KBC GROUP: ANTI MONEY LAUNDERING POLICY

30 October 2024

TABLE OF CONTENTS

1. THE GROUP

KBC Group is an integrated bank-insurance group, catering mainly for retail, private banking, SME and midcap customers. Our core markets are Belgium, the Czech Republic, Slovakia, Hungary and Bulgaria. We are present to a limited extent in several other countries.

Through our activities, we want to help our customers to both realise and protect their dreams and projects.
It is our ambition to be the reference for bank-insurance in all our core markets.

2. INTRODUCTION

In response to the international community's growing concern with regard to money laundering and possible financing of terrorism, many countries worldwide enacted or strengthened their laws and regulations regarding this subject. Money laundering in Belgium has been a punishable offence since 1990. In addition the Law on preventing the use of the financial system for purposes of laundering money and terrorism financing of 18 September 2017, based on Directives issued by European Parliament and Council, specifies relevant legal requirements for the financial sector (i.e., credit institutions and a wide range of other financial institutions) to effectively prevent money laundering and the financing of terrorism.

3. OBJECTIVES

The purpose of this policy is to establish the general framework for the fight against money laundering and terrorism financing throughout the KBC Group.
KBC Group is committed to high standards of anti-money laundering / counter terrorism financing (AML/CTF) compliance and requires management and employees to adhere to these standards in preventing the use of its products and services for money laundering or terrorism financing purposes.

Therefore, credit and financial institutions being part of the KBC Group are expected to develop a comprehensive AML-program. The cornerstone thereof is based on Group Compliance Rules and encompasses "Know Your Customer" (KYC) and "Know Your Transactions" (KYT) requirements. considered by the Group as minimum standards. Taking into account local regulatory requirements and Guidelines issued by the European Banking Authority (EBA), these standards are transposed to local procedures.

4. DEFINITIONS

Money laundering is:

- 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
- 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;
- 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.

Terrorism financing is the provision or collection of funds and other assets, by any means, directly or indirectly, with the intention that they will be used, or in the knowledge that they are to be used, in full or in part, by a terrorist organization or by a terrorist acting alone, even without any connection to a particular act of terrorism.

5. GOVERNANCE

The General Manager of the Financial Crime Unit within Group Compliance is responsible for AML/CTF and sanctions screening across KBC Group. He/She furthermore acts as the Group Anti-Money Laundering Compliance Officer (AMLCO)to whom all local AMLCO have a functional reporting line. He/She reports to the Group Chief Compliance Officer who reports directly to the Chief Risk Officer, member of the KBC Group Executive Committee who is responsible for group-wide adherence to applicable AML/CFT regulations and obligations.

6. MINIMUM STANDARDS

Following standards are to be considered as minimum requirements for all credit and financial institutions of the Group and are elaborated in more detail in group-wide Compliance Rules with respect to “Know Your Customer” and “Know Your Transactions”.

6.1. Enterprise-wide Risk Assessment (EWRA)

In accordance with the current EU AML Directives on the prevention of the use of the financial system for the purposes of money laundering or terrorism financing (Directive 2015/849) and as part of KBC Group’s risk-based approach, all entities of KBC Group are required to assess on a yearly basis the risks of money laundering and terrorism financing, taking into account risk factors relating to their customers, countries or geographic areas, products, services, transactions and delivery channels. These enterprise-wide risk assessments are documented, kept up-to-date and made available to the local competent authorities.

6.2. Know Your Customer (KYC)

6.2.1. Customer Identification and Verification

KBC Group has established standards regarding Know-Your-Customer. These standards require due diligence on each prospective customer before entering into a business relationship:

- via identification and verification of his identity and, as the case may be, his representatives and beneficial owners on the basis of documents, data or information obtained from a reliable and independent source including, where available, electronic identification means, relevant trust services as set out in the EiDAS Regulation (910/2014) or any other secure, remote or electronic identification process regulated, recognized, approved or accepted by the relevant national authorities

- via obtaining information on the purpose and intended nature of the business relationship, such as type and size of payments that can be expected.

- via obtaining information on the characteristics of the customer:
  - the home country or country of residence or registration
  - the country of birth or incorporation
  - the nationality
  - the profession
  - the economic activity
  - the appearance on sanction lists
  - the PEP-status (politically exposed persons) of customers, representatives and beneficial owners
  - the delivery channel (face-to-face or remotely with or without safeguards);
  - the source of wealth

- the complexity of the ownership structure
- the type of customer

6.2.2. Individual Risk Assessment

✓ The factors taken into account for the individual risk assessment and classification (unacceptable-high-medium-low risk) of our customers on a risk-sensitive basis are the ones that are in scope of the Enterprise-Wide Risk Assessment as mentioned above and relate to the same categories of risk:

- Delivery channel risk
- Product, service or transaction risk
- Customer risk
- Geographical risk

The relevant risk factors that are taken into account are the ones that are mentioned in:

- Directive 2015/849 (AMLD4) on the prevention of the use of the financial system for purposes of money laundering or terrorist financing, as amended by Directive 2018/843 (AMLD5)
- EBA Guidelines under Articles 17 and 18(4) of Directive (EU) 2015/849 on customer due diligence and the factors credit and financial institutions should consider when assessing the money laundering and terrorist financing risk associated with individual business relationships and occasional transactions (EBA/GL/2021/02)
- (supra-)national risk assessments
- local AML Law and/or regulations

✓ Customer Acceptance Policy

KBC Group refuses to establish or to maintain a business relationship if the ML/TF risk related to the business relationship appears too high. Therefore, KBC Group will not enter into/maintain business relationships if:

- It concerns a shell company/bank (= entities without any physical presence) or a credit institution or financial institution that allows its accounts to be used by a shell bank
- It concerns offshore patrimonial companies (= passive NFE's)
- It concerns cash, cheques or physical securities without the customer being identified face-to-face or identified remotely with safeguards
- It concerns opening and keeping of anonymous and fictitious named accounts;
- It concerns long-term products (loans, life insurance policies) as long as the customer has not been identified, his identity verified and accepted in an appropriate way
- It concerns unlicensed/unregulated banks, non-banking financial institutions, money remittance agents, exchange houses, football clubs, gambling entities, cryptocurrency platforms, custodial wallet providers or startups launching ICO's
- It is not satisfied that the purpose and nature of the business relationship are legitimate
- It is not satisfied that the ML/TF risk can be effectively managed, such as no or insufficient identification and verification of the identity of the customer, his representative(s) and/or beneficial owner(s)
- The customer's or beneficial owner's source of wealth or source of funds cannot be explained (for example through their occupation, inheritance or investments)

- There is no sound economic or lawful rationale for the customer requesting the type of financial service sought
- The customer, its representative and/or beneficial owner is a person or institution appearing on an embargo or terrorist list issued by EU, OFAC or local authorities
- The customer or beneficial owner or anyone associated with them have handled the proceeds from crime
- There is in-house negative information about the customer's or the beneficial owner's integrity, obtained, for example, in the course of a long-standing business relationship
- The customer, its representative and/or beneficial owner is a person with whom a KBC Group entity discontinued the business relationship in the past for AML/TF reasons

6.2.3. Ongoing Customer Due Diligence

Periodic and risk-based reviews are carried out to ensure that customer-related documents, data or information are kept up-to-date.

6.3. Monitoring of Transactions (Know your Transactions (KYT))

Local Compliance functions ensure that ongoing transaction monitoring is conducted to detect transactions which are unusual or suspicious compared to the customer's risk profile (expected versus real transactional behaviour).

This transaction monitoring is conducted on <u>two levels</u>:

1) each business line (first line of control) monitors all customers and their financial behaviour and applies an enhanced due diligence on those customers who are considered as a higher ML/TF risk;

2) the first line of control is supplemented by a risk-based second line of control, including an increased monitoring of transactions of customers regarded as a higher ML/TF risk.

A group-wide transaction monitoring founded on a risk-based approach has been defined to be followed by all entities using – as much as possible - the same transaction monitoring tool. Since rule-based monitoring tools have limitations when it comes to effectively set up thorough customer profiling, they are supplemented by AI-based monitoring models.

In a number of circumstances described in the group-wide KYC-rule, measures need to be taken to block the products or to terminate the business relationship.

6.4. Record keeping

Records of personal data obtained for the purposes of the prevention of money laundering and terrorist financing are processed and kept in accordance with the requirements from the EU General Data Protection Regulation (GDPR) and shall not be further processed in a way that is incompatible with those purposes.

7. ORGANISATION OF INTERNAL CONTROL

7.1. Suspicious Transactions Reporting (STR)

In each entity of the KBC Group that is subject to AML Law an AML Compliance Officer (AMLCO) is appointed to ensure that unusual transactions that have been detected are reported to the appropriate Financial Intelligence Unit (FIU). The reporting of suspicious transactions must comply with the laws and regulations of the respective local jurisdiction.

7.2. Procedures

All group entities have implemented AML/CTF rules, including minimum KYC standards, into operational procedures taking into account their type of activities, their volume and their size together with the local legal and regulatory requirements.

7.3. Training

All group entities develop a coherent training program, including follow-up trainings on a regular basis (in-class trainings, E-learnings, webinars), in order to create and maintain a satisfying AML/CTF awareness and knowledge. The content of this training program has been worked out in accordance with the kind of business the trainees are working for and the kind of functions they hold.

7.4. Compliance Monitoring Program

In order to assure the effectiveness of instructions, procedures and processes, recurrent quality controls are performed in the AML/CTF-domain pursuant to a Compliance Monitoring Program. Reviews and quality controls can be executed by the Group at its own initiative.

7.5. Reporting

AML/CTF issues and activity reports are submitted on a regular basis to the local Audit, Risk and Compliance Committees and to Group Compliance who reports to the Group Risk and Compliance Committee (at the consolidated level). On a yearly basis local Executive Committees or equivalent assess the quality of coverage of the internal control in this respect.

7.6. Corporate Audit

Compliance with the policy, the minimum KYC standards and the procedures encompassing local rules as the case may be falls within the scope of Corporate Audit who verifies if they are correctly implemented and obeyed.

8. EXCHANGE OF INFORMATION

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

- between financial and credit institutions belonging to KBC Group being established in EEA or FATF member- countries
- towards financial and credit institutions outside KBC Group as long as:
    - cases relate to the same customer and the same transaction,
    - these institutions are situated in EEA or FATF member-countries and
    - the info exchanged is exclusively used for the purpose of prevention of money laundering or terrorism financing.

The information shared amongst entities of the KBC Group is facilitated by the Group Compliance Function and is a.o. relating to the STRs that have been filed with the local FIU. Adequate safeguards on the confidentiality and the use of information exchanged is in place.