

Anti-Money Laundering (AML) Policy

Effective Date: 14.05.2025

1. Policy Overview

Olympus Holdings N.V. ("Olympus" or "the Company"), operating the website www.fireslots.bet is firmly committed to preventing any form of money laundering, terrorism financing, or illicit financial activities across its operations.

The purpose of this policy is to establish a framework to detect, deter, and report suspicious activities in accordance with the requirements of the Curacao Gaming Control Board (GCB), the Financial Action Task Force (FATF) guidelines, and other applicable anti-money laundering (AML) regulations.

2. Legal Framework

The AML Policy complies with:

- Curaçao National Ordinance on the Reporting of Unusual Transactions (NORUT)
- Curaçao Sanctions Ordinance
- Curaçao National Ordinance for Games of Chance (LOK) and its implementing directives
- FATF (Financial Action Task Force) Recommendations
- Curaçao Gaming Control Board (GCB) guidelines

3. Risk-Based Approach

Olympus shall apply a **risk-based approach (RBA)**, categorising customers into **low, medium, or high risk** based on:

- Customer profile
- Country of residence (especially high-risk jurisdictions as per FATF)
- Nature of transactions
- Source of funds

Enhanced due diligence (EDD) measures will be applied for high-risk customers, Politically Exposed Persons (PEPs), or suspicious transactions.

4. Customer Due Diligence (CDD)

Before establishing a business relationship, Olympus shall:

- Verify the identity of customers through reliable and independent documents (government-issued ID, utility bills, etc.).
- Obtain information about the purpose and intended nature of the business relationship.
- Screen customers against global sanction and PEP lists.
- Refuse anonymous or fictitious account openings.

Olympus applies sanctions screening to all customers, affiliates, vendors, and third-party service providers against global lists including the UN, EU, OFAC, and other relevant local lists, using [screening tool name or internal system]. Screening occurs at onboarding and on an ongoing basis.

Verification Requirements:

- Full name
- Date of birth
- Nationality
- Residential address
- Valid government-issued identification

Ongoing Monitoring:

- Transactions will be monitored continuously to detect suspicious patterns.
- Customer profiles and risk assessments will be updated regularly.

5. Politically Exposed Persons (PEPs)

Enhanced Due Diligence (EDD) must be applied when onboarding PEPs, including obtaining:

- Senior management approval
- Source of wealth and source of funds information
- Enhanced ongoing monitoring of the business relationship

6. Suspicious Transaction Monitoring and Reporting

All employees will be alert to any suspicious transactions, including:

- Unusually large or complex transactions
- Transactions with no apparent legitimate purpose
- Discrepancies in documentation or customer behaviour

All suspicious activities will be immediately reported to the MLRO, who will:

- Review the suspicion.
- Document findings.
- Report to the Financial Intelligence Unit (FIU) of Curacao, if necessary.

7. Record-Keeping

Olympus shall retain the following records for a minimum of **five (5) years**:

- Customer identification documents
- Business correspondence
- Transaction history
- Suspicious transaction reports

8. Payment Methods and Restrictions

Olympus only accepts deposits and processes withdrawals through:

- Verified bank accounts
- Approved credit/debit cards
- Reputable e-wallet providers

Strict limits and transaction monitoring will be applied to:

- Rapid deposit and withdrawal cycles
- Multiple payment instruments linked to the same customer

9. High-Risk Jurisdictions

Olympus does **NOT** onboard customers from jurisdictions identified by the FATF as high-risk and non-cooperative.

Prohibited jurisdictions include, but are not limited to:

- Iran
- North Korea
- Myanmar
- Syria
- Yemen

The country risk list will be reviewed at least quarterly.

10. Cooperation with Authorities

Olympus fully cooperates with law enforcement, regulators, and FIUs to support investigations and enforcement activities related to money laundering or terrorism financing.

11. Sanctions for Non-Compliance

Failure by any employee to comply with this AML Policy may lead to:

- Disciplinary action (up to and including termination)
- Reporting to regulatory authorities
- Civil and/or criminal penalties