**ANTI-MONEY LAUNDERING,**

**FINANCING OF TERRORIST ACTIVITIES AND**

**PROLIFERATION OF**

**WEAPONS OF MASS DESTRUCTION**

**COMPLIANCE POLICY**

April 2024

# PREAMBLE

As ZiraatBank BH d.d. our primary goal is to fully comply with applicable national and international laws and regulations and sanction regimes in order to prevent the products and services we offer to our customers from being used in activities related to money laundering, financing terrorist activities, financing the proliferation of weapons of mass destruction and other financial crimes.

In response to the international community’s growing concern about the problem of money laundering, potential terrorist financing and proliferation of weapons of mass destruction, Bosnia and Herzegovina established all necessary legal arrangements in accordance with the FATF's Recommendations and Directive of the European Parliament and the Council. It is the policy of ZiraatBank BH d.d. to prohibit and actively pursue the prevention of money laundering and any activity that facilitates money laundering and/or the terrorist activities funding and/or other criminal activities. The Bank is committed to AML/FTA/PWMD compliance in accordance with applicable law and requires its management and employees to adhere to these standards in preventing the use of its products and services for money laundering purposes. In compliance with its legal obligations, the Bank implemented its own AML program adopted by the Supervisory Board, with all of its strict internal regulations for the prevention, detection and reporting of unusual and suspicious transactions that may involve money laundering and financing of terrorist activities. AML/FTA/PWMD policy and practices are applicable to all business units of the Bank.

It is the policy of ZiraatBank BH d.d. to combat the laundering of the proceeds of crime and activities that facilitate it, as well as the financing of terrorist activities/the proliferation of weapons of mass destruction or other financial crime activities, and to pursue the prevention of these activities.

The Bank carries out its activities in accordance with the laws in force and international standards, in particular with the Law on prevention of money laundering and financing terrorist activities ("Official Gazette of the Federation of Bosnia and Herzegovina", No. 13/24).

In order to ensure and maintain compliance with legal regulations and international standards the Bank reviews the policy once a year.

## Purpose

Purpose of this policy:

* Preventing the use of our products and services in laundering of the proceeds of crime and the financing of terrorist activities, as well as the financing of the proliferation of weapons of mass destruction,
* Forbidding the activities that facilitate ML/FTA/PWMD and other financial crime activities,
* Ensuring that each personnel of the Bank is knowledgeable on the rules regulating the combat the laundering of the proceeds of crime, financing of terrorist activities, and is conscious about and responsible of abiding by these rules,
* Ensuring that the customers, transactions, products and services are assessed with a risk-based approach, and that the necessary actions are taken with regards to identifying and mitigating the reputational, operational, legal, and concentration risks Ziraat Bank BH d.d. may face in this regard,
* Complying with international sanction regimes, and preventing Bank from intermediating in transactions that may result in any sanction,
* Protecting the interest, reputation, and customer quality of the group,
* Conducting secure banking activities,
* Identifying the operation and rules in this field and defining roles and responsibilities,
* Establishing the principles and standards, that Bank must abide by.

## Scope and Legal Framework

This policy covers all branches of ZiraatBank BH d.d.

Law on prevention of money laundering and financing terrorist activities ("Official Gazette of the Federation of Bosnia and Herzegovina", No. 13/24), and the regulations and communiqués published regarding these laws constitute the legal basis of our Bank's AML/FTA/PWMD policy. This policy includes policies regarding risk management, monitoring and control, training, internal audit and information sharing.

## Roles and Responsibilities

All units and employees at every level apply principles mentioned in this policy. They avoid carrying out transactions and activities that can be associated to laundering of the proceeds of crime, financing of terrorist activities/the proliferation of WMD, or facilitating these actions. For this purpose, duties and responsibilities are fulfilled with necessary attention and care.

While the Compliance Department is responsible for the implementation of our Bank's AML/FTA/PWMD policy; The Board of Directors is ultimately responsible for ensuring that our Bank's obligations under the Law on prevention of money laundering and financing terrorist activities ("Official Gazette of the Federation of Bosnia and Herzegovina", No. 13/24) are fulfilled.

Compliance Department conduct activities regarding risk management, suspicious transaction reporting, monitoring and control within the scope of the compliance program included in the policy, while our Internal Audit Unit conducts internal audit activities.

# AML Compliance Function

The Compliance Department has the authority to request all kinds of information and documents related to their field of duty from all units within the Bank and to access them in a timely manner, in order to make a decision with an independent will. The Compliance Department act in accordance with the confidentiality principles stipulated in the relevant laws and regulations while carrying out their activities in accordance with the written policies and procedures. While carrying out their activities, they act in accordance with the confidentiality principles stipulated in the relevant laws and regulations.

## Risk Management Policy

Bank's risk management policy includes activities to define, rate, monitor and mitigate the risks that the bank may be exposed to in relation to the financing of the ML/FTA or proliferation of weapons of mass destruction.

The risk management policy includes, at a minimum, internal precautions and operating rules regarding know your customer principles. Activities regarding risk management include those about the identification of the customer and real beneficiary, conducting necessary controls for customer due diligence (CDD), and taking the risk-mitigating measures that are compatible with the risk levels after the risk assessment is conducted according to determined risk factors.

## Know Your Customer Principles

The most effective way to protect Bank from those desiring to use it as an intermediary for the acts of money laundering, financing of terrorist activities and other financial crimes is to know our customers, to establish our policies and procedures within the scope of “Know Your Customer” in line with legal legislation, and fully comply with them. This process includes the steps of obtaining information about new and existing customers, identification, and verification.

## Customer Acceptance Policy

Within the framework of the "Know Your Customer" principle at our Bank, it is essential to identify customers and persons acting on behalf of customers, and to implement the necessary controls and take measures to reveal the real beneficiary of the transaction.

Within this scope, a customer acceptance policy was formed in order to conduct CDD that is compatible with the customer’s risk profile, and to determine the customers that bear high risk related to AML/FTA/PWMD and those who will not be provided products/services by the Bank.

Obtaining adequate information in regards to the following is important in forming an open and trust-based bank-customer relationship:

* Identification and verification of customer/beneficial owner,
* Consistency of documents and information,
* Customer’s job, main field of profession that creates revenue,
* Customer’s financial profile,
* Work or business place.

## **Persons and Entities That Cannot to Be Accepted as** **Customers**

In order for a natural or legal person to be accepted as a customer, they must meet the criteria determined in accordance with this policy. In this context, the following are not accepted as customers and business relationships are not established with them:

* Persons and entities whose real identity and addresses cannot be determined and verified,
* Those who want to open an account under a different name,
* Those providing misleading information regarding their identities or are reluctant to provide any information,
* Those detected, as a result of detailed research, to have provided inconsistent or inaccurate information before,
* When the real beneficiary cannot be identified,
* When information about the nature and purpose of the business cannot be obtained,
* When adequate information cannot be obtained to comply with this policy,
* When there are persons whose funds are determined to be the proceeds of an illegal activity,
* Persons and entities mentioned in the sanctioned lists published by official institutions and in the lists monitored by the Bank,
* Shell banks and shell companies.

## Circumstances Requiring Rejection of Transaction and Termination of the Business Relationship

In establishing a continuous business relationship, information is obtained about the purpose and nature of the business relationship. Business relationships with customers who are detected to have used their accounts for the purposes of money laundering and the financing of terrorist activities are terminated. Ziraat Bank does not establish business relationships and does not perform the requested transaction in cases where they cannot identify or obtain sufficient information about the purpose of the business relationship.

The business relationship is terminated if the required identification and verification cannot be made as there is a suspicion regarding the adequacy and accuracy of the previously obtained customer identification information.

Business relationships are terminated with customers who are added on the sanction lists following the establishing an account relationship. If the customers monitored through the automatic filtering program do not provide adequate information and documents regarding the transaction they want to perform, the requested transaction is not conducted and the termination of the business relationship is taken into consideration.

Compliance Department also evaluate whether the issues stated below constitute suspicious transaction and the termination of the business relationship with the customer taken into consideration:

* when information about the source of the funds deposited into the customer account cannot be obtained,
* when individual accounts are detected to have been used for commercial purposes,
* when real beneficiary of the transaction and beneficial owner of the customer cannot be determined,
* high-risk products/services are intensely used or transactions incompatible with the customer profile are performed.

## Customer Due Diligence (CDD)

CDD includes the processes below:

* Identification of the customer and the beneficial owner,
* Verification of the customer identity based on reliable and independent information, data or documents to the extent required by the relevant legal regulations,
* Understanding of the purpose and nature of the business relationship, and applying enhanced measures in high risk situations,
* Screening the customers for the possibility of being on the sanction lists,
* Monitoring the transactions within the scope of continuous business relationship.

## Obligation of Identification

It is essential to determine the identity of the account holder, persons acting on behalf of the account owner, the real beneficiary of the transaction, and those authorized to represent, as well as the identity of shareholders and control structure of legal entity. Identities are verified before the establishment of a business relationship or the completion of the transaction.

## Correspondent Relationship

While establishing correspondent relationships:

* Reliable information is obtained from public sources on whether the relevant financial institution was subjected to an investigation regarding money laundering or terrorist financing and received punishment or warning, the nature, subject, and reputation of the business, and the audit adequacy upon it,
* System of the relevant financial institution on combating money laundering or terrorist activities financing is evaluated, it is made sure that the system is appropriate and effective,
* Senior executive approval is received before a new correspondent relationship is formed,
* The Bank does not enter into a correspondent relationship with sign banks and financial institutions that it cannot be sure not to have their accounts used by sign banks.

## Identity Verification

Identity verification process includes the verification of customer identity and address. During the identity verification process, information received for identification purposes is verified, and identities and addresses of the person and persons acting on behalf of the customer are determined and verified.

No business relationship is established or a transaction is conducted until the identity of the customer is determined and verified.

Verification of the legal entity's title, trade registry number, field of activity and address, documents pertaining to registration in the trade registry; verification of the tax identification number is made through the documents issued by the relevant administration.

With regards to the accuracy of the person authorized to represent the legal person, identity documents provided for the identification of real person, as well as documents regarding the registration issued or approved by the official institution authorized to keep records of the companies in the relevant country are used. Signatures are verified via the signature declaration prepared by the notary in the relevant country. In order for them to be provided when demanded by the authorities, original or notary-approved copies of the confirmed identity documents are submitted, than copied or saved as electronic image, or identity information is recorded.

In case there is suspicion regarding the authenticity of the documents used for the purpose of verifying the information obtained from the customers within the scope of identification, the authenticity of the document is verified, to the extent possible, by applying to the person or institution that issued the document or other competent authorities.

## Monitoring the Customer Status and Transactions

Branches constantly monitor, within the scope of continuous business relationship, whether the transactions conducted by their customers are compatible with the information regarding their profession, commercial activities, business history, financial status, risk profile, and fund sources, and keep the information, documents, and records about their customers up to date. Moreover, with regards to customer identification, the accuracy of the phone number, fax number, and e-mail address is verified by using these tools, when necessary, to contact with the relevant person within the framework of the risk-based approach. In case a transaction incompatible with the purpose of the establishing the business relationship and customer profile, about which information is provided by the customer during the customer acceptance process, the business relationship is reevaluated.

## Risk Management Activities

Activities regarding risk management are comprised of the following at the minimum level:

* Developing the risk identification, rating, classification, and evaluation methods based on customer, product, sector and geography risk,
* Rating and classification of services, transactions, and customers according to risks,
* Ensuring that the clients, transactions or services are monitored and controlled, reported to the relevant units, and developing appropriate operation and control rules in order for the execution of the transaction with the approval of the higher authority and its supervision when necessary,
* Retrospectively inquiring the consistency and effectiveness of risk identification and assessment methods through case studies or realized transactions, re-evaluating and updating them according to the results and developing conditions,
* Conducting the necessary improvements by following the national legislation, and the recommendations, principles, standards, and guides of international institutions on issues within the scope of risk,
* Reporting the risk monitoring and assessment results regularly to the Board of Directors,
* Taking additional measures for high-risk groups.

## Training

The purpose of Bank’s AML/FTA/PWMD training policy is to ensure that Bank complies with the obligations imposed by the Law and other regulations enacted in accordance with the Law-related, to create a corporate culture and update the knowledge of the personnel by increasing the awareness of responsibility in the matters of corporate policy and procedures and risk-based approach.

Training activities are conducted under the supervision and coordination of the Compliance Department. It is essential for the training activities to be conducted within the scope of the annual training program prepared in a way to include the following subjects.

All personnel in the bank are provided with training on the prevention of laundering proceeds of crime and financing of terrorist activities. Priority is given to the training of personnel who are in direct contact with the customer. It is essential to provide training to newly recruited personnel during the orientation process. It is ensured that the Compliance Department personnel and training staff participate in domestic/international training, seminars and certification programs on this subject for the purpose of professional specialization. Trainings are organized using in-class, on-the-job and distance education methods.

## Internal Audit

The efectiveness and adequacy of the whole Compliance Program of the Bank is audited by the Internal Audit, External Audit (independent audit company), T.C. Ziraat Bankası A.S. audit and the authorized controllers of the Banking Agency of the Federation of Bosnia and Herzegovina.

## **Sanction Policy**

Ziraat Bank BH d.d., together with financial institutions within Ziraat Finance Group, conduct their operations in compliance with national legislation and international standards which govern the Bank’s international operations. Ziraat Bank follow the international sanction programs, especially those of United Nations Security Council, and takes the necessary measures to comply with them. Bank shall not provide any service to countries and activities subject to sanctions, and shall not mediate any banking services that violate the sanctions.

Bank shall not enter into business relationships with persons and organizations that are listed in the sanction lists, shall not conduct transactions requested or ordered by these persons and organizations, shall not mediate the transactions which directly or indirectly involve such persons and organizations. The Bank shall not open accounts for customers who are included in United Nations Security Council and other sanctions lists followed.