-16 and 442-1;*
- *Articles 31 and 31-1 of the law of 31 January 1948 on the regulation of air navigation, as amended;*
- *Article 2 of the law of 11 April 1985 approving the Convention on the physical protection of nuclear material, opened for signature in Vienna and New-York on 3 March 1980, as amended;*
- *Article 65-1 of the law of 14 April 1992 establishing a disciplinary and Criminal Code for the Navy, as amended.*

*(3) It is also an act of financing terrorism to provide or collect by any means, directly or indirectly, unlawfully and deliberately, funds, securities or goods of any kind, with the intention that they should be used or in the knowledge that they will be used, in whole or in part, by a terrorist or terrorist group, including in the absence of a link with one or more specific terrorist acts, even if they have not actually been used by the terrorist or terrorist group.*

*(4) The term "funds" shall include goods of any kind, whether tangible or intangible, movable or immovable, acquired by any means, and legal documents or instruments in any form, including electronic or digital form, which evidence a right of ownership of, or interest in, such property, and bank credits, travellers' cheques, bank cheques, money orders, shares, securities, bonds, drafts and letters of credit, economic resources, commodities and other natural resources, without this list being exhaustive.*"

Generally, money laundering operations involve large sums of money, whereas transactions related to terrorist financing are rather smaller.

## 5. SCOPE

The Policy shall apply to Alkemya. The Policy shall apply to all businesses of the group to which Alkemya belongs.

The Policy is binding for all employees of Alkemya. For the purposes of the Policy, the term "employee" shall also include executive employees and members of Alkemya's executive bodies.

In this context, the AML-CTF obligations to be complied with may be categorised as follows:

- the obligation to know the customer (or counterparty);
- the obligation to have an internal organisation; and
- the obligation to cooperate with the competent authorities.

## 6. ROLES AND PERSONS RESPONSIBLE FOR COMPLIANCE WITH AML/CFT OBLIGATIONS

The Policy covers all professional duties and include, among other things, the precise definition of the respective responsibilities of the various staff functions with regard to AML-CTF, as well as the procedure for appointing a person responsible for compliance with the professional obligations in relation to AML-CTF (the "**RR**") and a compliance officer ("**RC**").

This Section covers the AML-CTF roles and responsibilities at the level of Alkemya. Each member of management and employee is responsible for compliance with the provisions of this Policy and must exercise vigilance in relation to the risk of ML-TF.

### 6.1. Managers

The Managers of Alkemya are responsible for the organisation and supervision of AML-CTF. In particular, the Managers regularly initiate a reassessment of all high-risk business relationships, at least once a year. The Managers approve the definition of ML-TF of Alkemya.

The Managers are ultimately responsible for the implementation of an efficient AML-CTF system which complies with the AML-CTF obligations of Alkemya.

The Managers approve this Policy. The Managers review and, if necessary, approve annually any change to this Policy proposed by the RC as well as the report prepared by the RC (as detailed below).

The Managers approve any entry into a relationship with a potential high-risk customer according to Alkemya's AML-CTF definitions.

A member of the Managers is appointed as RR, in line with the below Section 6.2. of the Policy.

### 6.2. Compliance function

In line with Article 4 (1) of the AML Law, Alkemya appoints two different persons in charge of AML-CTF matters:

(i) a **person responsible for compliance with the professional obligations** in relation to AML-CTF, (*responsable du respect*, hereinafter referred to as the "**RR**")

who must be appointed amongst the members of Alkemya's management bodies; and

(ii) a **compliance officer** at a hierarchical level **in charge of the control of the professional obligations** (*responsible du contrôle du respect*, hereinafter referred to as the "**RC**").

Each RR and RC must have the professional experience, knowledge of the Luxembourg legal and regulatory framework relating to AML-CTF, the hierarchy and powers within Alkemya (including the power to access on a timely basis the identification data of customers of other information and documentation required by the due diligence measures), as well as the availability necessary to the effective and autonomous exercise of their functions.

**The RR**

The RR is the representative of the Managers for AML-CTF matters and is in charge of approving the AML-CTF supervisory system.

The situations in which the RR's approval is required include *i.a.*:

- high-risk customers, including PEPs;
- customers identified as having a very high-risk relationship with a PEP;
- customers identified as having a relationship with a high-risk country.

**The RC**

The RC is responsible for the compliance function of Alkemya as well as for the control of the compliance of Alkemya with Alkemya's AML-CTF obligations. The accumulation of the function of RC with one or more other functions must not jeopardise the independence, objectivity and decision-making autonomy of the RC. The workload of the RC is adapted so that the efficiency of the AML-CTF framework of Alkemya is not compromised.

The RC acts as the focal point for all activities in Alkemya relating to AML-CTF.

The RC must act independently in its role and has free and direct access to all relevant regulatory bodies and appropriate law enforcement agencies. The RC is the privileged contact person for the competent AML-CTF authorities regarding all AML-CTF matters and for cooperating with the competent authorities with regard to the application of financial restrictive measures. The RC is in charge of the transmission of any information or statement to these aforementioned authorities.

The RC may, without prejudice to his/her responsibility, delegate the exercise of his/her function to one or more employees connected to Alkemya, provided that such employees have the professional experience, knowledge of the Luxembourg legal and regulatory framework relating to AML-CTF, the hierarchy and powers within the entity (including the power to access on a timely basis the identification data of customers and other information and documentation required by the due diligence measures), as well as the availability necessary to the effective and autonomous exercise of their functions.

In practice, the responsibilities of the RC include:

- ensuring the quality of the AML-CTF controls carried out by the first line of defence and, as for the second line of defence, verifying compliance by Alkemya with all AML-CTF obligations;
- where relevant, controlling the compliance with Alkemya's branches and majority-owned subsidiaries of Alkemya in Luxembourg and abroad by analysing, among others, the summary of all the reports of the audit missions, and, where appropriate, of the compliance function of these entities that Alkemya must obtain;

- ensuring compliance by Alkemya with the group-wide policies, procedures and measures concerning, in particular, data protection and sharing of information within the group for the purposes of AML-CTF in accordance with applicable legal provisions in Luxembourg;
- making suspicious activity reports as soon as practicable. The decision on whether or not to report a suspicion to the financial intelligence unit lies with the RC who must not be influenced by any other member of the senior management;
- transmitting any information or statement to the aforementioned authorities;
- preparing, implementing and ensuring the realisation of the continuing training and awareness-raising programme of the personnel;
- reporting in writing on a regular basis and, if necessary, on an ad hoc basis to the RR, to the authorised management and, where appropriate, to the Managers of Alkemya – such reports must focus on the follow-up of the recommendations, problems, shortcomings and irregularities identified in the past as well as the new problems, shortcomings and irregularities identified. Each report must specify the risks related thereto as well as their seriousness (measuring the impact) and propose corrective measures, as well as in general the position of the persons concerned as well as allow the assessment the scale of the suspicions or reasonable grounds for suspicion of money laundering, an associated predicate offence or terrorist financing which were identified and expressing a judgement on the adequacy of this Policy, other AML-CTF procedures and systems and on the collaboration between Alkemya's departments as regards AML-CTF;
- preparing, at least once a year, a summary report on his/her activities and his/her operation which must be submitted to the RR, the authorised management and the Managers;
- submitting to the CSSF, on an annual basis, the summary report referred to in the previous bullet point within five months following the end of Alkemya's financial year.

### 6.3. Responsibilities of Alkemya's employees

All employees have to comply with the elements set out in this Policy. Where relevant, all employees will receive training to correctly apply the measures set out in the Policy and in order to ensure that they comply with their AML-CTF obligations under any circumstances.

Any suspicion related to a potential or existing customer must be communicated to the RC within 24 hours of its discovery. The employee is required to report all suspicious elements to the RC in order to enable him to determine whether it will be necessary to submit a suspicious activity report to the CRF.

If there are any questions regarding the implementation of the measures described in this Policy, please contact one of the members of the Compliance team:

- RR: Mr Carlo Guido Della Peruta;

- RC: Mrs Cristina Donna Rubino.

## 7. RISK ASSESSMENT

### 7.1. Risk assessment

Alkemya is committed to combating financial crime and ensuring that its products are not misused for the purposes of ML-TF.

Alkemya takes appropriate steps to identify, assess and understand the risks of ML-TF to which it is exposed. The risk factors to be taken into account when assessing the risks of ML-TF to which Alkemya is exposed can be classified in the following categories:

- customers;
- countries/geographical areas;
- products;
- services;
- transactions or distribution channels.

To this end, Alkemya also take into account the following sources:

- supranational report of the European Commission on the risks of money laundering and terrorist financing;
- national assessment of the risks of money laundering and terrorist financing;
- sub-sectoral ML/TF risk assessments;
- joint guidelines issued by the three European Supervisory Authorities (ESMA, EBA and EIOPA) on money laundering and terrorist financing risk factors;
- the relating CSSF publications.

Alkemya determines its risk-based approach based on the definition of the AML-CTF risk appetite. The strategy of Alkemya must be consistent with this approach. The AML-CTF policies, procedures and controls implemented within Alkemya are consistent with the previously defined risk appetite. This definition and strategy are communicated in a precise, clear and understandable way to all the concerned staff.

Alkemya documents, keeps up-to-date and makes available to the competent authorities the risk assessment carried out.

### 7.2. Risk assessment of each new business relationship

Where applicable, all customers shall be categorised based on their ML-TF risks, *i.e.* low, standard or high. This risk assessment is carried out before entering into a relationship with the customer and determines the extent of customer due diligence measures to be applied to each customer depending on the level of ML-TF risks presented by the customer. To that effect, a low level of risk may justify the application of simplified due diligence measures whilst a high level of risk leads to the application of enhanced due diligence measures. The assessment of the level of risk must not, under any circumstances, allow the application of enhanced due diligence measures to be waived when such enhanced due diligence measures shall be applied by law.

The level of ML-TF risks of the customers is assessed according to a consistent combination of risk factors inherent to the following risk categories:

- type of customers;
- countries and geographic areas;
- products, services and transactions;
- delivery channels.

Alkemya takes into account the risk factors listed under Annex III (lower risk of ML-TF) and IV (high risk of ML-TF) of the AML Law. These risk factors, taken into account individually or in combination, may increase or decrease the potential risk of ML-TF. Alkemya assigns an overall rating to the business relationship. On the basis of this rating, the level of customer due diligence applied to the business relation is determined.

Where relevant, Alkemya duly documents in writing and keeps up-to-date the result of the risk assessment carried out for each customer.

Alkemya reserves the right to refuse to enter into a business relationship with a potential customer if Alkemya considers that the ML-TF risks are too high.

During the course of the business relationship, Alkemya monitors any evolution of the ML-TF risks of the business relationship and adapts its assessment according to any significant change affecting the customers or any new risk.

Alkemya must also ensure that ML-TF risks at the level of the investments are covered. Therefore, Alkemya carries out an analysis of the ML-TF risks posed by any investments and takes customer due diligence measures adapted to risk assessed and documented. This risk analysis must be reviewed on an annual basis as well as when a particular event requires it.

### 7.3. Risk assessment report

Alkemya documents and keeps up-to-date a risk analysis report identifying and assessing the ML-TF risks to which it is exposed.

This analysis must take into account the risk factors listed above in Sections 7.1 and 7.2 and assesses the risks associated with the use of new products, practices or technologies prior to their launch and shall enable measures to be put in place to manage and limit the associated risks.

This risk assessment report must be a separate document prepared by the Compliance Officer of Alkemya. Such report takes into account the main characteristics of Alkemya's activities as well as the practical information provided by the business relationships entered into by Alkemya with its customers.

To that end, Alkemya uses information and guidance from a variety of sources, including the sources listed above under Section 7.1.

## 8. KNOW-YOUR-CUSTOMER OBLIGATION

### 8.1. Timing

Customer due diligence measures generally apply in the following situations:

- when entering into a new business relationship;
- when carrying out, on an occasional basis, a transaction that exceeds a certain threshold or constitutes a transfer of funds; in case of suspicion of ML-TF, irrespective of any applicable thresholds, exemptions or derogations;
- in case of doubts as to the veracity or relevance of previously obtained customer identification data.

### 8.2. Customer due diligence measures

The customer due diligence measures to be applied by Alkemya include:

- identifying the customer and verifying the customer's identity on the basis of documents, data or information obtained from “reliable and independent sources, including, where available, electronic identification means and relevant trust services as set out in Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC or any other secure electronic or remote identification process regulated, recognised or accepted by the relevant national authorities;

- identifying the beneficial owner and taking reasonable measures to verify his or her identity, using relevant information or data obtained from a reliable and independent source, in such a way that Alkemya can be sure of knowing the beneficial owner, and, in the case of legal persons, trusts, companies, foundations and similar legal arrangements, taking reasonable steps to understand the ownership and control structure of the customer.

    - for customers qualifying as legal persons, Alkemya identifies and takes reasonable measures to verify the identity of the beneficial owners by means of the following information:

        - the identity of the natural persons, if any, who ultimately hold a controlling interest within the definition of Article 1(7)(a)(i) of the 2004 Law in a legal person; and
        - where, after applying i), there are doubts as to whether the persons having a controlling interest are the beneficial owners, or where no natural person exercises control through a participation, the identity of the natural persons, if any, exercising control over the legal person by other means; and
        - where no natural person is identified as a part of the implementation of points (i) and ii), the identity of any relevant natural person who holds the position of senior managing official.

Alkemya keeps records of the measures taken as well as any difficulties encountered during the above verification process.

- for customers that are qualified as legal arrangements, Alkemya identifies the beneficial owner and take reasonable measures to verify the identity of those persons using the following information:

    - for *fiducies* and trusts, the identity of the settlor(s), *fiduciaire*(s) or trustee(s), protector(s), if any, of the beneficiaries or, where the persons who will be the beneficiaries of the legal arrangement or legal entity have not yet been designated, the category of persons in the main interest of which the construction or legal entity was established or operates and any other natural person exercising an ultimate control over the trust or trust by direct or indirect ownership or by other means, including through a chain of ownership or control;
    - for other types of legal arrangements similar to *fiducies* or trusts, the identity of any person holding equivalent or similar functions to those referred to above for *fiducies* and trusts;

- assessing and understanding of the purpose and intended nature of the business relationship and, where applicable, obtaining information on the purpose and intended nature of the business relationship;

- exercising a constant vigilance of the business relationship, in particular by examining the transactions concluded throughout the duration of the business relationship and, if necessary, the origin of the funds, so as to verify that these transactions are consistent with Alkemya's knowledge of the customer, its business activities and its risk profile, and by ensuring that the documents, data or information obtained in the exercise of the due diligence of customer remain up to date and relevant. In this context, Alkemya examines existing elements, particularly for customers qualified as high-risk customers.

### 8.2.1. Identification and verification of the customer's identity

The purpose of the identification and verification of identity of the customer is to remove the customer from anonymity. This identification is done on the basis of an AML-CTF survey to be completed by the customer.

Any contact with a potential customer is duly documented.

#### *8.2.1.1. Timing*

In principle, the customer must be identified, and his/her identity verified before the establishment of the relationship.

The customer may also be identified, and his/her identity verified during the establishment of a business relationship if it is necessary not to interrupt the normal exercise of business and when there is a low risk of ML-TF if the relationship is efficiently managed. In these situations, these measures are taken as soon as possible after the initial contact and adequate steps to effectively manage the risk of ML-TF must be taken.

Customer due diligence measures are applied not only in relation to new customers but also, at appropriate times, to existing customers based on the assessment of risks, taking into account the existence of previous customer due diligence procedures and when they were implemented or when relevant elements of a customer's situation change or when Alkemya, during the calendar year in question, is required by law to contact the customer in order to review any relevant information in relation to the beneficial owner(s) or if this obligation has fallen to Alkemya pursuant to applicable laws.

The frequency and periodicity are also determined on the basis of the criteria as set out below.

#### *8.2.1.2. Data to be collected*

In the case of a natural person, the following data must be collected:

- surname and first name;
- place and date of birth;
- nationality(-ies);
- full postal address of the customer's main residence;
- number and telephone number and email;
- where applicable, the official national identification number.

The identity must be verified on the basis of one valid authentic official identification document issued by a public authority and which bears the customer's signature and picture such as the customer's passport, his ID, his residence permit, his driving licence or any other similar document. In case of high-risk business relationship, Alkemya takes additional verification measures such as, for example, the verification of the address indicated by the customer through the proof of address or by contacting the customer, among others, per registered letter with acknowledgement of receipt

Electronic identification means, including relevant trust services as set out in Regulation (EU) No 910/2014 or any other secure, remote or electronic, identification process regulated, recognised, approved or accepted by the relevant national authorities may be used by Alkemya to fulfil its due diligence obligation.

In the case of a legal entity or legal structure, the following data must be collected:

- denomination;
- legal form;
- address of the registered office as well as, if different, the principal place of business;
- where applicable, the official identification number;
- name of the directors (*dirigeants*, members of the authorised management) (for the legal persons) and directors (*administrateurs*) or persons exercising similar positions (for the legal arrangements) and involved in the business relationship with the professional
- provisions governing the power to bind the legal person or arrangement;
- authorisation to enter into a relationship.

The identity must be verified on the basis of the following official documents:

- an extract from the commercial register or equivalent;
- up-to-date or coordinated articles of association or equivalent.

According to their risk assessment and without prejudice to other enhanced due diligence obligations, Alkemya takes additional verification measures, such as, for example:

- an examination of the last management report and the last accounts, where appropriate certified by a *réviseur d'entreprises agréé* (approved statutory auditor);
- the verification, after consulting the companies register or any other source of professional data, that the company was not or is not subject to a dissolution, deregistration, bankruptcy or liquidation;
- the verification of the information collected from independent and reliable sources such as, among others, public and private databases;
- a visit to the company, if possible, or contact with the company through, among others, registered letter with acknowledgement of receipt.

For both natural and legal persons, Alkemya must determine whether the customer acts for its own account or, where appropriate, for the account of other persons. The customer must sign an explicit declaration in that respect and commits to communicate any subsequent changes of beneficial ownership without delay to Alkemya. Alkemya ensures the credibility of this declaration. Where units or shares of a collective investment scheme are subscribed

through an intermediary acting on behalf of his investors (*e.g.* a nominee), Alkemya must ensure that enhanced customer due diligence measures are performed for this intermediary.

Alkemya must document, record and keep up-to-date all of the information mentioned in the present Section.

#### 8.2.2. Identification and verification of the identity of the person purporting to act on behalf of the customer

The person(s) purporting to act on behalf of the customer must also be identified and their identity verified in the same way as the customer (in line with the above Section 8.2.1.).

Person(s) purporting to act on behalf of the customer include *e.g.* legal representatives of the customer as well as proxyholders.

#### 8.2.3. Identification and verification of the beneficial owner's identity

The customer's beneficial owner(s) must be identified and their identity verified. It must therefore be determined whether the customer is acting on behalf of another person and all reasonable measures to obtain sufficient identification data to verify that person's identity must be taken.

The concept of beneficial owner is defined by Article 3 (6) of AML 4 as:

" *any natural person(s) who ultimately owns or controls the customer and/or the natural person(s) on whose behalf a transaction or activity is being conducted and includes at least:*

*(a) In the case of corporate entities:*

*(i) the natural person(s) who ultimately owns or controls a legal entity through direct or indirect ownership of a sufficient percentage of the shares or voting rights or ownership interest in that entity, including through bearer shareholdings, or through control via other means, other than a company listed on a regulated market that is subject to disclosure requirements consistent with Union law or subject to equivalent international standards which ensure adequate transparency of ownership information.*

*A shareholding of 25 % plus one share or an ownership interest of more than 25 % in the customer held by a natural person shall be an indication of direct ownership. A shareholding of 25 % plus one share or an ownership interest of more than 25 % in the customer held by a corporate entity, which is under the control of a natural person(s), or by multiple corporate entities, which are under the control of the same natural person(s), shall be an indication of indirect ownership. This applies without prejudice to the right of Member States to decide that a lower percentage may be an indication of ownership or control. Control through other means may be determined, inter alia, in accordance with the criteria in Article 22(1) to (5) of Directive 2013/34/EU of the European Parliament and of the Council;*

*(ii) if, after having exhausted all possible means and provided there are no grounds for suspicion, no person under point (i) is identified, or if there is any doubt that the person(s) identified are the beneficial owner(s), the natural person(s) who hold the position of senior managing official(s), the obliged entities shall keep records of the actions taken in order to identify the beneficial ownership under point (i) and this point."*

*(b) in the case of trusts all following persons:*

*(i) the settlor(s);*
*(ii) the trustee(s);*
*(iii) the protector(s), if any;*
*(iv) the beneficiaries, or where the individuals benefiting 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;*
*(v) any other natural person exercising ultimate control over the trust by means of direct or indirect ownership or by other means;*

*(c) in the case of legal entities such as foundations, and legal arrangements similar to trusts, any natural person holding equivalent or similar positions to those referred to in point (b)*."

Several texts further clarify the notion of beneficial owner and provide useful indications for the purpose of determining who should be considered as BO in a given situation:

- in the case of customers which are natural person(s), the beneficial owner is usually the customer himself/herself. Alkemya must check whether the natural person is acting on his/her behalf or not. Where the beneficial owner is different than the customer, Alkemya applies the necessary measures for identifying and verifying the identity of that person.
- in the case of customers which are legal person(s), Alkemya relies on the definition of beneficial owner to determine, depending on the type legal person at hand, who is to be considered as beneficial owner, as well as on the indications given in CSSF Circular 19/732. If the customer is a legal person, Alkemya uses a three-step procedure to identify the beneficial owner:

  (i) firstly, Alkemya must identify any natural person directly or indirectly owning more than 25% of the shares, voting rights or property rights in the customer;

  (ii) then, if no natural person has been identified under (i), Alkemya must identify any natural person, if any, exercising control over the customer by other means; and

  (iii) lastly, when no natural person has been identified under (i) and (ii), any natural person who holds the position of senior manager (as defined in CSSF Circular 19/732[3]) must be considered as beneficial owner(s) of the customer.

[3] According to the CSSF Circular 19/732, the "senior managing official" can be understood as either the executive official or the member(s) of the board of directors to whom the daily management has been delegated, and if no delegation has taken place, all members of the board of directors. This must be assessed on a case-by-case basis.

The identification of the beneficial owner(s) shall be made on the basis of the same data collected for customers that are natural person(s), in line with Section 8.2.1.

The verification of the identity of the beneficial owner(s) is made on the basis of the same documents than customers that are natural person(s), in line with Section 8.2.1.

If necessary, a request to the Luxembourg Register of Beneficial Owners may be carried out or a declaration of the beneficial owner may be requested.

Regarding beneficiaries of *fiducies*, trusts or similar legal arrangements that are designated by particular characteristics or category, Alkemya collects sufficient information on the beneficiaries to ensure the identification of the beneficiary at the time of payment of benefits or at the time the beneficiary exercises his or her acquired rights.

All of the information mentioned in the present Section must be documented, recorded and kept up-to-date.

#### 8.2.4. Sanctions lists, restrictive measures

It must be verified that the customer, the person(s) purporting to act on behalf of the customer and the customer's beneficial owner, if applicable, are not subject to any international financial sanctions or restrictive measures on the basis of the lists published by the United Nations, the European Union and, where relevant, the local competent authority. This verification takes place both at the time of entering into the business relationship or of completion of the contemplated transaction and throughout the duration of the business relationship.

If the customer, the person(s) purporting to act on behalf of the customer or the customer's beneficial owner(s) is being subject to such a financial sanction, the relevant restrictive measures shall be applied without delay in case where States, persons, entities or groups involved in a relevant transaction or business relationship are subject to restrictive measures in financial matters. If applicable, the relevant competent authorities shall also be informed.

Following the adoption or update of the official lists as referred to above, it must be ensured that the internal system used for such control or made available by an external service provider, is adapted without delay.

### 8.3. Asset/investment due diligence measures

Alkemya carries out an analysis of the ML-TF risks posed by the investment activity and take due diligence measures adapted to the ML-TF risk assessed per asset class. This assessment is appropriately documented in written, formalised and reviewed at least on an annual basis.

Alkemya ensures that due diligence measures are performed to mitigate any ML-TF risks. Alkemya, either directly or through a third-party (*e.g.* the portfolio manager of investment advisor) must establish appropriate due diligence controls by asset type on a risk-based approach and carry out the screening of all assets and, depending on the assets types, on the parties linked to the transactions.

Prior to investing in an asset, Alkemya screens the name of such assets and/or of its issuer against all applicable sanctions lists.

### 8.4. Due diligence measures and service providers

The due diligence measures provided for in the present Section 8 shall be applied on the service providers. Such due diligence measures are adapted to the ML-TF risks presented by these service providers.

The name of each service provider shall be screened prior to entering into a contractual relationship.

### 8.5. Object and purpose of the business relationship

At the time of the identification of the customer, relevant information on the origin of the customer's funds and on the type of transactions for which the customer enters into a business relationship, as well as all adequate information to determine the purpose of the business relationship contemplated by the customer shall be collected.

### 8.6. Impossibility to obtain the necessary information/documentation

When Alkemya is unable to comply with its customer due diligence obligations, as set out above, it must not carry out a transaction nor establish a business relationship and must terminate the business relation and consider making a suspicious activity report to the financial intelligence unit ("**FIU**").

### 8.7. Simplified due diligence

If a lower risk of ML-TF is identified, simplified customer due diligence measures may be applied.

Before applying simplified customer due diligence measures, it is necessary to ensure that the relevant business relationship or transaction presents a lower level of ML-TF. To that end, it is necessary to take into account at least the factors of potentially lower risk situations set out in Appendix III of the AML Law. It is also recommended to apply the indications given in CSSF Circular 21/782.

Alkemya gathers sufficient information in all circumstances to establish whether the customer meets the conditions required for the application of simplified due diligence measures.

Alkemya carries out sufficient monitoring of transactions and business relationships to determine whether simplified due diligence measure may be applied to a given customer and to monitor the business relationship to ensure that the conditions for applying simplified due diligence measures continue to be met.

To the extent that Alkemya determines that the business relationship or transaction presents a lower degree of ML-TF risk and that simplified due diligence measures may be applied, Alkemya may reduce the scope of the measures applied in relation to the contemplated transaction/business relationship. However, this does not constitute an exemption from all measures and Alkemya remains obliged to identify and verify the identity of the customer, the person(s) purporting to act on behalf of the customer and the beneficial owner(s), where applicable.

The simplified due diligence measures that Alkemya may apply in respect of the low-risk business relationship include *i.a.*:

- for customers subject to a compulsory authorisation or registration regime for AML-CTF purposes, the verification that the customer is subject to this regime by

performing, for example, searching on the official website of the regulator and documenting the results of the search;
- the presumption that a payment debited from an individual or joint account held in the name of a customer by a credit institution or financial institution regulated in a country member of the European Economic Area or a third country imposing equivalent AML-CTF obligations, fulfils the requirements provided for in point (a) of the first subparagraph of Article 3(2) of the AML Law;
- the exceptional acceptance of other types of ID documents which meet the criteria of reliable and independent sources, for example a letter addressed to the customer by a governmental body or other reliable public body, where the customer cannot provide the usual identification documents and, insofar as there are no grounds for suspicion;
- the update of the information on the customer due diligence measures only in case of certain trigger events, for example if the customer requests a new or riskier product or service or in the event of changes in the behaviour or transaction profile of the customer which seem to indicate that the risk associated with the relationship is no longer low;
- for persons purporting to act on behalf of a customer and for initiators, promoters who launched an investment fund, obtaining information on the country of residence of these persons instead of asking for the full postal address;
- for persons purporting to act on behalf of a customer, where a customer is a regulated credit or financial institution, instead of asking the complete identification of these persons, obtaining a letter confirming that the institution applied due diligence measures to these persons and that it carried out regular controls of these persons with respect to the applicable lists of restrictive measures in financial matters.

In the presence of information suggesting that the degree of ML-TF risk is not low, when there is a suspicion of ML-TF or where there is doubt as to the veracity or relevance of previously obtained data or in specific cases of higher risk, the application of the simplified due diligence regime is not possible for these particular customers, geographical areas, products, services, transactions or distribution channels.

## 8.8. Enhanced due diligence

### *8.8.1. General rules*

Alkemya must apply, according to its risk assessment, enhanced customer due diligence measures, in addition to the above-mentioned due diligence measures, in situations which may present a high risk of ML-TF and in certain specific situations mentioned below.

When assessing ML-TF risks, Alkemya must at least take into account the factors of potentially higher risk situations set out in Annex IV of the AML Law. It is also recommended to make use of the indications given in CSSF Circular n°21/782.

When Alkemya enters into a business relationship with natural persons or legal entities established in third countries which do not apply or insufficiently apply AML-CTF measures, Alkemya is required to apply the following enhanced due diligence measures:

- obtaining additional information on the customer and updating more regularly the identification data of customer and beneficial owner;
- obtaining additional information/documents on the intended nature of the business relationship or on the source of funds involved and of wealth;
- obtaining information and, where applicable, evidence on the reasons for and economic background of the intended or performed transactions and on the plausibility of these transactions;

- obtaining the approval of the authorised management to commence or continue the business relationship;
- requiring the first payment to be carried out through an account in the customer's name with a professional subject to similar customer due diligence standards;
- verifying the additional information obtained by using independent and reliable sources;
- visiting the customer/company or contacting the customer/company via registered letter with acknowledgement of receipt;
- conducting enhanced monitoring of the business relationship, by increasing the number and timing of controls applied, and selecting patterns of transactions that need further examination.

Particular attention shall be paid to any ML-TF threats that may result from products or transactions favouring anonymity, and take measures, where appropriate, to prevent their use for ML-TF purposes.

*8.8.2. Politically exposed person(s)*

It must be verified whether the customer, the person purporting to act on behalf of the customer and the customer's beneficial owner(s), if applicable, fall within the definition of politically exposed person ("**PEP**"). Article 3 (9) of AML 4 defines PEPs as: "*a natural person who is or who has been entrusted with prominent public functions and includes the following:*

*(a) heads of State, heads of government, ministers and deputy or assistant ministers;*
*(b) members of parliament or of similar legislative bodies;*
*(c) members of the governing bodies of political parties;*
*(d) members of supreme courts, of constitutional courts or of other high-level judicial bodies, the decisions of which are not subject to further appeal, except in exceptional circumstances; (e) members of courts of auditors or of the boards of central banks;*
*(f) ambassadors, chargés d'affaires and high-ranking officers in the armed forces;*
*(g) members of the administrative, management or supervisory bodies of State-owned enterprises;*
*(h) directors, deputy directors and members of the board or equivalent function of an international organisation.*

*No public function referred to in points (a) to (h) shall be understood as covering middle-ranking or more junior officials.*"

This verification takes place both at the time of entry into a business relationship or of the conclusion of the transaction and throughout the duration of the business relationship. This verification is carried out by soliciting relevant information from the customer, by using publicly available information or by accessing computer databases on PEPs. The detection of PEPs among existing customers must be carried out at least every six months.

Family members shall, mean all physical persons, including in particular:

(a) the spouse, or a person considered to be equivalent to a spouse, of a PEP;

(c) the children and their spouses, or partners considered by national law as equivalent to a spouse;

(d) the parents;

(e) the brothers and sisters.

Persons known to be close associates shall mean all natural persons, including:

(a) any natural person who is known to have joint beneficial ownership of legal entities or legal arrangements, or any other close business relations, with a PEP;

(b) any natural person who has sole beneficial ownership of a legal entity or legal arrangement which is known to have been set up for the benefit de facto of the PEP.

The identification of a customer, person purporting to act on behalf of the customer and/or customer's beneficial owner(s) as a PEP automatically leads to the classification of the business relationship as high risk and the application of enhanced due diligence measures.

When entering into a business relationship with a PEP or carrying out a transaction for a PEP, in addition to the customer due diligence measures set out under Section 8, Alkemya must ensure that it:

- has appropriate risk management systems, including risk-based procedures, to determine if the customer or beneficial owner is a PEP;
- obtains senior management approval for establishing or continuing a business relationship with a PEP;
- takes adequate measures to establish the source of wealth and of funds involved in the business relationship our transaction;
- conducts enhanced ongoing monitoring of the business relationship with the PEP.

When natural person ceases to be a PEP, Alkemya continues to consider, for at least twelve months, the risk that such PEP continues to pose and to apply appropriate measures on a risk-based approach until such person no longer poses a risk.

It is to be noted that when the customer is a public entity, the identification of PEPs will not enhance the risk of the entity, as far as the reason for this person to be categorized as PEP is a result of its position within the entity, or when being appointed to the public entity is directly linked with the position held.

### *8.8.3. High-risk countries*

A specific procedure for the acceptance and monitoring of transactions and business relationships involving customers, persons purporting to act on behalf of them or beneficial owners from high-risk countries shall be implemented.

Special attention and enhanced due diligence measures shall be applied to transactions and business relationships involving customers, persons purporting to act on behalf of them or beneficial owners from high-risk countries.

Such measures include *i.a.*:

- obtaining additional information on the customer and on the customer's beneficial owner(s) and updating more regularly the identification data of the customer and beneficial owner(s);
- obtaining additional information on the intended nature of the business relationship;
- obtaining information on the source of funds and wealth of the customer and of the beneficial owner(s);
- obtaining information on the reasons for the intended or performed transactions;
- the systematic involvement of the Compliance Officer in the customer acceptance procedure and the written authorisation of the authorised management;

- enhanced monitoring of the transactions and business relationship, notably by increasing the number and timing of controls applied, and by selecting patterns of transactions that need further examination and by obtaining supporting evidence.

Alkemya ensures that the first payment received is carried out through an account in the customer's name opened with a credit institution subject to customer due diligence standards that are not less robust than those laid down in AML 4.

Where applicable, Alkemya shall also apply one or more additional mitigating measures to persons and legal entities carrying out transactions involving high-risk third countries. Those measures shall consist of one or more of the following:

- the application of additional elements of enhanced due diligence;
- the introduction of enhanced relevant reporting mechanisms or systematic reporting of financial transactions;
- the limitation of business relationships or transactions with natural persons or legal entities from the third countries identified as high risk countries.

### 8.9. Remote entry into a business relationship

When carrying out a transaction or entering into a business relationship without the physical presence of the customer, measures such as requesting additional identification documents, data or information or requesting the certification of identification documents and the verification of identity on specific lists may be applied. Such measures also include obtaining additional documents, data or information that ensure the proper identification of customers.

However, in order to provide an adequate and effective risk-based approach, not all customer relationships will be classified as automatically high risk due to their remote nature.

### 8.10. Ongoing monitoring

Alkemya has procedures and control mechanisms enabling them, when accepting customers and monitoring business relationships, to detect, in particular:

- persons referred to in Articles 30, 31 and 33 of the CSSF Regulation 12-02;
- funds coming from or going to countries, persons, entities or groups referred to in Article 33 of the CSSF Regulation 12-02 or countries referred to in Article 31 of the CSSF Regulation 12-02;
- complex or unusual transactions referred to in Article 32 of the CSSF Regulation 12-02;
- transfers of funds with missing or incomplete information within the meaning of Regulation (EU) 2015/847 as referred to in Article 15 of the CSSF Regulation 12-02.

The implementation of a complete and up-to-date customer database is an integral part of this supervisory mechanism. In the event of encoding by an employee who is a natural person of Alkemya, this will have to be checked in accordance with the "4-eyes principle". This monitoring systems covers all customer accounts and transactions and is aimed at customers, persons purporting to act on behalf of the customer, initiators and beneficial owners. The system takes into account the risks identified by Alkemya as far as it is concerned, based, in particular, on the characteristics of its business and its clientele.

The detection searches carried out with the help of the monitoring system must be duly documented, including in cases where they do not produce positive results.

### 8.11. Detection of complex and unusual transactions

The background and purpose of any transaction that is:

- complex;
- unusually large;
- conducted in an unusual pattern;
- does not have an apparent economic or lawful purpose

shall be verified.

The degree and nature of monitoring measures shall be increased to determine whether such transactions or activities appear unusual or suspicious.

### 8.12. Activities requiring special attention

In the context of ongoing monitoring, the activities of customers whose acceptance has been subject to a specific examination under the client acceptance procedure referred to in Article 10 of the CSSF Regulation 12-02 require particular attention.

### 8.13. Update of information

Customer due diligence measures shall be applied not only when entering into a relationship but also, at the appropriate times, to existing customers, depending on the risk assessment. The frequency of the review varies according to the risk assessment presented by the relevant business relationship. In all cases, it must be ensured that the information remains up to date.

In principle, the frequency of review depending on the level of risk assigned to a customer is summarised as follows:

| Level of risk | Frequency of review |
|---|---|
| Low risk | Every 5 years |
| Standard risk | Every 3 years |
| High risk | Every year |

Regardless of the frequency of review of the business relationship, it must be verified at least once a year that the conditions that allowed for the application of simplified due diligence measures are still complied with. If there has been no transaction during this period, this verification shall be carried out the next time the business relationship is reactivated.

In addition to applying customer due diligence measures on a regular basis, certain specific events will require an employee to request an update of a customer's identification documents, such as:

- the identity of the customer, beneficial owner or agent has changed;
- a transaction does not appear to be consistent with the customer’s profile;
- the purpose or intended nature of the business relationship has changed;
- an external factor results in a change in the customer’s risk category (low, standard or high);
- a change in the customer’s business or jurisdiction of establishment or in the jurisdictions with which the customer usually has contact;
- a restructuring of the customer;
- a change of interest of the customer;
- the identification of a PEP in the customer's structure;
- a significant update of the texts in force in the field of AML-CTF;

- new investments or commitment are made by the customer;
- any other element that may affect the customer's level of risk.

## 9. PERFORMANCE OF CUSTOMER DUE DILIGENCE MEASURES BY THIRD PARTIES

Alkemya may have recourse to third parties for the performance of the above-mentioned due diligence measures. There are two possible mechanisms in this context: the conclusion of an outsourcing arrangement (9.1.) or the recourse to a third-party introducer (9.2.).

### 9.1. The conclusion of an outsourcing arrangement

Alkemya may conclude outsourcing arrangements with third parties for the performance of the customer due diligence measures. Alkemya ensures that such third parties have the necessary resources to perform all outsourced functions.

A risk assessment in relation to the outsourced functions and, if applicable, the outsourcing chain must be carried out prior to the conclusion of each outsourcing arrangement.

An outsourcing service provider will not have the authority to determine a customer's risk assessment and draw conclusions in the name and on behalf of Alkemya. Alkemya will remain fully responsible for compliance with its AML-CTF obligations.

Furthermore, the outsourcing service provider will never have the authority to enter into a business relationship in the name and on behalf of Alkemya.

The outsourcing arrangement must include at least the following elements:

- a detailed description of the customer and due diligence measures to be implemented, in compliance with the AML Law and the CSSF Regulation 12-02 and, in particular, of the information and documents to be requested and verified by the outsourcing service provider;
- the roles, responsibilities and tasks of each party to the outsourcing arrangement – in particular, where the service provider is a registrar and transfer agent acting on behalf of an investment fund, the board of directors of the fund (or equivalent) and/or the fund manager outsourcing certain tasks to the registrar and transfer agent must remain responsible. Therefore, the fund board (or equivalent) and the fund manager should ensure that the relevant arrangements contain detailed clauses specifying the roles and responsibilities of each party. They should also ensure that the contract allows them to have access to any information necessary to perform their function and to carry out ongoing, formalised monitoring of the service providers;
- the conditions relating to the transmission of information to Alkemya including, in particular, the immediate provision, without opposition to confidentiality rules or professional secrecy or any other obstacles whatsoever, of the information gathered in the context of the fulfilment of the customer due diligence obligations and the transmission, upon request and without delay, of a copy or of the originals of evidentiary documents obtained in this respect.

### 9.2. The recourse to a third-party introducer

The recourse to a third-party business introducer is a mechanism by which a company uses certain categories of persons to fulfil the obligations to (**i**) identify and verify the identity of

customers, beneficial owner(s), person purporting to act on behalf of the customer and (**ii**) to obtain information on the purpose and nature of the envisaged business relationship.

Through this mechanism, Alkemya obtains information and documents collected by third parties and rely on these data and documents as part of their own professional obligations.

In this context, only certain persons may act as third-party introducers (*e.g.* distributors). These persons are professionals who fall within the scope of the AML-CTF frameworks, the organisations or federations that are members of these professionals or other institutions or persons, located in a Member State or a third country:

- which apply customer due diligence measures and record-keeping measures for the conservation of documents and records with regard to customers which are consistent with those provided for by AML 4; and

- which are subject, with regard to compliance with the requirements of AML 4 or equivalent rules applicable to them, to supervision consistent with Chapter VI, Section 2 of AML 4.

Such persons may include credit institutions, financial institutions, external accounts or auditors, tax advisors, legal professionals and trust or company service providers.

Alkemya is prohibited from using third parties which are established in countries which do not apply or insufficiently apply AML-CTF measures.

Alkemya shall ensure that such third party provides without delay, upon request, the mandatory documents concerning customer due diligence obligations, including, where applicable, data obtained through the use of electronic means of identification, the relevant trusted services provided for by Regulation (EU) No 910/2014, or any other secure, electronic or remote identification process regulated, recognised, approved or accepted by the relevant national authorities.

Alkemya must also ensure that this third party is subject to regulation and supervision, and that it has taken measures to comply with customer due diligence and record-keeping obligations that are consistent with those provided for under AML 4.

Final responsibility for the performance of the above obligations remains with Alkemya notwithstanding the use of a third-party introducer.

## 10. RECORD-KEEPING OBLIGATIONS

A copy of the following documents, data and information shall be kept:

- with regard to customer due diligence measures, a copy of or references to the documents, data and information that are necessary to comply with customer due diligence obligations including, if applicable, data obtained through the use of electronic identification means, the relevant trust services provided for by Regulation 910/2014 or any other secure identification process, electronic or remote access, regulated, recognised, approved or accepted by the competent national authorities, the account books, business correspondence and the results of any analysis carried out during 5 years after the end of the business relationship with the client or after the date of the transaction concluded on an occasional basis;
- supporting documents and records of transactions which are necessary to identify or reconstruct individual transactions in order to provide, if necessary, evidence in the

framework of a criminal investigation or enquiry, for a period of 5 years after the end of the business relationship with the customer or after the date of the transaction concluded on an occasional basis;
- information on the measures that have been taken to identify the beneficial owner(s) and person(s) purporting to act on behalf of the customer.

The documents relating to the transactions must be sufficient to enable the reconstruction of the various transactions to provide, if necessary, evidence in the event of criminal proceedings.

Where relevant, the aforementioned documents and information shall be kept at the disposal of the competent authorities so that Alkemya is able to respond quickly to requests for information from them in the course of their duties.

## 11. DATA PROCESSING

The processing of personal data under AML 4 is subject to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC ("**GDPR**").

Personal data are processed on the basis of AML 4 only for the purposes of the prevention of ML-TF and are not further processed in a way incompatible with those purposes. The processing of personal data for any other purposes is prohibited.

Alkemya communicates to all new customers the information required under Articles 13 and 14 of the GDPR before entering into a business relationship or executing a transaction on an occasional basis. In particular, this information shall contain a general warning regarding Alkemya's legal obligations under AML 4 with regard to the processing of personal data for the purposes of the prevention of ML-TF.

Personal data is retained for the retention period required under AML 4, *i.e.* at least five years, and will be deleted at the end of such retention periods. Where applicable, the supervisory authorities may, however, require in specific cases, when necessary for the performance of their duties under AML 4, that Alkemya keeps the data for an additional period which may not exceed five years.

Notwithstanding the foregoing, Alkemya shall keep personal data for an additional period of five years where this is necessary for the effective implementation of internal measures for the prevention or detection of acts of ML-TF.

## 12. RECRUITMENT AND TRAINING

Alkemya applies recruitment procedures that ensure that all employees, and in particular the members of the Compliance function, meet the required requirements in terms of good repute and expertise.

Alkemya organises regular training at least once a year for all staff, including members of the management bodies and the effective management, on the professional obligations with regard to AML-CTF and the applicable data protection requirements.

In this context, the training and awareness programme for staff must include, in particular:

- for newly recruited employees, as soon as they are hired, participation in a basic internal or external training, making them aware of Alkemya's AML-CTF policy as well as the relevant legal and regulatory requirements;
- for all employees, regular participation in continuous internal or external training, particularly for staff in direct contact with customers, to help them detect unusual transactions and recognise attempts at ML-TF. This training must also cover Alkemya's internal procedures to be followed by employees in the event of the detection of a suspicion of ML-TF;
- regular informational meetings for employees in order to keep them informed of developments in ML-TF techniques, methods and trends, as well as the preventive rules and procedures to be followed in this area;
- designation of one or more contact persons for employees who are competent and available to answer any question relating to ML-TF, and who may deal, in particular, with all aspects of the laws and obligations relating to AML-CTF, internal procedures, customer due diligence and suspicious transaction reporting;
- the periodic distribution of AML-CTF documentation, including examples of ML-TF operations.

The above-mentioned training courses and participation in them will be documented in writing.

Alkemya's employees will receive regular updates on the relevant legislation and regulations at regular intervals.

All employees have access to this Policy.

## 13. SCREENING

Alkemya carries out initial and on-going screening of the customers, its related parties including their beneficial owners, persons purporting to act on behalf of the customers and board members against lists of politically exposed persons and targeted financial sanction lists. Where the customer is an intermediary and Alkemya receives a potential name match on the name/other information related to the intermediary's customer, even if this person is not to be considered as the customer of Alkemya, the latter must follow up with the intermediary by making a request for information on the particular underlying customer.

In case of a positive match, Alkemya will refrain from entering into a business relationship or block any redemption and will immediately inform the relevant competent authorities.

## 14. COOPERATION WITH COMPETENT AUTHORITIES

Alkemya is required to cooperate with the competent authorities in matters of AML-CTF either:

- by responding to requests for information from these authorities;
- by spontaneously communicating information to the CRF *via* the carrying out of a suspicious transaction report.

### 14.1 Spontaneous reporting to the CRF

Alkemya is required to submit a suspicious activities report to the CRF whenever, in the course of their professional activities falling within the scope of the AML Law, one of their employees is confronted with a situation that may give rise to a suspicion of ML-TF.

Alkemya must therefore make such a report when they know, suspect or have good reason to suspect that ML-TF is in progress, has taken place, or has been attempted, in particular because of the person concerned, its development, the origin of the assets, the nature, purpose or methods of the transaction.

Alkemya does not have to qualify the underlying infraction, nor to prove it.

Suspicion is not defined as such. The CRF has provided guidance on typologies of situations that may give rise to a suspicious activity report: https://justice.public.lu/content/dam/justice/fr/legislation/circulaires/declarations/2021-04-01-suspicious-operations-report-version-2-1.pdf

Alkemya is strictly prohibited from revealing to the customer concerned or to third parties that any information has been communicated to the CRF.

In practice, in the event that an employee knows, suspects or has good reason to suspect that ML-TF is taking place, has taken place or has been attempted, he must refer the matter to the RC. Under no circumstances should an employee spontaneously submit a suspicious activity report on his/her own initiative.

The RC then carefully examines the information and documents at his/her disposal and, if necessary, obtains additional information/elements. After consultation with a member of management (*i.a.* the RR), a decision is made as to whether a suspicious activity report should be issued or not. This decision is in any case duly documented with a brief written explanation of the reasons leading to the suspicious activity report or the decision not to submit a suspicious activity report.

The suspicious activity report will then be made *via* the goAML application. The declaration must be supported by all information and documents which justified the declaration.

The RC shall in parallel communicate to the CSSF the information transmitted to the CRF if such information refers to a professional subject to the supervision of the CSSF or, to his knowledge, to a member of the staff or management bodies of the funds subject to the supervision of the CSSF, or if such information is likely to have a wider impact on the financial sector.

The employee in charge of the business relationship must refrain from executing the transaction he knows or suspects to be related to ML-TF before having informed the CRF and complied with any specific instructions of the CRF. The CRF may give instructions not to execute the operations related to the transaction or the customer. When such abstention is not possible or is likely to prevent the prosecution of the beneficiaries of a suspected ML-TF operation, the employee must consult the RC and a member of management, *i.a.* the RR, who shall subsequently inform the CRF of the impossibility of abstention.

In the event of an oral instruction, this communication must be followed within three working days by written confirmation. In the absence of written confirmation, the instruction will cease to have effect on the third working day at midnight. Alkemya is not authorised to report this instruction to the client without the express prior consent of the CRF.

A business relationship that has been the subject of a suspicious activity report to the CRF must be monitored with increased vigilance and, where appropriate, in line with the instructions of the CRF. In the event of new indications of ML-TF, Alkemya will issue an additional suspicious activity report.

Professional secrecy is not applicable towards the CRF.

The disclosure in good faith to the Luxembourg authorities responsible for the fight against ML-TF by Alkemya or any of its employees or directors of information in the context of a suspicious activity report does not constitute a breach of any restriction on disclosure of information imposed by a contract, by professional secrecy or by a legislative, regulatory or administrative provision and does not entail any liability of any kind for Alkemya or the employee concerned, even in a situation where they did not have precise knowledge of the associated underlying infringement, regardless whether an unlawful activity actually occurred or not.

Individuals, including employees and agents of Alkemya may not be subjected to threats, retaliatory measures or hostile acts, and in particular prejudicial or discriminatory employment measures, for having reported a suspicion of ML-TF to the CRF. Persons exposed to threats, retaliation, hostile acts or prejudicial or discriminatory employment measures for having reported a suspicion of ML-TF to the CRF have the right to file a complaint to the CSSF.

Any contractual stipulation or any act contrary to the above paragraph, and in particular any termination of the employment contract in breach of the provisions of the above paragraph, shall be null and void by operation of law.

In the event of termination of the employment contract, the employee may avail himself of the remedies provided for in paragraphs (4) to (7) of Article L. 271-1 of the Labour Code.

Alkemya, its directors and employees may not reveal to the customer concerned or to third parties that information is, will be or has been communicated or provided to the authorities pursuant to Article 5, paragraphs (1), (1bis), (2) and (3) of the AML Law or that an investigation by the CRF on ML-TF is in progress or could be opened.

### 14.2 Reporting to the CRF upon request

In addition to the spontaneous obligation to submit a suspicious activity report in certain situations, Alkemya must also respond or be able to respond, without delay, to requests for information from the CRF.

The transmission of such information or documents on which such information is based takes place exclusively through the goAML application.

## 15. WHISTLEBLOWING

If an employee or agents of Alkemya is found to be in potential or actual non-compliance with the AML-CTF obligations within Alkemya, he/she has the possibility to report the non-compliance to the Compliance Officer. The Compliance Officer will examine the seriousness of the reported facts and, if necessary, take the necessary measures to prevent potential or actual violations.

In this context, it is recalled that any persons, including employees and agents of Alkemya may not be subject to threats, reprisals or hostile acts, and in particular prejudicial or

discriminatory measures in employment matters, for having reported internally or to a supervisory authority a suspicion of ML-TF.

## 16. SANCTIONS

### 16.1 Money laundering

Any natural person who commits a money laundering offence is liable to imprisonment (one to five years) and/or a fine between EUR 1,250 and 1,250,000 euros. This sanction is increased in case the offence is committed by a professional falling under Article 2 of the AML Law in the exercise of his profession (three to five years of imprisonment).

### 16.2 Terrorist financing

Any natural person who commits a terrorist financing offence is liable to the same sanctions as the terrorist acts themselves, *i.e.* fifteen to twenty years of imprisonment for a terrorist act or life imprisonment if the terrorist act has led to the death of one or several persons.

### 16.3 Breach of professional obligations

Administrative sanctions for non-compliance with professional obligations include:

- a warning;
- a reprimand;
- a public statement specifying the identity of the natural or legal persons and the nature of the violation;
- where a professional is subject to an authorisation granted by a supervisory authority, a withdrawal or suspension of such authorisation;
- a temporary ban for a term not exceeding five years:
    - to engage in a professional activity in the financial sector or to carry out one or more transactions against persons subject to supervisory powers; or
    - to exercise managerial functions with professionals subject to supervisory powers, against any person holding managerial responsibilities in such a professional or any other natural person held liable for the violation;
- administrative fines of up to twice the amount of the benefit resulting from the breach, where it is possible to determine the breach, or up to a maximum of EUR 1,000,000.

For companies subject to the supervision of the CSSF, the administrative fines can reach EUR 5,000,000 or 10% of the total annual turnover according to the latest available accounts approved by the management body. The total turnover to be taken into account is the total annual turnover of the latest available consolidated accounts approved by the management body of the ultimate parent company.

Supervisory authorities, *i.a.* the CSSF, may impose a fine between EUR 250 and EUR 250,000 in respect of natural and legal persons obstructing the exercise of their supervisory powers or who knowingly provide documents or information that are found to be incomplete, inaccurate or false.

Criminal sanctions may also be imposed to anyone knowingly contravening their AML-CTF obligations, such as a criminal fine between EUR 12,500 and EUR 5,000,000.

The intentional breach to AML-CTF obligations is a criminal offence separate to ML-TF and may be pursed even in the absence of an underlying money laundering offence.

## APPENDIX A - NON-EXHAUSTIVE LIST OF RISK VARIABLES THAT THE PROFESSIONALS SHALL CONSIDER WHEN DETERMINING TO WHAT EXTENT TO APPLY CUSTOMER DUE DILIGENCE MEASURES

(i) the purpose of an account or relationship;

(ii) the level of assets to be deposited by a customer or the size of transactions undertaken;

(iii) the regularity or duration of the business relationship.

## APPENDIX B – NON-EXHAUSTIVE LIST OF RISK FACTORS INDICATIVE OF POTENTIALLY LOWER RISK AND TRIGGERING SIMPLIFIED CUSTOMER DUE DILIGENCE MEASURES

### 1. Customer risk factors:

(a) public companies listed on a stock exchange and subject to disclosure requirements (either by stock exchange rules or through law or enforceable means), which impose requirements to ensure adequate transparency of beneficial ownership;
(b) public administrations or enterprises from countries or territories having a low level of corruption;
(c) (c) customers that are resident in geographical areas of lower risk as set out in point (3);

### 2. Product, service, transaction or delivery channel risk factors:

(a) life insurance policies for which the premium is low;
(b) insurance policies for pension schemes if there is no early surrender option and the policy cannot be used as collateral;
(c) a pension, superannuation or similar scheme that provides retirement benefits to employees, where contributions are made by way of deduction from wages, and the scheme rules do not permit the assignment of a member's interest under the scheme;
(d) financial products or services that provide appropriately defined and limited services to certain types of customers, so as to increase access for financial inclusion purposes;
(e) products where the risks of money laundering and terrorist financing are managed by other factors such as purse limits or transparency of ownership (particularly, certain types of electronic money);

### 3. Geographical risk factors - registration, establishment, residence in:

(a) Member States;
(b) third countries having effective anti-money laundering and counter terrorist financing systems;
(c) third countries identified by credible sources as having a low level of corruption or other criminal activity;
(d) third countries which, on the basis of credible sources such as mutual evaluations, detailed assessment reports or published follow-up reports, have requirements to combat money laundering and terrorist financing consistent with the revised FATF Recommendations and effectively implement those requirements.

## APPENDIX C - NON-EXHAUSTIVE LIST OF RISK FACTORS INDICATIVE OF A POTENTIALLY HIGHER RISK AND TRIGGERING ENHANCED CUSTOMER DUE DILIGENCE MEASURES

### 1. Customer risk factors:

(a) the business relationship is conducted in unusual circumstances;
(b) customers that are resident in geographical areas of higher risk as set out in point (3);
(c) legal persons or arrangements that are personal asset-holding vehicles;
(d) companies that have nominee shareholders or shares in bearer form;
(e) businesses that are cash-intensive;
(f) the ownership structure of the company appears unusual or excessively complex given the nature of the company's business;
(g) customer is a third-country national who applies for residence rights or citizenship in exchange of capital transfers, purchase of property or government bonds, or investment in corporate entities.

### 2. Product, service, transaction or delivery channel risk factors:

(a) private banking;
(b) products or transactions that might favour anonymity;
(c) non-face-to-face business relationships or transactions, without certain safeguards, such as electronic identification means, relevant trust services as defined in Regulation (EU) No 910/2014 or any other secure, remote or electronic, identification process regulated, recognised, approved or accepted by the relevant national authorities;
(d) payment received from unknown or unassociated third parties;
(e) new products and new business practices, including new delivery mechanism, and the use of new or developing technologies for both new and pre-existing products;
(f) transactions related to oil, arms, precious metals, tobacco products, cultural artefacts and other items of archaeological, historical, cultural and religious importance, or of rare scientific value, as well as ivory and protected species.

### 3. Geographical risk factors:

(a) without prejudice to Article 3-2(2), countries identified by credible sources, such as mutual evaluations, detailed assessment reports or published follow-up reports, as not having effective anti-money laundering and counter terrorist financing systems;
(b) countries identified by credible sources as having significant levels of corruption or other criminal activity;
(c) countries subject to sanctions, embargos or similar measures issued by, for example, the European Union or the United Nations;
(d) countries providing funding or support for terrorist activities, or that have designated terrorist organisations operating within their country.