

Anti-Money Laundering Policy Compliance

Last Updated

May 2024

1. The Company

Fasqon Unipessoal LDA is a company - provider of communication services Fasqon to different users worldwide. Therefore, it is important to ensure the appropriate identification of the company clients and the prevention of illicit activities, as specified below.

2. Objectives

The purpose of this policy is to establish the general framework of the company for the fight against money laundering (ML) and financing of terrorism (FT).

The company is committed to high standards of anti-money laundering/counter the financing of terrorism (AML/CFT) compliance and requires management and employees to adhere to these standards in preventing the use of its services for money laundering or terrorism financing purposes.

The AML program of the company is designed to be compliant with:

- International standards: recommendations and papers from the Financial Action Task Force (FATF).
- EU: "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".
- 5th AML Directive (The 5AMLD), which entered into force on January 10, 2020.

We evaluate the laws and regulations specific to each geographic location where we operate and build our compliance program in that jurisdiction to meet those requirements along with the following international requirements.

3. Money Laundering and Terrorism Financing

3.1. Money Laundering means:

- a) the conversion or transfer of property, knowing that such property is derived from criminal activity or from an act of participation in such activity, for the purpose of concealing or disguising the illicit origin of the property or of assisting any person who is involved in the commission of such an activity to evade the legal consequences of that person's action.
- b) the concealment or disguise of the true nature, source, location, disposition, movement, or rights with respect to, or ownership of, property, knowing that such property is derived from criminal activity or from an act of participation in such an activity.
- c) the acquisition, possession, or use of property, knowing, at the time of receipt, that such property was derived from criminal activity or from an act of participation in such an activity.

d) participation in, association to commit, attempts to commit, and aiding, abetting, facilitating, and counseling the commission of any of the actions referred to in points (a), (b), and (c).

Money laundering shall be regarded as such even where the activities that generated the property to be laundered were carried out in the territory of another country.

3.2. Terrorism financing means:

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

4. Organization of the AML/CFT function

4.1. Corporate organization

In accordance with the AML/CFT legislation, the company has appointed a responsible at the “highest level” – The Director, who is in charge of the enforcement of the AML policy and procedures within the company.

4.2. Employee training

All new hires will undergo the mandatory 6-hour AML training prior to the start of their employment.

Refreshing training will be provided at 18-month intervals, or upon major changes in AML legislation in force.

4.3. Enterprise-wide risk assessment

The 4th European Directive on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing requires financial institutions to take a risk-based approach to combating ML and TF. The risk assessment is a critical component of the company compliance management program.

As part of its risk-based approach, the company has identified and assessed risks specific to the company and its business, the customers to whom products and services are offered, transactions performed by these customers, delivery channels used by the company, the geographic locations of the customers and transactions and other qualitative and emerging risks.

The identification of AML/CFT risk categories is based on the company’s understanding of regulatory requirements, regulatory expectations, and industry guidance.

5. Minimum standards

5.1. The company has established standards regarding Antifraud Protection and Know-Your-Customer (“KYC”). These standards require the application of anti-fraud procedures on each prospective and existing customer via applying for real-time anti-fraud protection and if necessary, identification and verification of his identity on the basis of documents, data, or information obtained from a reliable source compliant with the European AML/CFT.

Interpretation of the KYC principle begins with the identification of the customer by means of the necessary identification documents.

In addition to these objective criteria, there are subjective elements that may arouse suspicions regarding a customer and to which particular attention should be paid.

Finally, as KYC does not involve static data, but dynamic data through the relationship with the customer, it also needs follow-up and ongoing monitoring of the customer.

6. Customer acceptance policy

6.1. Several elements require the establishment of a customer acceptance policy, in particular:

- accepting as customers only persons with which the company may and wishes to develop commercial relations.
- avoiding the company entering into business relations with persons who might involve it in money laundering or terrorism financing transactions.
- meeting a legal/regulatory requirement.
- applying the risk-based approach run by the company in categorizing customers in relation to risk criteria.

6.2. The acceptance policy is applied to any person asking for a product or service from the company.

As a general rule, customers who may be accepted by the company are persons:

- Fully identified in accordance with the company procedures.
- Designated as low risk.

Will not accept customer relations with persons not meeting the above acceptance criteria, or whose legitimate intentions do not immediately appear to be sufficient, or included in the European Union and the USA lists of persons or entities under financial sanction, or carrying on a commercial activity which is considered by the company as particularly at risk.

The company will ensure at all times separation between balances of different beneficiaries.

7. Ongoing transaction monitoring

AML-Compliance ensures that “ongoing transaction monitoring” is conducted to detect transactions that are unusual or suspicious compared to the customer profile.

Determination of the unusual nature of one or more transactions essentially depends on a subjective assessment, in relation to the knowledge of the customer (KYC) and their financial behavior.

8. Organization of internal control

8.1 Suspicious transactions

In its internal procedures, the company describes, for the attention of its staff members, when it is necessary to report and how to proceed with such reporting.

Reports of atypical transactions are analyzed by the management in accordance with internal procedures.

Depending on the result of this examination and on the basis of the information gathered, the management:

- will decide whether it is necessary or not to require additional verification procedures.
- will decide whether or not it is necessary to terminate the business relations with the customer.

8.2. Procedures

The AML/CFT rules, including minimum KYC standards, have been translated into procedures.

8.3. Record keeping

Records of data obtained for the purpose of identification must be kept for at least one year after the business relationship has ended.

Records of all transaction data must be kept for at least one year following the carrying out of the transactions or the end of the business relationship.