# Anti-Money Laundering and Counter-Terrorist Financing Policy

## COMPLIANCE DEPARTMENT

| Scope | Confidentiality level |
|---|---|
| **Group** | **Public** |

| Status | Date | Author |
|---|---|---|
| **Creation** | May 2020 | Compliance Department |
| **Update** | January 2025 | Compliance Department |

| | Location |
|---|---|
| **Storage** | SharePoint > Compliance |
| **Accessibility** | Intranet and extranet |

## I - PREAMBLE

The rules and guidelines described in this policy reflect the regulatory requirements applicable to real estate service providers and are applicable to Emeria and its companies (hereinafter referred to as "the Group"). The anti-money laundering and counter-terrorist financing (AML-CTF) policy is the responsibility of the Compliance Department, which reports to the Legal Department.

This policy must be applied by every employee. It defines all the procedures, controls and level of supervision to be put in place to mitigate risks in accordance with the regulatory obligations in force. It is updated regularly to ensure its relevance and adaptation to legislative changes.

The management, aware of the challenges and its responsibility in terms of compliance and risk prevention related to money laundering and terrorist financing, is fully involved in this fight. It is kept informed of the main warning signs and risks.

The Group oversees the AML/CFT system within the parent company and its subsidiaries. The compliance officers appointed in each Group company are responsible for disseminating the Group's policies, procedures and systems at the local level.

When local regulatory requirements are more stringent than those of the Group, the entities concerned must comply with them. It is their responsibility to adapt these specific requirements to their own operational procedures.

### 1. Reference texts

- Directive (EU) 2018/1673 of the European Parliament and of the Council of 23 October 2018
- 5e European Directive (5AMLD): Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018.
- FATF Recommendations
- Articles L561-1 et seq. of the French Monetary and Financial Code
- Articles 324-1 et seq. of the French Criminal Code

If you have any questions or require assistance in applying this policy, please contact the Compliance Department at the following address: compliance@emeria.eu

## 2. Scope

***Which staff members are affected?***

This policy applies to all persons holding a position or performing a function within the Group: corporate officers, managers, employees, temporary staff (temporary workers, work-study students, interns, volunteers).

It must also be respected and applied to all partners, subcontractors, suppliers, principals, customers and prospects.

***Which professions are affected?***

- Transactions
- Rental management for monthly rents greater than or equal to €10,000
- Insurance brokerage, reinsurance and insurance intermediary activities

# II - DEFINITIONS

The fight against money laundering and terrorist financing must be part of everyday professional life. Everyone's commitment is essential to ensure an appropriate level of vigilance and risk control. In order to understand the issues at stake (AML-CFT), it is important to correctly understand the following terms and concepts:

- **Money laundering**: the act of facilitating, by any means, the false justification of the origin of funds, property or income belonging to the perpetrator of a crime or offence that has provided them with a direct or indirect profit[1].

Money laundering also includes assisting in the investment, concealment or conversion of the direct or indirect proceeds of a crime or offence. **Money laundering is punishable by 5 years' imprisonment and a fine of €375,000.**

*Example: Mrs X approaches a real estate agency in the south of France to purchase an exceptional property worth €3 million. Her husband, who like her lives in a country outside the European Union, will transfer the funds from his account located in a tax haven. Mr X is known in his country as a notorious drug trafficker. The money used to finance the property could be the proceeds of drug trafficking.*

In concrete terms, money laundering refers to the process by which funds acquired illegally, for example through crime or fraud, are made legitimate through a series of financial transactions. The aim is to make the system as opaque as possible in order to conceal the fraudulent origin of the funds.

The property sector is particularly targeted by money laundering practices: it allows large sums of money to be laundered through investment in real estate.

[1] Art 324-1 of the Penal Code

It is therefore imperative that all employees comply with the regulatory requirements imposed and exercise vigilance in their daily professional practice.

- **Terrorist financing**: the act of financing a terrorist enterprise by providing, gathering or managing funds, securities or any other assets, or by giving advice for this purpose, with the intention of seeing these funds, securities or property used or knowing that they are intended to be used, in whole or in part, to commit any of the acts of terrorism provided for, regardless of whether such an act actually occurs[2].

- **The customer in a business relationship**: a customer is considered to be engaged in a "business relationship" when there is a contract between the professional and the customer using their services, under which several successive transactions are carried out between the contracting parties, or which creates ongoing obligations for them. Thus, the following may be considered a business relationship:

  - A customer who carries out several transactions in the same year.

  - A customer who gives a mandate to the professional.

  - A customer who signs a lease for a rental property.

  - A customer who has taken out an insurance policy.

- **Occasional customer**: an occasional customer is someone who carries out a one-off transaction, outside of a contract, with a regulated professional.

- **A politically exposed person (PEP)**: a person who holds (or has held) a high public office (political, judicial or administrative) on behalf of a State (including France). This person may also be a direct member of their family or a person known to be closely associated with them[3].

In practical terms, certain persons who hold high office (National Assembly, government, judiciary, etc.) are considered politically exposed persons. Outside the political sphere, this category also includes certain persons closely associated with PEPs (family, close associates). It should be noted that, by virtue of the powers conferred on them by their positions, PEPs present an increased risk of involvement in money laundering or even terrorist financing. Consequently, additional monitoring and control measures are necessary.

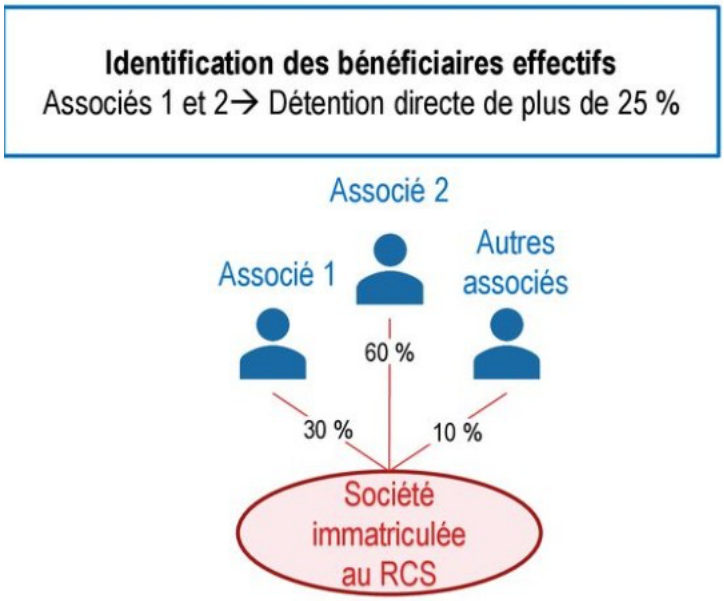
*Example: In the Panama Papers affair, several prominent leaders, including members of the EPP, were implicated in yet another tax evasion scandal, such as British Prime Minister David Cameron and his Icelandic counterpart Sigmundur David Gunnlaugsson. Several senior leaders placed their assets outside the reach of national tax authorities.*

- **Asset freezing:** measures taken by government or international authorities to prevent access to funds, assets or other economic resources belonging to specific individuals, entities or groups. France has a national system for freezing funds and economic resources that belong to, are owned, held or controlled by natural or legal persons, or any other entity that commits or attempts to commit

[2] Art. 421-2-2 of the Penal Code
[3] FATF Guide on PPE

commit, facilitate or finance acts of terrorism, incite them or participate in them. These measures enable compliance with the requirements of United Nations Security Council Resolution 1373 (2001).

- **The beneficial owner (BO)**: refers to the natural person or persons who, alone or in concert, directly or indirectly hold more than 25% of the capital or voting rights of the company, or exercise, by any other means, control over the management, administrative or executive bodies of the company or over the General Meeting of Shareholders.



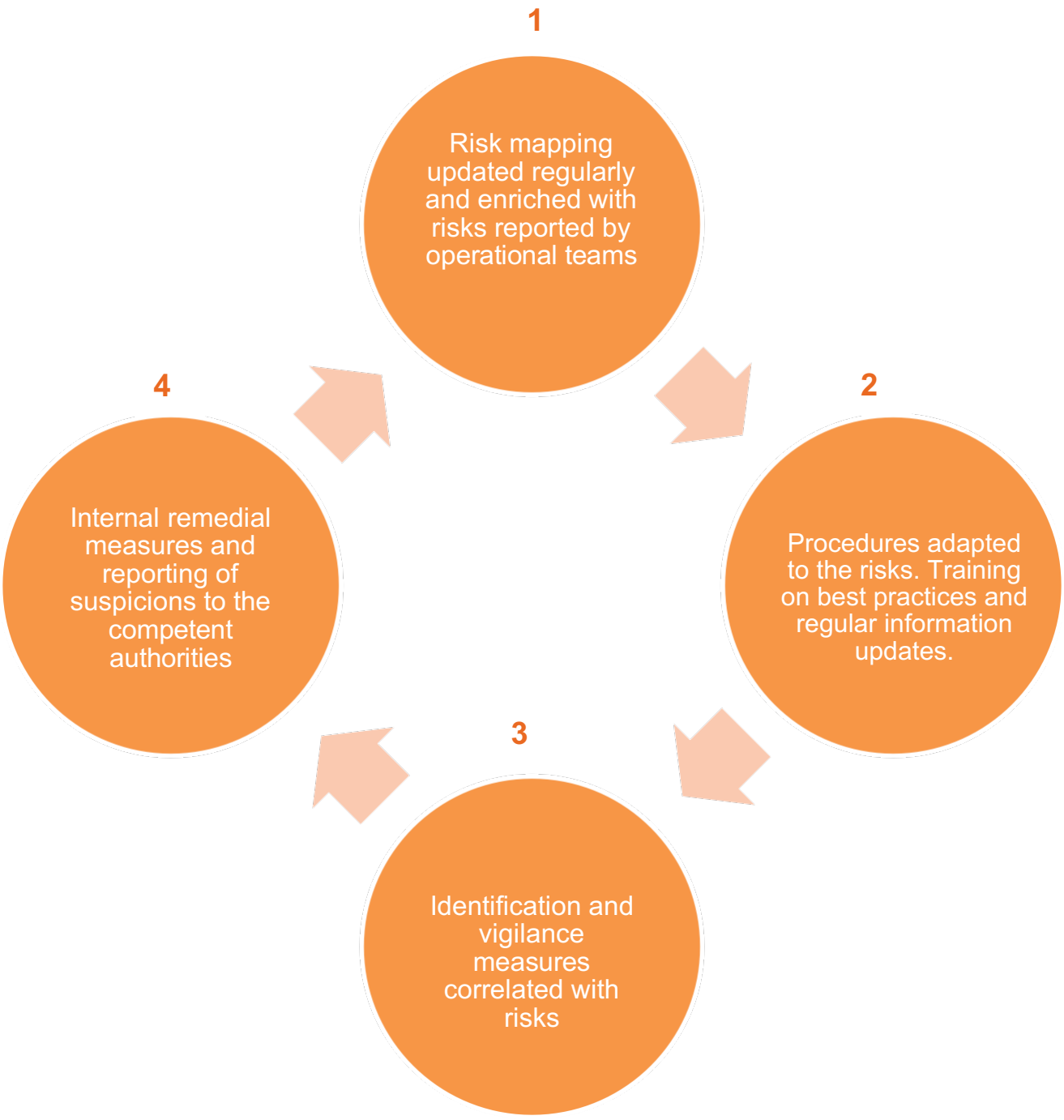

In the absence of any suspicion of money laundering, the legal representative or manager may be considered as the beneficial owner on a subsidiary basis when a natural person cannot be identified on the basis of the criteria of holding more than 25% of the shares, voting rights or control by any other means. For French public law legal entities located in the European Economic Area or in an equivalent third country, in accordance with the transparency rules governing them, the legal representative must be identified.

- **The financial intelligence unit**: a national body responsible for collecting, analysing and enriching suspicious activity reports that professionals are required by law to submit to it concerning suspicious facts that may relate to money laundering, associated predicate offences or terrorist financing. In France, the competent financial intelligence unit is TRACFIN.

- **The FATF (Financial Action Task Force)**: an intergovernmental body created in 1989 by the G7, which has developed a series of 40 recommendations recognised as the international standard for AML/CFT and monitors the progress made by its members in implementing them.

- **Country risk**: risk associated with financial transfers and transactions involving specific countries that have strategic deficiencies in their AML/CFT regime.

## III - AML/CFT MEASURES



Emeria and its subsidiaries must establish an internal organisation and procedures adapted to their sectors of activity. The Group ensures that its policy complies with national and international laws and regulations, and regularly updates it in order to protect its integrity.

Compliance with this policy prevents the Group and its subsidiaries from exposing themselves to reputational damage and/or financial loss for failing to comply with applicable standards. At the same time, it protects each employee from the risk of involvement in money laundering and terrorist financing.

## 3. Measuring risk

In accordance with its regulatory obligations and the recommendations of the competent authorities, the Group adopts a risk-based approach. Risk mapping enables the Group to analyse, identify and prioritise the risks it may encounter in the course of its activities. Risk mapping provides a clear and structured overview of the activities, areas and departments at risk within the entity. Based on this, procedures are developed and measures to prevent, mitigate, control and eliminate risks are identified.

Risk mapping is regularly updated, enabling risk management strategies to be adapted.

## 4. Training and information

The Group guarantees training for every employee. Upon joining the Group, new employees, whether permanent or temporary (corporate officers, managers, employees, casual workers, temporary workers, interns, work-study students, apprentices, volunteers, etc.), are given a training kit containing explanatory documents on the fight against money laundering and terrorist financing. The kit also includes simple scenario cards to illustrate different cases and explain the appropriate behaviour to adopt.

If necessary, internal communications will be sent out as soon as possible (emails, intranet) to inform employees of any changes in the law.

In addition, a **compliance officer** is appointed within each company of the group to answer any questions that may arise. If the compliance officer is unable to provide a satisfactory answer based on their knowledge, they must refer the matter to the Compliance Department by email at compliance@emeria.eu.

The Compliance Department is available to assist with any difficulties or questions relating to anti-money laundering and counter-terrorist financing.

## 5. Knowing the customer

Tailored to each situation, vigilance and control measures are correlated to the level of risk established when the relationship is established. The Group applies control and vigilance measures to varying degrees depending on the customer and the business relationship envisaged or in progress. These degrees of control and vigilance enable measures to be taken that are proportionate to the level of risk identified for each customer or transaction.

### a. Normal identification and vigilance[1st]level (KYC):

The most basic identification and vigilance measures are classified as "normal". The Group ensures that normal vigilance measures are implemented for all its customers for whom the initial identification does not present any particular risks and does not require enhanced monitoring. These cases do not require in-depth analysis as the risk of money laundering and terrorist financing appears low in view of the information gathered.

- **Normal identification:**

It must provide the customer's full name, date of birth and place of birth. In the case of a corporate customer, its legal form, company name, registration number and registered office address must be identified. Normal identification also makes it possible to identify the nature of the desired transaction and to collect the corresponding supporting documents.

As part of this identification process, it is necessary to:

- identify the customer on the basis of official, valid documentation from an independent and reliable source.
- identify and verify, where applicable, under the same conditions, the identity of the beneficial owners.

It is necessary to determine the natural person(s) who fall within the definition of beneficial owner and to apply to these persons the due diligence obligations appropriate to their profile.

*Example: Company O purchases a property for €750,000. After reviewing the documentation, it appears that Company O is wholly owned by Mr X, who holds a senior executive position. Mr X, the beneficial owner, is therefore considered a politically exposed person (PEP). In this case, "additional" due diligence measures should be applied*.

- Ensure that you have a good understanding of the purpose and nature of the proposed business relationship.
- determine that the business relationship does not involve criteria requiring a stricter classification (the business relationship does not involve PPE; the persons are not subject to restrictive measures; the nature of the proposed transaction is straightforward).

These identification measures are carried out as soon as the relationship with the customer is established and, failing that, imperatively before any binding signature.

When the identification does not present any particularities requiring enhanced controls, normal identification is sufficient. The vigilance measures that will then be put in place will also be classified as normal.

- **Normal vigilance:**

Throughout the business relationship, the customer identification file is updated with the information necessary to maintain appropriate customer knowledge for the maintenance and/or development of the business relationship. It is essential to ensure that the transactions carried out are consistent with the information known about the customer. (professional activities; risk profile; destination of funds). This vigilance is continuous throughout the customer relationship.

If, during the course of the relationship, one or more factors affect the categorisation of the customer profile, enhanced and/or additional vigilance measures may be necessary.

### b. Additional identification and vigilance:

#### ❖ Additional identification:

In certain cases, determined by law, it is mandatory to apply additional controls and vigilance. Due to these specific criteria, the persons identified present a higher risk of being involved in money laundering and terrorist financing. In addition to the "normal identification" elements, it is necessary to carry out a so-called "additional" check and to maintain a heightened level of vigilance throughout the business relationship.

When identification of the person reveals that:

- The customer or beneficial owner is a Politically Exposed Person. (The status of PEP also covers the immediate family of the PEP and natural persons acting as their permanent representatives).

- The transactions are carried out with a customer established in a territory included on a list of high-risk countries.

#### ❖ **Additional vigilance**:

In both cases, additional vigilance measures must be implemented:

- Identification at the outset of the relationship with the PPE. If, during the course of the relationship, the customer becomes a PPE, the customer will need to be reclassified and the additional procedures and controls will need to be applied.
  .

- Ensure the origin of the assets and funds involved in the relationship or transaction.

- Increased diligence, through more thorough research and controls, to clarify the situation.

- Enhanced and continuous monitoring of activity.

All these elements should enable a decision to be made on whether to establish or maintain a business relationship with this person.

In the event that it is impossible to carry out one of the additional measures and/or the customer refuses to provide the information necessary to verify their identity and/or the transaction, the decision will be made in accordance with regulatory obligations not to enter into or to terminate the business relationship with the customer.

In the event of serious doubt as to the legality of the desired transaction, these suspicions will be reported without delay to the competent national supervisory authorities.

### c. Enhanced identification and vigilance:

When certain characteristics specific to the product or transaction indicate that the risk of money laundering or terrorist financing should be considered high, an "enhanced" review must be carried out as part of the enhanced control and vigilance obligations.

#### ❖ Enhanced identification

The following criteria, without being exhaustive, may be considered as characteristics of a high risk of money laundering and/or terrorist financing:

If:

- the transaction is complex due to its nature or the number of parties involved.
- the amount of the transaction appears unreasonably high.
- The transaction appears to have no economic justification.
- The transaction has no lawful purpose.
- The transaction involves a luxury property.
- There is a discrepancy between the amount of the property for sale or rent and its actual value.

#### ❖ Enhanced vigilance

When one or more of the above points arise in the context of the operation or transaction, appropriate measures must be taken:

- a meticulous assessment of the risks of the operation and/or transaction must be carried out.
- The level of risk of the operation or transaction must be updated.
- If necessary, the Group shall report any activity that appears suspicious to the competent authorities in a timely manner.
- If necessary, the business relationship must be suspended while further checks are carried out.
- If the checks reveal any suspicion of money laundering and/or terrorist financing, the supervisory authority (TRACFIN) must be informed and follow the instructions given regarding the outcome of the transaction.

It is entirely possible, in view of the identification details and characteristics of the transaction, that additional vigilance measures and enhanced vigilance measures will need to be carried out.

**At each stage of the verification process, it is essential to keep evidence of all the steps taken.**

### 6. Dealing with persistent suspicions

As previously announced, if, due to the nature, identity of the person, transaction or operation, there are suspicions or reasonable grounds to suspect that the funds are of illegal origin or could be used to finance terrorism, the Compliance Department shall report the suspicious activity to the competent authorities as soon as possible.

The mapping is continuously updated with the risks encountered and information collected by the operational teams.

Where necessary, corrective measures are implemented and existing preventive measures are updated in order to resolve situations that do not comply with current regulatory requirements.

## IV - CONTINUOUS MONITORING

Emeria and its subsidiaries ensure **constant vigilance** of their customers and their operations, in particular through:

- A periodic review of the customer base;
- General monitoring of transactions carried out at various levels;
- An analysis of the consistency of transactions carried out with up-to-date knowledge of the customer.
- Detection and control tools.

If Emeria or one of its subsidiaries encounters an **unusual** or **suspicious transaction**:

- A suspicious transaction report must be filed with the relevant national financial intelligence unit.
- If a customer or beneficial owner is listed on a national asset freeze register, Emeria and its subsidiaries shall carry out the necessary due diligence specific to each jurisdiction and terminate the business relationship, if necessary.

The whistleblower procedure stipulates the conditions under which the Group guarantees confidentiality to the whistleblower.

## V - INFORMATION WITHIN THE GROUP

### 1. Exchange of information within the Group

The AML/CFT system implemented by Emeria is centralised at Group level.

This policy is common to the entire Emeria Group. Group employees and managers may share information with each other regarding anti-money laundering control and vigilance obligations.

Subject entities must promptly inform the Group's Compliance Department when they know, suspect or have reasonable grounds to suspect that funds, regardless of the amount involved, originate from criminal activity or are linked to **terrorist** financing.

Official reporting officers are appointed and only they will report any suspicions to the financial intelligence unit (TRACFIN) in the strictest confidence and where appropriate. The information collected must not be shared under any circumstances, even with employees and managers of Group entities or even with Emeria's senior management.

### 2. Document retention

All documentation relating to customer due diligence must be retained for a period not exceeding five years from the end of the business relationship or from the completion of the one-off transaction, in accordance with the legislation in force. This period is subject to more restrictive legal requirements regarding data retention.

The archiving system must enable those in charge to respond quickly to any request from a competent authority.

Each subsidiary is required to obtain information about and be familiar with the national law applicable to it in terms of data archiving and retention.

## VI - PENALTIES

In the event of non-compliance with this policy, disciplinary measures provided for in the Group's internal regulations may be taken.

In addition, criminal penalties, such as imprisonment and fines, may also be incurred. Entities or individuals affected by the violation of anti-money laundering and counter-terrorist financing obligations may seek redress and obtain damages.

## VII - FINAL PROVISIONS

This policy shall apply as soon as it is published on the Group's intranet. It shall be implemented under the responsibility of the Group Compliance Department, which shall also update it.

**GOOD PRACTICES:**

**If you have any questions, please contact your legal entity's compliance officer in the first instance. If necessary, the Group Compliance Department is at your disposal: compliance@emeria.eu**