



AML & CTF Policy

JEWELPAY OÜ Anti-Money Laundering (AML) and Counter Terrorist Financing (CTF) Policy

General Provisions

Anti-Money Laundering and Counter Terrorist Financing Policy (the “AML&CTF Policy”) of JEWELPAY OÜ (the “Company”) is not to enter into business relationship with criminals or terrorists, process transactions which result from criminal or terrorist activity or facilitate any transactions involving criminal or terrorist activity including terrorist financing.

The Company will establish and implement adequate and appropriate anti-money laundering (AML) and counter terrorist financing (CFT) policies, procedures and controls taking into account factors including types of customers, products and services offered, delivery channels and geographical locations involved.

Senior management, officers and employees of the Company shall at all times make every effort to maintain the highest standards of ethics, integrity, and prudence in the Company’s operation and administration so as to ensure that the Company creates and maintains a good reputation and standing.

Compliance Function

The Company has appointed a dedicated Compliance Officer to oversight the Compliance Function and who will be responsible for ensuring the Company’s compliance with all regulatory requirements and internal policies.

The Compliance Officer will oversight all activities related to the prevention and detection of ML/TF and provide support and guidance to the senior management to ensure that ML/TF risks are adequately managed and mitigated.

The Compliance Officer will also act as a central reference point for reporting suspicious or unusual transactions/activity to the Financial Intelligence Unit.

Risk Identification and Assessment

The Company will apply a risk-based approach to assess which customers represent higher ML/TF risks.

Enhanced due diligence measures shall be applied to identify and verify customers that represent higher ML/TF risks.

Due Diligence Measures

The Company will determine and take due diligence measures appropriate to identify and verify its customers when opening accounts or establishing business relationship.

The Company will adopt a risk-based approach to utilize appropriate controls and oversight and to determine the extent of due diligence to be performed and the level of ongoing monitoring to be applied, accordingly.

The Company will monitor the business relationship with its customers on an ongoing basis.

The Company will not open an account or establish a business relationship with a customer if the customer fails to provide all documents and information required in the course of conducting due diligence, or if based on due diligence documents provided, the Company suspects ML or TF.

The Company will not open or maintain anonymous accounts or accounts in fictitious names for any new or existing customers.

The Company will not open or maintain accounts in the names of customers who are subject to the International Sanctions.

The Company shall not establish any relationship with shell banks or other institutions that knowingly allow shell banks use their accounts.

Record Keeping

The Company shall ensure that customers' data are registered in the Company's customer database within the required scope.

The Company shall keep the documents obtained in the course of identifying and verifying the identity of the customer and maintain the documents obtained in connection with the transactions performed for at least five (5) years following the termination of the business relationship with the customer.

Training

The Company shall ensure that all Company's employees and representatives who are dealing with customers, customers' transactions or matters involving money laundering and/or terrorist financing are provided with regular training and information about the nature of the money laundering and terrorist financing risks, as well as any new trends within the field.

The Company will provide training to all relevant staff (including new staff) in order to ensure they will be able to recognize suspicious or unusual activities/transactions.

The Compliance Officer is responsible to arrange regular training concerning prevention of money laundering and/or terrorist financing to explain the respective requirements and obligations.

Suspicious Transactions and Reporting

The Company has the obligation to notify the FIU in case of any suspicious or unusual transactions/activity on the customer's account.

The Company will give sufficient guidance to all relevant staff to enable them to take appropriate actions when detecting suspicious or unusual transactions/activity and to report the suspicious or unusual activities/transactions to the compliance Officer as soon as possible.

Internal Monitoring System

The Company will carry out regular assessments of the adequacy of its systems and controls to ensure the ML/TF risks are managed effectively and that internal policies and controls are compliant with applicable AML/CFT laws and regulations.

Regular Review

This AML&CFT Policy will be regularly reviewed and updated if necessary to ensure appropriate policies, procedures and internal controls are in place to account for both changes in the regulatory environment as well as the changes in business .