otpbanka

Anti-Money Laundering and Counter Terrorist Financing Policy

Content

1. INTRODUCTION

OTP Bank Plc (hereinafter: "Bank" or "Parent Bank"), as a member of the OTP Group and as the Parent Bank (the bank directly or indirectly controlling the subsidiaries) and OTP banka d.d. are committed to comply with the provisions on the prevention of domestic and international money laundering and terrorist financing and take into account the recommendations and guidelines issued in this regard.

In order to comply with AML/CFT requirements, the Banking Group develops internal policies and establishes effective processes, procedures and controls built into processes.
OTP Group applies a risk-based approach to its AML/CFT activities, handling higher money laundering or terrorist financing (ML/TF) risks with priority.

The soundness, integrity and stability of credit and financial institutions and confidence in the financial system as a whole could be seriously jeopardised by the efforts of criminals and their associates either to disguise the origin of criminal proceeds, or to channel legal or illegal money for terrorist purposes.

This Anti-Money Laundering and Counter-Terrorist Financing Policy represents an umbrella regulation implemented by the Bank and its employees for the purpose of detection and prevention of money laundering and terrorist financing. Each business segment has laid down detailed regulations for their respective areas.

The Bank has zero tolerance towards any breach of anti-money laundering and counter-terrorist financing (hereinafter referred to as: AML&CTF) regulations.

The Bank adheres to the applicable AML&CTF legislation, and has put in place adequate systems and procedures to fend off any attempt of using its business operations for the above-mentioned criminal offences.

The requirements indicated herein apply to all employees of the Bank, and to any third parties, including clients and business partners. All of the involved shall observe the fundamental principles of the Bank's operations, and any breach of this Policy and other applicable regulations shall be sanctioned.

The following regulations provide for the prevention of use of the financial systems for money laundering and terrorist financing activities:

- Anti-Money Laundering and Counter-Terrorist Financing Act (OG 108/17)
- Act Amending the Anti-Money Laundering and Counter-Terrorist Financing Act (OG 39/2019 and 151/2022)
- Act on International Restrictive Measures (OG 133/2023)
- Ordinances passed by the Finance Minister
- CNB Decisions and Guidelines
- EBA Guidelines
- Regulation (EU) 2015/847 of 20 May 2015 on information accompanying transfers of funds and repealing Regulation (EC) No 1781/2006
- Other EU Directives and Regulations
- Recommendations and standards of FATF
- Resolutions of the United Nations Security Council
- National and supranational risk assessment

2. PURPOSE

By virtue of their respective national legislation, EU directives, internal regulations and the best international practice, the members of OTP Group shall develop framework regulations and standard operational procedures that effectively promote the fight against money laundering and terrorist financing, thereby strengthening (preserving) the reputation of the Group.

3. MINIMUM REQUIREMENTS

In the areas listed below, OTP banka shall apply at least the following measures:

3.1. Money laundering and terrorist financing risk analysis

Pursuant to Article 12 of the AML&CTF Act, the Bank regularly assesses/analyses the money laundering and terrorist financing risks, taking into account its size, scope and complexity of its operations.

The methodology for conducting such risk analysis has been harmonised at the Group level, and it is based on the EBA guidelines and international practice.

Risk self-assessment includes the following main components:

- General information about the bank
- National and supranational risk assessment and criminal environment
- Findings of external, internal and supervisory audits for the previous period
- Inherent risks in accordance with the EBA guidelines
  - Threats
  - Weaknesses
- Assessment of residual risk and prescribing measures for its mitigation
- Action plan for the implementation of the prescribed measures

The observed risks always arise from the actual operations of the Bank and are related to customer risk, country or geographical risk, product and service risk, delivery channel risk, and modus operandi risks (e.g. cash operations, offshore, social engineering, tax fraud, virtual currencies, etc.).

The risk self-assessment, which shall be documented, shall be carried out once a year, at year-end, as well as at any time when there are significant changes in the business or in the relevant regulatory framework.

In addition, prior to any significant changes in the business processes and business practice that could affect the AML&CTF measures, and upon launching of a new product, outsourcing an activity or a delivery channel, and introducing new technologies for the existing or new products, the Bank shall assess the related risks to determine whether such changes affect the exposure to money laundering and terrorist financing, and shall take appropriate measures for managing and containing the identified risks.

At last but not least, the Bank shall analyse and assess the risks of all its customers, business relations and (occasional) transactions.

3.2. Customer due diligence

Customer due diligence measures shall be applied in the following instances:

a. a) when establishing a business relationship;
b. when carrying out occasional transactions amounting to EUR 10.000 or more, whether the transaction is carried out in a single operation or in several operations which appear to be linked;
c. when carrying out an occasional transaction that constitutes a transfer of funds exceeding EUR 1.000 within the meaning of Regulation (EU) 2015/847;
d. when there is a doubt about the veracity or adequacy of previously obtained customer identification data;
e. whenever there is a suspicion of money laundering or terrorist financing, regardless of any derogation, exemption or threshold.

Customer due diligence measures include customer identification and verification of the customer's identity based on the official personal documents, valid public documents and data obtained from reliable and independent sources, establishing the identity of the beneficial owner(s), obtaining information on the purpose and intended nature of the business relationship or transaction, and other information in line with legal regulations, and ongoing monitoring of the business relationship including, where necessary, obtaining information on the source of wealth and source of funds.

OTP banka d.d. applies all customer due diligence measures listed above, but the extent of such measures is based on risk assessment and may vary depending on the type of customer, business relationship, product or transaction.

For all the high risk customer categories, the Bank applies enhanced due diligence measures, including, but not limited to: gathering of additional information and documentation, additional control of publicly available information and information from other reliable sources, senior management approval prior to establishing a business relationship, introducing of additional controls, enhanced transaction monitoring, more frequent updating of the customer information and files, etc.

If the Bank is unable to implement the above mentioned due diligence measures, it **shall not** establish the business relationship or perform the transaction, and **it may** terminate an existing business relationship.

In addition, the Bank ensures that KYC data and documents related to the existing customer relationships are up-to-date.

3.3. Identification of beneficial owner(s)

Customer due diligence measures also include the identification of the beneficial owner, where the beneficial owner(s) of the customer shall be any natural person (persons) who ultimately owns the customer or controls the customer or in any other way manages it, and/or any natural person (persons) on whose behalf the transaction is being conducted, including a natural person (persons) who exercise ultimate effective control over a legal person or legal arrangement.

3.4. Identification of politically exposed persons (so called PEPs)

A politically exposed person shall be any natural person who acts or has acted during the at least previous 12 months at a prominent public function in a member state or a third country, including their immediate family members or persons known to be close associates of a politically exposed person.

As for transactions or business relations with the politically exposed persons, the minimum requirements in place at the level of OTP banka Group include:

a. procedures based on the risk assessment for the determination whether customer is a politically exposed person;
b. a written consent of the senior management for the establishment of a business relationship with politically exposed person;
c. adequate measures to establish the source of wealth and the source of funds that are involved in the business relationship or the transaction, and
d. enhanced, ongoing monitoring of the business relationship with a politically exposed person.

3.5. Enhanced due diligence

The Bank applies enhanced due diligence to all customers that entail high risk of money laundering or terrorist financing, which include seeking the information, documentation and data on top of the standard requirements, all in order to fully understand the business relationship that runs high risk, and to adequately manage the identified risk. To this end, additional consents (AML, Compliance, or even the Board of the Bank in certain cases) are necessary to establish such business relationships.

Enhanced due diligence shall be applied, inter alia, in the following cases: for non-residents, PEPs, customers from the high-risk third countries, customers connected to off-shore zones, customers with complex ownership structure, private banking customers, non-profit organisations, companies registered at the address of company service providers, and clients dealing with high-risk activities (for example: gambling, betting, arms and military equipment, precious metals, oil, construction and similar).

3.6. Reporting obligation

For the purpose of efficient combat against money laundering, the Bank has set up internal procedures and application support that ensure timely reporting of suspicious transactions to the competent authorities.

Being legally bound, the Bank has developed a system of monitoring any activity that, due to its nature, is regarded as particularly likely to be related to money laundering or terrorist financing, especially any complex or unusually large transactions and all unusual patterns of transactions which have no apparent economic or visible legal purpose. In the event they detect any information, fact or circumstance that may suggest money laundering or terrorist financing, OTP bank Group members shall, without delay, file a report to the competent authorities.

In line with the local legislation, mandatory reporting also includes all cash transactions equalling or exceeding EUR 10,000.

3.7. Customer and transaction screening

The Bank runs all payment system transactions against the sanction lists (UN, EU, OFAC, and UK) in real time. The sanction lists are updated on the system on daily basis.

In addition, the Bank carries out an overnight screening of the entire customer data base against the mentioned sanction lists, where such screening includes natural and legal persons, as well as all related persons (beneficial owners, authorised representatives, and so on).

In compliance with the legal provisions and common requirements of OTP Group, the Bank has implemented a software created by an experienced international software manufacturer in order to monitor unusual and suspicious transactions on the accounts of Bank's customers.

3.8. Application of a country-risk model

In accordance with the applicable legislation and the business requirements of OTP Group, in addition to the implementation of the automated transaction monitoring system that is based on the set parameters, the Bank applies a uniform country-risk rating model at all levels, thus filtering the suspicious transaction to or from the countries:

- whose anti-money laundering and counter-terrorist financing systems have been identified, by reliable sources, as inefficient;
- which have been identified, by reliable sources, as having significant level of corruption or other criminal offences;
- which are considered tax heavens;
- which are subject to international sanctions or international restrictive measures;
- which finance or support terrorist activities or have active terrorist organizations within their territory;

all in order to reduce the risks arising from such transactions.

3.9. Training

The OTP banka Group members shall take appropriate measures to ensure that the concerned employees are aware of the provisions in force relating to money laundering and terrorist financing, that they are able to recognize operations, business relationships and transactions which may be related to money laundering or terrorist financing, and to instruct them as to how to proceed in such cases when noticing information, facts or circumstances that may suggest money laundering or terrorist financing.

The concerned employees shall attend at least one training session per year.

3.10. Correspondent banking relations

In OTP Group, the minimum requirement for cross-border correspondent banking relationships are as follows:

a. to gather sufficient information about a respondent institution to understand fully the nature of the respondent's business and to determine, from publicly available information, the reputation of the institution and the quality of supervision;
b. to assess the respondent institution's anti-money laundering and anti-terrorist financing controls;
c. to obtain approval from a senior executive before establishing a new correspondent banking relationship;
d. to document the respective responsibilities of each institution;
e. with respect to payable-through accounts, be satisfied that the respondent credit institution has verified the identity of and performed ongoing due diligence on the customers having direct access to accounts of the correspondent and that it is able to provide relevant customer due diligence data to the correspondent institution, upon request.

At the level of OTP Group, establishment or maintenance of correspondent banking relations with shell banks is strictly forbidden, and group members shall take appropriate measures to ensure that no correspondent banking relation can be initiated or maintained with a bank known to allow the use of its accounts by any shell bank.

An additional minimum requirement concerning correspondent banking relations at OTP Group level includes screening of SWIFT transactions against UN, EU, OFAC and UK sanction lists.

3.11. Prohibitions and restrictions

The Bank shall not open, issue or keep anonymous accounts, passbooks to a code or a bearer, safe deposit boxes in anonymous names, or other anonymous products.

The Bank shall not establish or maintain correspondent relationships with shell banks, or with financial institutions that allow their accounts to be used by a shell bank.

The Bank shall not buy, sell or issue virtual currencies, or execute any orders for transfer of virtual currencies in its name and on its behalf, whereas a business relationship with a client carrying out those activities can be established solely subject to parent bank's approval.

The Bank shall not establish business relationship with, or perform a transaction for a natural person or legal entity named on the sanction lists.

4. DATA SAFEKEEPING AND PROTECTION

The Bank shall process all personal data collected pursuant to AML&CTF Act and the related secondary legislation solely for the purpose of preventing money laundering and terrorist financing, and they shall not be processed further for any other purpose.
Pursuant to AML&CTF Act, the Bank shall keep all data and documents collected for AML&CTF purposes for 10 years.

5. COOPERATION WITH AUTHORITIES

The Banking Group cooperates fully with national supervisory and investigative authorities and local financial intelligence units, providing the requested information in a timely manner. It fulfils its reporting and data provision obligations in accordance with the relevant requirements.

6. TRANSITIONAL AND FINAL PROVISIONS

This Policy is adopted by the Management Board, subject to consent of the Supervisory Board. The Policy shall take effect on the day of its publication on the Bank's web site.

The Anti-Money Laundering and Counter Terrorist Financing Policy adopted in 2022 shall be put out of force on the date this Policy becomes effective.

Done in Split on April 2024.

President of the Management Board
Balázs Békeffy