Information and Bank Security Division
AML Dept.

Version: 7
Approval date: December 14th 2021.

Anti-Money Laundering and Counter Terrorist Financing Policy

TABLE OF CONTENTS:

OTP banka d.d. (hereinafter referred to in: Bank) at Board meeting No._____, held on December 14th 2021. brought:

1 Introduction

AML Policy is main document, which together with other internal acts in this area, primarily the AMLFT Bylaw constitutes the normative AMLFT framework of the bank in which all activities and obligations in this area are explained in detail.

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 lawful or unlawful money for terrorist purposes.

Owing to several successful acquisition in recent years, OTP Bank Plc. Group (hereinafter: OTP Group[1]), is acting in nine countries in the region in addition to Hungary through its subsidiaries, thus developing into the leading bank group of the region.

OTP banka d.d. (hereinafter: the Bank) is a member of OTP Bank Plc. Group, but it is also the mother company of Croatian OTP Group (hereinafter: Group of OTP banka[2]).

The regulatory framework of the anti-money laundering and counter-terrorist financing area consists of:

- Anti-Money Laundering and Counter-Terrorist Financing Act (OG 108/17, OG 39/2019)
- Act on International Restrictive Measures (OG 139/2008, OG 41/2014, OG 63/2019)
- 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

Money laundering and terrorist financing often occurs across the boarders, therefore the effort to fight against it should also be a global action. It is especially true for a bank group like OTP Group, operating regionally.

The objective is to avoid that the members of OTP Group are being used for money laundering and terrorist financing.

[1] In terms of this Policy, ***OTP Group*** means the mother Bank - OTP Bank Plc., and its subsidiaries, as follows: OTP banka d.d., OTP Bank Romania S.A., DSK Bank AD, Banka OTP Albania SHA, JSC OTP Bank Ukraine, Joint Stock Company OTP Bank Russia, Crnogorska Komercijalna Banka AD, , Mobiasbanca – OTP Group S.A. Moldavia, OTP banka Srbija a.d. Novi Sad, and SKB banka d.d. Ljubljana.

[2] In terms of this Policy, ***Group of OTP banka*** beside the mother bank - OTP banka d.d., comprises its following subsidiaries: OTP Invest d.o.o., OTP Nekretnine d.o.o. and OTP Leasing d.d.

2 Scope

Members of the Group of OTP banka are committed to developing framework regulations and standard operational procedures in accordance with the EU directives and the international best practice, which effectively promote the fight against money laundering and terrorist financing, thereby increasing (preserving) the reputation of the bank group.

3 Minimum requirements

In the areas listed below members of the Group of OTP banka shall apply measures equivalent to at least the following ones:

3.1 Business-Wide Risk Assessment

Pursuant to Article 12 of the AML&CTF Act, the Bank regularly makes the enterprise-wide analysis of the money laundering and terrorist financing risks, proportionate to its size, scope and complexity of its operations.

The methodology for conducting 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
- Activity 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 Assessment must be performed and documented in writing at least once a year, and at any time when there are significant changes in the business or in the relevant regulatory framework.

OTP Group AML Unit makes the Group-wide BWRA, followed by the appropriate action, if necessary.

3.2 Customer due diligence

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

a) when establishing a business relationship;
b) when carrying out occasional transactions amounting to HRK 105.000 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;
- verifying the true 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;
- 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 requirements listed above, but the extent of such measures, considering the risk sensitivity, may vary depending on the type of customer, business relationship, product or transaction, including that it can be performed repeatedly for a customer who previously underwent customer due diligence.

For all the high risk customer categories, the Bank applies enhanced due diligence measures, including, but not limited to:

- requesting additional information and documentation;
- verifying all the collected information at publicly available sources and other reliable and independent sources;
- senior management approval prior to establishing a business relationship;
- additional controls;
- enhanced monitoring;
- more frequent review of customer files, etc.

If the Bank is unable to perform the legally prescribed due diligence measures, it must not establish the business relationship or perform the transaction, i.e. it can terminate the already existing business relationship.

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

3.3 Identification of beneficial owner(s)

Customer due diligence measures also include the identification of the beneficial owner. "Beneficial owner" is defined as the natural person(s) who ultimately owns or controls the customer, or exercises control over the customer by other means, and/or the natural person(s) on whose behalf a transaction or activity is being conducted.

3.4 Reporting obligation

Members of the Group of OTP banka shall pay special attention to any activity which they regard as particularly likely, by its nature, to be related to money laundering or terrorist financing and in particular complex or unusually large transactions and all unusual patterns of transactions which have no apparent economic or visible lawful purpose.

In the event of noticing any information, fact or circumstance that may suggest money laundering or terrorist financing, they shall, without delay, file a report to the competent authorities.

Mandatory reporting also relates to all cash transactions equalling or exceeding HRK 200.000.

3.5 Identification of politically exposed persons (PEP)

"Politically exposed persons" are defined as natural persons entrusted with prominent public functions currently or in the past 12 months, as well as their immediate family members, and persons known to be close associates of such a person.

In respect of transactions or business relationships with a politically exposed person, the minimum requirements within the Group of OTP banka are as follows:

a) to have appropriate risk-based procedures to determine whether the customer is a politically exposed person;
b) to have senior management approval for establishing the business relationship with such a customers;
c) to take adequate measures to establish the source of wealth and source of funds that are involved in the business relationship or transaction
d) to conduct enhanced ongoing monitoring of the business relationship.

3.6 Customer and transaction screening

Monitoring of suspicious bank transactions by rule-based automated screening system, as well as existence of automatically updated screening system containing the data of entities and persons included in international sanction lists (UN, EU, OFAC, and UK) are essential elements of fighting against money laundering and terrorist financing.

In compliance with the legal provisions and common requirements of OTP Group, the Bank has implemented systems of software manufacturers having significant experience on the international market, in order to monitor unusual or suspicious transactions and compare customer data with the international sanction lists.

3.7 Application of country-risk model

According to the legal regulations, and business requirements of OTP Group, in addition to the implementation of the rule-based automated transaction monitoring system, the Bank applies common country-risk rating model at all levels for filtration of suspicious transaction to or from 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.

3.8 Training

Members of the Group of OTP banka shall take appropriate measures to ensure that their relevant 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.

As a minimum requirement employees shall have training at least once a year.

3.9 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.

Within 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, UK and OFAC sanction lists.

3.10 Prohibitions and restrictions

The Bank does not open, issue or keep anonymous accounts, passbooks to a code or a bearer, or other anonymous products, including the accounts opened in false names which, directly or indirectly, allow a customer’s identity to be concealed.

The Bank does not establish or maintain correspondent relationships with shell banks, nor with financial institutions that allow its accounts to be used by a shell bank.

The Bank is not allowed to establish business relationship with, or perform a transaction for, a private person, legal entity or any other subject found on the sanction lists.

4 Data safekeeping and protection

All customer information collected pursuant to AML/CTF Act and the related legislation, is regarded as strictly confidential and may be processed exclusively for anti-money laundering and counter-terrorist financing purposes.

Pursuant to AML/CTF Act, the Bank is obliged to keep all data and documents collected for AMLCTF purposes for 10 years.

5 Transitional and final provisions

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

The Policy on prevention and combating of money laundering and terrorism financing of 29th May 2018, shall cease to have effect by virtue of the entry into force of this Policy.

Split, December 14th, 2021.

President of the Management Board

_____

Balázs Békeffy