



MONEY LAUNDERING AND TERRORISM FINANCING PREVENTION POLICY

VERSION 1.0



SUMMARY

1. PURPOSE	4
2. DEFINITIONS	4
3. GOALS	6
4. PUBLIC	7
5. CONTENT	7
5.1. KYC – KNOW YOUR CUSTOMER	8
5.2. ENTITIES SUBJECTED TO SPECIAL MONITORING	8
5.3. ANALYSIS OF COMMERCIAL TRANSACTIONS	9
5.3.1. EXPORT AREA	9
5.3.2. FINANCIAL AREA	10
5.4. ORIGIN OF RECEIPT OF FUNDS AND RETURN	10
5.5. PREVENTION ACTIONS	11
5.6. EVIDENCE OF MONEY LAUNDERING AND TERRORISM FINANCING	12
5.7. TRAININGS	13
5.8. VIOLATIONS REPORT	13
6. GENERAL PROVISIONS	14
7. CONFIDENTIALITY STATUS	14

Marfrig's Compliance Policies may be adapted due to applicable laws in different jurisdictions. These adaptations, when issued, will be published through the document "Appendix- Country- Policy's Name" and will be available on the Intranet and local Human Resources.

1. PURPOSE

The purpose of this policy is to establish minimum guidelines for employees of the Company, Stakeholders and Third Parties under the guidelines for evaluating Third Parties and for preventing and combating Money Laundering and Financing of Terrorism.

2. DEFINITIONS

Company: Marfrig Global Foods S.A., its subsidiaries and the companies controlled and/or managed by it.

Sanctioned Entities: These are persons and/or entities identified by consolidated lists subject to financial or commercial sanctions based on national and international security policies against countries, regimes, terrorists and traffickers at the international level (e.g. Office of Foreign Assets Control - OFAC).

Financing of Terrorism: Financing of Terrorism consists of any practice that provides financial support to the group or individual that encourages, plans, or practices terrorist acts. The assets responsible for financing such acts may be collected from **lawful sources** (through personal donations and/or profits from "front" companies and charitable organizations) or **illicit** (through profits from drug trafficking, arms smuggling, fraud, among others).

Because it receives assets anonymously, the fight against Terrorism is closely connected to the fight against Money Laundering, since the two practices use essentially the same techniques for hiding resources.

Know Your Customer (KYC): Process of prior inspection of potential Partners, in order to verify potential risks that may adversely affect the Company.

Money Laundering: The practice of Money Laundering is regulated by Laws No. 9,613/1998 and 12,683/2012 and consists of concealing or dissimulating the nature, origin, location, disposition, movement



or ownership of goods, rights or values arising, directly or indirectly, from illegal and criminal activities, such as corruption, terrorism, tax fraud, among others. This set of commercial and financial operations is carried out through a dynamic process, in which the phases are:

a. Placement: The proceeds from illegal activity are placed in the economic system and, in order to hide its origin, this amount is moved in countries with more permissive rules, with a liberal financial system, the so-called Tax Havens;

b. Concealment: After entering the value into the economic system, assets are moved electronically, preferably to anonymous accounts or through transactions in accounts opened in the names of "front men" or fictitious companies. With the concealment, the evidence trail of Money Laundering is erased and the accounting tracking and monitoring of illicit resources is significantly impaired;

c. Integration: The assets are formally incorporated into the economic system as legal resources and are generally applied in markets such as real estate, luxury goods and capital markets.

Countries Subjected to Sanctions: Countries with which any transactions are prohibited under the European Union (EU) and United Nations (UN) sanction programs, observed the rules for allowing the negotiation of items considered humanitarian, such as: food and medicine.

Tax Havens: These are regions that have more liberal financial regulation and allow transactions of financial resources to be carried out without identifying those involved and with reduced or even non-existent rates. The confidentiality of the accounts and the strong banking secrecy make these regions great hubs for Money Laundering, Corruption and Financing of Terrorism practices.

Stakeholders: Controllers, shareholders, directors and members of the Company's committees.

PEPs: Politically Exposed Persons (PEPs) are considered to be individuals who have or have performed, in the last 5 (five) years, in Brazil or in foreign countries, territory and dependencies, positions, jobs or relevant public functions, as well as their representatives, family members and close collaborators.

Third Parties: Include various entities and individuals acting on behalf of a company, including, but not limited to, agents, consultants, sales representatives, customs agents, resellers, subcontractors, franchisees, lawyers, accountants, similar intermediaries or entities with no business relationship with the Company and who make payment on behalf of the Company's end customers.

Commercial Transactions: These comprise exports and re-exports of goods, the transportation of these items to their final destination and financial operations to receive funds from export/re-export operations.

3. GOALS

This policy aims to:

- Establish minimum guidelines to prevent and detect possible concealment of assets and financial resources, operations with Sanctioned Countries, persons or Entities and/or transactions

that have suspicious characteristics that may incur in crimes of Money Laundering and Financing of Terrorism at the national level and/or international;

- Establish minimum guidelines on the expected behavior of the Company's employees, Stakeholders and Third Parties acting on behalf of the Company, as well as presenting mechanisms for internal controls to prevent and detect any situations that may be interpreted as non-conformities;
- Highlight the need for the knowledge of the Third Parties with whom the Company relates and maintains commercial and financial relations.

4. PUBLIC

It applies throughout the value chain, regardless of geographic location. Thus, this policy is applicable to all employees of the Company, Stakeholders and Third Parties acting on behalf of the Company.

5. CONTENT

The Company's relationship with its customers is one of the most important links in its commercial activity and, for this reason, it deserves to be highlighted in this policy.

When relating to third parties, the Company's image and reputation is directly affected by the actions that its business partners take.

Compliance with this policy is essential to maintain the transparency and reputation of our businesses and activities, which is why the Company does not tolerate the practice of any illegal acts, such as paying bribes, kickbacks and other acts of corruption.

5.1. KYC – KNOW YOUR CUSTOMER

In order to protect itself and protect the Company, it is important that all employees, Stakeholders and Third Parties, acting on behalf of the Company, are attentive to carry out all prevention procedures with caution. For this reason, the registration and collection of information of each Third Party that comes to deal with the Company is mandatory.

This way is possible to verify whether the partner is in accordance with the rules, guidelines and values of the Company and whether or not its commercial activity represents a substantial risk to our business.

The Third Party's knowledge plays a fundamental role in the Company's contracting structure, and the identification and knowledge of this partner and its activities is essential.

For this reason, any and all contracting with a Third Party that fits one of the profiles mentioned in item 5.2., at national and/or international level, is forbidden, without it being submitted to the proper Know Your Customer (KYC) Company procedure.

The procedures for hiring the Company's Third Parties must be included in a specific procedure.

5.2. ENTITIES SUBJECTED TO SPECIAL MONITORING

These are people/companies that deserve more attention and, therefore, greater monitoring because they are identified as highly sensitive Third Parties for the Company:

- Companies that have a relationship or that have a member of the Senior Management and/or Partner with more than 5% equity related to Politically Exposed People (PEPs);
- People/Companies known by media for involvement in illegal activities;

- Consultancies, engineering companies, law firms, commercial development companies, tourism agencies and NGOs;
- Third parties that are headquartered or maintain relationships with countries with favorable taxation (tax havens);
- Third parties that are based in or maintain relationships with Countries Subjected to Sanctions (e.g. Iran);
- Agent responsible for intermediating Commercial Transactions;
- Entities benefiting from Commercial Transactions.

5.3. ANALYSIS OF COMMERCIAL TRANSACTIONS

All Commercial Transactions must be preceded by a wide and prior verification by all parties involved.

5.3.1. EXPORT AREA

It is the responsibility of the Director of the Foreign Trade area to collect, in advance for the completion of Commercial Transactions, the registration data/document of all parties involved in such transactions.

Based on the information obtained, all parties involved in Commercial Transactions must be submitted to the Know Your Customer (KYC) process, made available by the Company, and the entire process must be kept on file.

5.3.2. FINANCIAL AREA

The Financial Area is responsible for making sure that the remittances of resources from Commercial Transactions are in accordance with the negotiations and export documentation, and that the resources were remitted directly by the final customer or by Third parties that have been submitted to the Company's Know Your Customer (KYC) process.

It is the responsibility of the Chief Financial Officer to evaluate and ensure that remittances of funds can only be processed by the Company and, consequently, received, if they are strictly in accordance with the Commercial Transactions dealings.

5.4. ORIGIN OF RECEIPT OF FUNDS AND RETURN

Any and all receipt of funds by the Company must be supported by documents that prove the operation that gave rise to the payment. The amounts must always come from bank accounts owned by the client with whom the Company has done business or from financing institutions related to the operation, being exceptionally acceptable to receive amounts sent by Third Parties, provided they have been submitted to the Company's Know Your Customer (KYC) process.

In the event that the Company receives funds from bank accounts that are not owned by the final customers or their financing institutions related to the operation or Third Parties that have not been submitted to the Company's Know Your Customer (KYC) process, the Company must expressly notify its final customer in the sense that it does not recognize the receipt of funds to satisfy the client's debts and that the receipt of such funds will be rejected by the Company with the receiving financial institution.

In any event in which the Company has to make a return of funds to its customers, in any capacity, the return can only be carried out upon express request from the customer and indication of bank accounts owned by the customer and kept in the jurisdiction in which the funds have been sent.



5.5. PREVENTION ACTIONS

All the phases already described in this Policy are part of a group of actions that aim to allow the prevention and monitoring of suspicious activities that may have a connection with the crimes of Money Laundering and Financing of Terrorism, reflecting the Company's commitment and values. For this reason, the procedure is periodically reviewed and updated, in accordance with the best national and international compliance practices.

For prevention and monitoring to be effective, it is highlighted:

- Know Your Customer (KYC) procedure;
- Implementation of a control and monitoring tool that allows the detection of suspected third parties;
- Procedure for interaction between the Company's Export, Financial and Compliance areas.

5.6. EVIDENCE OF MONEY LAUNDERING AND TERRORISM FINANCING

It is of utmost importance that all the Company's employees are fully aware of this policy, so that it can identify any signs that characterize Money Laundering and Financing of Terrorism, such as:

- Legal Entities other than those that maintain a commercial relationship with the Company make the payment for any Commercial Transaction;
- Evidence a sudden and objectively unjustified change in relation to the operational modalities usually used by the involved;
- It is not possible to identify the final beneficiary;
- There is resistance in providing information necessary to carry out the Know Your Customer (KYC) procedure;
- There are characteristics that may constitute an artifice to circumvent the identification of the personnel involved and/or beneficiaries in Commercial Transactions;
- Declaring several bank accounts and/or modifying them as usual.

5.7. TRAININGS

In order to maintain the high standards of conduct of the Company, as well as its commitment to Fighting Money Laundering and Financing of Terrorism, the Company offers a training program that addresses Money Laundering and Financing of Terrorism Prevention, which is based on this policy, in order to inform its employees about all the topics mentioned here.

For the group of people identified as having a greater relationship with the topic, targeted training will be given, addressing the topics provided for in this policy.

5.8. VIOLATIONS REPORT

Any and all employees who become aware of a violation of the law and/or this procedure must report the facts directly to the Company's Compliance Area. Violations may also be reported through the Helpline (Whistleblower Channel) via e-mail etica@marfrig.com.br, through the website www.marfrig.com.br/compliance or by calling 0800 223 1000.



6. GENERAL PROVISIONS

When observing potential conflicts between the internal rules/guidelines of the Company, employees must guide their conduct considering the most restrictive rule/guideline.

7. CONFIDENTIALITY STATUS

This is a public policy.





www.marfrig.com.br