

PROTECTION AGAINST MONEY LAUNDERING

1. As part of our commitment to financial security and regulatory compliance, PKO Bank Polski S.A. (hereinafter "the Bank") strictly adheres to Anti-Money Laundering (AML) and counter-terrorist financing (CTF) regulations in both Poland and Romania. Our AML framework is designed to prevent, detect, and report suspicious activities related to money laundering (ML) and terrorist financing (TF).
2. Our Bank complies with:
 - i. Romanian AML Laws (the primary legislation establishing the Bank's obligations regarding ML and TF is outlined in Law no. 129/2019 for preventing and combating money laundering and terrorist financing, as subsequently amended and supplemented).
 - ii. Polish AML Laws – Based on the EU's Anti-Money Laundering Directive (AMLD) and local regulations.
 - iii. EU Regulations – Ensuring compliance with European financial security standards.
3. In accordance with national and international legislation, the Bank performs the following activities:
 - a) Customer identification and verification based on Know Your Customer (KYC) policies,
 - b) The identification of the Ultimate Beneficial Owner (UBO) and taking adequate measures to verify the UBO's identity,
 - c) Obtaining information on the purpose and intended nature of the transaction or of the business relationship,
 - d) Verification of whether the Customer or the Customer's UBO is a publicly exposed person (PEP) or a sanctioned individual,
 - e) The determination of the origin of funds or property used in the transaction or business relationship, depending on the risk of money laundering or terrorist financing,
 - f) Verifying whether the Customer is acting on their own behalf,
 - g) Ongoing monitoring of the business relationship, including the review of particular transactions carried out throughout the duration of the business relationship,
 - h) The collection and the review of the official documents (ID, company registration, Ultimate Beneficial Owner details, etc.),
 - i) Updating the Customer's documents, data or information available to the Bank.
4. The Bank has the legal obligation to keep the following records:
 - i. Customer's identification data, contact details and any other documents received by the Bank from the Customer – for at least 5 years from the moment of the termination of the business relationship;
 - ii. All financial data and documents related to a transaction – for at least 5 years from the moment of carrying out a transaction;
 - iii. Information about UBOs – for at least 5 years from the moment of the termination of the business relationship.
5. The Bank processes and collects Customer's personal data in order to fulfill its legal obligations related to AML and CTF regulations, particularly for the following, but not limited to:
 - 1) Customer identification and verification – to ensure compliance with laws regarding AML/CTF;
 - 2) Monitoring of financial behavior and transactions – to detect unusual or suspicious activities, as part of the Bank's efforts to prevent ML/TF;
 - 3) Reporting suspicious transactions – to apply KYC measures, including the use of the Customer's collected data for reporting transactions to the relevant authorities.
 - 4) Complying with other applicable requirements and regulations in the field.
6. The Bank reserves the right to restrict the Customer or any authorized representative from executing transactions and to freeze/block funds in the account in the cases provided by the legislation in force.
7. To fulfill its obligations under the legislation, the Bank may require the Customer to provide additional documentation or explanations necessary for executing the transaction.
8. The Bank reserves the right to refuse to execute a transaction to countries, entities or individuals subject to national or international sanctions or embargoes, in particular the sanctions implemented by the European Union, the United States of America or the United Nations in connection with the execution of duties, based on anti-money laundering and terrorist financing regulations or sanctions policies.
9. The Bank identifies and assesses the risk of ML/TF associated with a business relationship or occasional transaction. The Bank has implemented an internal ML/TF risk assessment system, which examines, in particular, factors related to: type of Customer, geographical area, type of products, services and methods of their distribution, level of assets deposited by the Customer or value of transactions performed, objective, regularity or duration of business relationship, and the Customer's behavior.
10. The Bank applies appropriate technical and organizational measures to ensure the confidentiality, integrity and availability of the Customer's personal data.
11. This Information Notice may be updated periodically to reflect changes in legal or regulatory requirements. In the event of significant changes, the Bank will notify Customers accordingly.