ANTI-MONEY LAUNDERING POLICY

AML COMPLIANCE

Belfius

Table of Contents

1. The Company

Belfius Bank ("Belfius") is an autonomous Belgian banking and insurance group wholly owned by the Belgian federal state through the "Société Fédérale de Participations et d'Investissement" (SFPI).

Belfius is, above all, a local bank, collecting savings deposits and investments via its distribution networks in Belgium and reinvesting these funds into Belgian society by providing loans to individuals (mainly mortgage loans), the self-employed, small and medium-sized enterprises and the liberal professions, corporates, and, in particular public and social institutions.

Belfius is registered in Brussels as a credit institution according to Belgian law and regulations.

Belfius is regulated by both the National Bank of Belgium (NBB) and the Financial Services and Markets Authority (FSMA).

Belfius is an obliged entity as referred to in Article 5, § 1, 4° of the Belgian law on the prevention of money laundering and terrorist financing and on the restriction of the use of cash (hereafter 'Belgian AML Law') and in Article 2 of the European Directive on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing ("Directive 2015/849 of the European Parliament and Council and its subsequent amendments").

2. Introduction

Money laundering and terrorist financing pose significant threats to the global financial system, undermining economic stability and facilitating criminal activities.

This policy is an integral part of Belfius' commitment to uphold the integrity of the financial system and to protect our customers and stakeholders from the risk associated with financial crime.

This AML Policy is reviewed and updated regularly to reflect changes in legislation, emerging risks and best practices.

3. Definition

'Money laundering' means the conduct set out in Article 3, paragraphs 1 and 5, of Directive (EU) 2018/1673

(a) the conversion or transfer of property, knowing that such property is derived from criminal 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, rights with respect to, or ownership of, property, knowing that such property is derived from criminal activity;

(c) the acquisition, possession or use of property, knowing at the time of receipt, that such property was derived from criminal activity.

It also includes aiding and abetting, inciting and attempting to commit that conduct.

'Terrorist 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, to commit, or to contribute to terrorist activities.

4. Objectives

The objective of this policy is to establish the general framework within Belfius for the fight against money laundering (ML) and the financing of terrorism (FT), in accordance with applicable laws, directives, regulations, international standards, guidelines and recommendations.

Belfius puts reasonable measures in place to control and to limit ML/FT risk, including dedicating the appropriate means.

Belfius is committed to high standards of anti-money laundering/countering the financing of terrorism ("AML/CFT") compliance and requires management, employees and subsidiaries to adhere to these standards in preventing the use of its products and services for money laundering or terrorism financing purposes.

5. Governance at group level

This policy outlines a comprehensive approach for managing AML/CFT risks across the entire banking and insurance group that Belfius forms with its main financial subsidiaries.

For this purpose, the Anti-Money Laundering Compliance Officer ("AMLCO") of Belfius Bank also assumes the role of Group AMLCO.

In this capacity, the Group AMLCO is responsible for ensuring that these subsidiaries have themselves designated an AML manager or, when legally required, an AMLCO. Additionally, the Group AMLCO verifies that the subsidiaries have implemented policies aligned with the principles outlined herein, tailored appropriately and proportionately to their specific activities.

He/she reports to the Chief Compliance Officer who reports directly to the Chief Risk Officer, a member of the management board who is responsible at the highest level for the prevention of ML/FT.

Information sharing within the group is ensured by the use of a common customer repository, allowing the coordination of acceptance policies and customer due diligence measures.

6. Policy implementation requirements

Each major change of the Belfius AML Policy is subject to approval by the bank's management board.

6.1 Group-wide Risk Assessment ("GWRA")

As part of its risk-based approach, an AML Enterprise-Wide Risk Assessment ("EWRA") is conducted at group level (a "GWRA") to identify and understand risks specific to Belfius, its business lines and subsidiaries.

The Belfius AML risk profile is determined after identifying and documenting the risks inherent to its business lines such as the products and services the bank offers, the customers to whom such products and services are offered, the transactions performed by these customers, the delivery channels used by the bank, the geographic locations of the bank's operations, customers and transactions and other qualitative and emerging risks.

The GWRA is documented, kept up to date and reviewed yearly. Furthermore, it is kept at the disposal of the NBB.

Belfius Banque SA - Place Charles Rogier 11, 1210 Bruxelles · Téléphone +32 2 222 11 11 · belfius.be
RPM Bruxelles TVA BE 0403.201.185 · IBAN BE23 0529 0064 6991 · BIC GKCCBEBB · FSMA n° 19649 A

6.2 Know Your Customer (“KYC”)

6.2.1 Customer identification and verification

The primary goals of the identification and verification procedures are to (i) gather relevant information that clearly distinguishes customers, agents and beneficial owners from other individuals, and (ii) verify this information against reliable documents or sources to ensure a high degree of certainty regarding the identities of the individuals involved.

These procedures are based on the following key principles:

- Every customer, agent, or beneficial owner must be identified and their identity verified using original, reliable, and independent supporting documents, such as a valid ID or passport, before entering into a business relationship or exercising their authority to make binding agreements on behalf of the customer they represent (in the case of agents).
- When verifying the identities of beneficial owners of legal entities, Belfius will take reasonable measures to understand the ownership and control structure of the entity. This will be supported, when necessary, by original, reliable, and independent documents, such as extracts from the Belgian Gazette or documents filed with the registry of the Commercial Court.
- Identification must be completed through "face-to-face" contact. Remote identification is also permitted through a dedicated acceptance process but may restrict the ability to carry out certain transactions or access specific products.
- The Know Your Customer-Policy as defined in chapter 6.2.2 outlines which customer data is collected and the frequency of its review, mainly depending on the client’s risk level.

If Belfius cannot meet the identification and verification obligations within the required time limits, it will not establish a business relationship or conduct transactions for the customer.

6.2.2 Individual Risk Assessment and Know Your Customer-Policy (“KYC Policy”)

The primary objective of the KYC Policy is to establish guidelines that help mitigate the risks associated with ML/TF when Belfius initiates business relationships with new clients or re-evaluates existing ones.

This policy outlines the risks linked to each business relationship, as identified by the GWRA. It also aligns Belfius Bank's primary objective to support the Belgian economy by serving households, businesses, and public services that are established in Belgium or generate income from activities within the country.

Characteristics of the client and the purpose and nature of the business relationship are collected through responses registered by the relationship manager or client in the 'Know Your Customer' questionnaire.

The KYC Policy details the decision-making process for establishing or ending a business relationship or executing an occasional transaction in accordance with the guidelines of the NBB concerning de-risking.

Belfius will not establish or maintain business relationships if the associated risks are deemed too high. Consequently, Belfius Bank will not engage with or retain business relationships with, among others:

- Entities or individuals seeking to operate anonymous or fictitiously named accounts.
- Unlicensed /unregulated banks or non-banking financial institutions (NBFIs).
- Entities or individuals providing banking services to unlicensed banks.
- Shell company/banks or entities known for accepting shell bank accounts .

- Unlicensed or unregulated remittance agents, exchange houses, casas de cambio, bureaux de change, cryptocurrency platforms, or money transfer agents. (custodial wallet providers or startups launching ICO's)
- Entities or individuals whose business relationship's purpose and nature are not sufficiently clear. Belfius considers the purpose and nature of the relationship insufficiently clear when the customer does not possess a sufficiently strong economic tie or economic activity with or in Belgium.
- Customers, representatives, or beneficial owners who cannot sufficiently explain or prove his/her source of funds or source of wealth.
- Customers, representatives, or beneficial owners who cannot be identified or whose identities cannot be sufficiently verified.
- Customers, representatives, or beneficial owners listed on embargo or terrorist lists issued by the UN, EU, OFAC, OFSI, or local authorities.
- Customers, representatives, or beneficial owners associated with serious negative news.
- Customers, representatives, or beneficial owners with ML/TF risks that cannot be managed due to the presence of high-risk indicators as described in detail in the KYC Policy.
- Customers, representatives, or beneficial owners with whom the Bank previously terminated a business relationship due to concerns related to ML/TF.
- The customer or beneficial owner or anyone associated with them have handled the proceeds from crime.
- There is no sound economic or lawful rationale for the customer requesting the type of financial service sought.

The KYC Policy is reviewed annually and updated whenever significant events occur could alter the nature and extent of the bank's risks.

6.2.3 Politically Exposed Persons-Policy ("PEP Policy")

The PEP Policy of Belfius is part of its KYC Policy, developed in accordance with Article 8, § 2, 1° of the Belgian AML Law.

Politically Exposed Persons (PEPs) are individuals who are exposed to particular risks as a result of the prominent public (political, judicial, or administrative) functions they hold or have held.

The Belgian AML Law requires that the PEP characteristic must be considered a risk criterion in the individual assessment of the customer's AML risk, necessitating enhanced vigilance measures both at the time of acceptance and in the context of ongoing vigilance towards the customer and their transactions.

The PEP Policy aims to establish principles for mitigating money laundering risks when a customer is or becomes a PEP, or is a family member or close associate of a PEP, as defined by the Belgian AML Law.

6.2.4 Ongoing Customer Due Dilligence ("CDD")

Ongoing CDD is an essential mechanism that complements the initial customer due diligence conducted during the onboarding process.

This ongoing CDD is ensured by a KYC review and automated transaction monitoring.

6.2.4.1 KYC Review

Regular KYC reviews are conducted and monitored following a risk based approach.

6.2.4.2 Transaction monitoring

Cfr. Infra: Chapter 6.3 'KYT' – 'Monitoring of Transactions'.

6.3 Know your transactions (“KYT”)

6.3.1 Monitoring of transactions

The Anti Money Laundering Unit (“AML Unit”), under the direct supervision of the AMLCO, is responsible for conducting ongoing transaction monitoring to identify any transactions that appear atypical or suspicious when compared to the customer's expected transactional behavior.

Belfius has implemented an automated transaction monitoring system designed to detect unusual or suspicious activities. This real-time system employs advanced and future proof anomaly detection techniques. To ensure its effectiveness, the system is regularly updated and retrained.

The AML Unit conducts manual reviews and investigations of alerts generated by the transaction monitoring system, which identifies potentially suspicious transactions, through the application of a risk-based approach, either by the alert classifiers or by the built-in high-end thresholds.

Investigations can also be initiated based on notifications from various sources, such as Belfius’s business lines, negative news reports and external entities like the prosecutor’s office or the Financial Intelligence Unit (FIU), and specific queries such as those detecting fund repatriations.

Belfius has established clear internal guidelines instructing staff on when and how to report to the AML Unit, ensuring an efficient reporting process. The AML Unit follows a detailed methodology for analyzing atypical transactions as specified in these internal procedures.

6.3.2 Suspicious Transactions reporting (“STR”)

Reports and signals of atypical transactions are analyzed within the AML Unit under the direct supervision of the AMLCO.

Reports of suspicious transactions are submitted to the Belgian Financial Intelligence Unit (“FIU”). If the individual assessment outlined in the declaration to the FIU determines that vigilance cannot be ensured, Belfius may terminate the relationship in accordance with the NBB's derisking guidelines. The reports are accurate, complete, and submitted in a timely manner, in accordance with regulatory requirements and internal policies.

6.3.3 Sanctions and Embargoes Policy (“S&E Policy”)

The S&E Policy outlines the principles and standards for Belfius’ sanctions compliance program, designed to mitigate exposure to sanctions risk. It defines the roles and responsibilities that must be integrated into the operational procedures of all business lines, including control and monitoring measures during client onboarding, ongoing client relationships and regarding transactions processed through Belfius.

To ensure compliance with applicable sanctions against individuals and entities, Belfius has implemented a list matching system in order to compare the names of its customers with official lists from Belgium , the European Union, OFAC, OFSI and the UN. Additionally, transactions are filtered through an online matching system to ensure adherence to sanctions obligations for fund transfers with other banks.

To ensure compliance with applicable trade sanctions (embargoes), Belfius employs an online matching system to monitor transactions involving jurisdictions under embargo.

Belfius Bank internally edits and maintains a Country Watchlist (“BCWL”), in order to give all business lines access to current information regarding jurisdictions under embargo.

This list includes the following jurisdictions:

- Jurisdictions subject to EU export sanctions (including the sanctioned goods).
- Jurisdictions subject to EU import sanctions (including the sanctioned goods).
- Jurisdictions subject to US sanctions (including the sanctioned goods or transactions).
- Jurisdictions designated by officials (such as FATF) as subject to a higher money laundering risk.
- Jurisdictions considered tax havens by the Belgian authorities.

7. Organization and internal control

7.1 Procedures

Belfius has established detailed and operational instructions and requirements covering the entire AML/CFT value chain. These guidelines are validated under the supervision of the AMLCO. It is distributed to all concerned staff, and updated regularly, particularly following any changes in the overall risk assessment.

7.2 Training and awareness

Belfius has put in place training and awareness programs to educate employees about ML/TF risks, methods, trends, typologies, and the risk-based approach implemented to mitigate these risks.

These initiatives aims to ensure that all employees understand their roles and responsibilities in preventing and detecting ML/TF activities and sanction and embargoes breaches.

Training programs will be continuously updated to reflect changes in regulations, emerging risks, and internal policies.

The bank will maintain comprehensive records of all training and awareness activities.

7.3 Record keeping

Belfius will ensure that records collected for the purpose of preventing money laundering and terrorist financing are retained in accordance with the EU General Data Protection Regulation (GDPR) and the Belgian AML Law.

These records shall not be subjected to any further processing that is inconsistent with the intended purposes.

Belfius will ensure records are readily accessible for regulatory reviews and audits.

7.4 Auditing / Monitoring

As a second line of defense, the Compliance function is also responsible for proactively testing and monitoring on a risk based approach to ensure that the policies, procedures, processes and controls established by the first line of defense are operating effectively and in accordance with AML regulatory requirements.

This includes conducting independent risk assessments to identify and evaluate the accuracy and effectiveness of various processes, to verify compliance with applicable regulations.

Furthermore, Key Risk Indicators (“KRIs”) are established to assess whether the compliance policies, procedures, and controls are effective.

In addition to routine monitoring, certain incidents or events, such as fraud, audit findings, or regulatory remarks, may necessitate temporary enhanced monitoring.

Belfius | **Belfius Banque SA** - Place Charles Rogier 11, 1210 Bruxelles · Téléphone +32 2 222 11 11 · belfius.be
RPM Bruxelles TVA BE 0403.201.185 · IBAN BE23 0529 0064 6991 · BIC GKCCBEBB · FSMA n° 19649 A

Where appropriate, Compliance can also initiate additional measures such as the attribution of recommendations.

The primary AML key risks are consolidated quarterly into formal risk reports ("Risk Appetite Framework Report") and presented to the governance bodies.

7.5 Exchange of information

The prohibition not to disclose information transmitted to the FIU does not apply:

- to notifications from Belfius to the NBB in its capacity as competent supervisory authority, nor to disclosures for law enforcement purposes.
- among entities of the Belfius Group (established within the European Economic Area (EEA) or member countries of the Financial Action Task Force (FATF).
- towards financial and credit institutions not belonging to the Belfius Group, provided that:
  - the financial institution receiving this information is involved in the same transaction with the same customer.
  - the recipient being subject to equivalent AML/CFT legislation
  - the exchanged information is exclusively used for the purpose of prevention of money laundering or terrorism financing.
  - the recipient being subject to equivalent obligations of professional secrecy and personal data protection.

7.6 Internal whistleblowing

Belfius has established an internal whistleblowing procedure to uncover violations of the AML Law / Regulations or to report suspicious activities.

This procedure provides whistleblowers with specific legal protections within a strict legal framework. Belfius considers the whistleblowing procedure to be a very specific, preferably internal alarm system that allows whistleblowers to report violations confidentially and in good faith, so that Belfius can timely prevent or mitigate any damage.

This procedure is utilized by the whistleblower when they believe that all other internal procedures are unsuitable, particularly when it is impossible, inappropriate, or inopportune to discuss the (suspected) violation with their direct hierarchy.

Belfius Banque SA - Place Charles Rogier 11, 1210 Bruxelles · Téléphone +32 2 222 11 11 · belfius.be
RPM Bruxelles TVA BE 0403.201.185 · IBAN BE23 0529 0064 6991 · BIC GKCCBEBB · FSMA n° 19649 A