

Anti-Money Laundering (AML) Program Olympus Holdings N.V.

Effective Date: [Date]

1. Introduction

Olympus Holdings N.V. ("Olympus"), operating www.casinoempire.com, is committed to the highest standards of anti-money laundering (AML), counter-terrorism financing (CTF), and sanctions compliance. This AML Program describes the company's internal policies, procedures, and controls to prevent the use of its services for money laundering and terrorist financing activities.

2. Legal Framework

This AML programme is developed in compliance with:

- Curaçao National Ordinance on Offshore Games of Hazard (NOOGH)
- Curaçao National Ordinance for Games of Chance (LOK) and its implementing directives
- Financial Action Task Force (FATF) Recommendations
- Applicable Curaçao Gaming Control Board (GCB) regulations
- Global standards on anti-money laundering and countering financing of terrorism

3. Governance Structure

- **Board of Directors:** Ultimate responsibility for AML compliance.
- **Compliance Officer/MLRO:** Ms. Marwa Tarek Korayem is designated as Compliance Officer and MLRO, responsible for implementing and overseeing the AML Programme.
- **Employees:** All employees are individually responsible for complying with the AML Programme.

4. Risk Assessment

Olympus maintains a risk-based AML framework including:

- Country/Geographical Risks

- Customer Risks
- Product/Service Risks
- Transaction Risks
- Delivery Channel Risks

Risk assessments are reviewed annually or upon material changes in business activities.

5. Customer Due Diligence (CDD)

To strengthen AML controls across its affiliate network, Olympus Holdings N.V. implements the following measures:

5.1. Standard CDD Procedures:

- Collect full name, date of birth, nationality, residential address, and valid ID.
- Verify identification documents against trusted sources.
- Screen customers against global PEP, sanctions, and adverse media lists.

5.2. Enhanced Due Diligence (EDD): Applied for:

- Politically Exposed Persons (PEPs)
- High-risk jurisdictions
- Unusually large transactions
- Complex or opaque ownership structures

EDD measures include:

- Senior management approval
- Source of funds and wealth verification
- More frequent ongoing monitoring

Initial Due Diligence:

- Conduct KYC/KYB checks on affiliate businesses, including beneficial ownership verification
- Review business model, marketing channels, and geographic focus

- **Ongoing Monitoring and Re-KYC:**
 - Perform re-KYC on affiliates every 12 months or upon significant change
 - Review affiliate-provided customer data and performance reports
- **Source-of-Traffic Monitoring:**
 - Use automated systems to monitor affiliate traffic for:
 - Geolocation mismatches
 - Use of VPNs, proxies, or anonymizers
 - Traffic spikes from restricted or blacklisted jurisdictions
- **Contractual Requirements:**
 - Require affiliates to include AML and geoblocking obligations in contracts
 - Reserve the right to terminate agreements for AML or compliance breaches
- **Audit Rights:**
 - Olympus retains the right to audit affiliates and their traffic sources periodically

5.3. Simplified Due Diligence (SDD): Considered only for very low-risk scenarios and subject to regulatory approval.

All customers, affiliates, vendors, and third-party service providers are screened against global sanctions lists including the UN, EU, OFAC, and local sanctions regimes using [screening tool name or internal system]. Screening is conducted at onboarding and continuously updated.

Crypto Onboarding and Transaction Monitoring Policy

If Olympus Holdings N.V. begins accepting cryptocurrencies, the following controls will apply:

- **Wallet Verification:**
 - Match customer identity to registered crypto wallet
 - Verify wallet ownership through signed message or third-party validation
- **Source of Funds/Wealth Checks:**
 - Obtain documentation of crypto source (e.g., mining records, trading history)
 - Conduct blockchain analytics to review wallet activity and provenance
- **Blockchain Analysis:**
 - Screen wallet addresses using third-party blockchain analytics tools (e.g., Chainalysis, Elliptic) to detect links to darknet markets, ransomware, or sanctioned entities

- **Transaction Monitoring:**
 - Monitor crypto deposits and withdrawals $\geq$ €2,000
 - Apply real-time alerting for unusual patterns, such as rapid in-and-out flows
- **Record-Keeping and Reporting:**
 - Maintain complete records of crypto KYC, risk scoring, transaction history, and alerts
 - Report suspicious crypto transactions to the Financial Intelligence Unit (FIU) in accordance with Curaçao regulatory requirements

6. Ongoing Monitoring

- Continuous monitoring of customer activity and transactions.
- Review of patterns inconsistent with the known profile.
- Automated alerts for suspicious behaviours such as rapid deposit-withdrawal cycles.

7. Suspicious Activity Reporting (SAR)

Employees must immediately report suspicious activities to the MLRO. The MLRO shall:

- Investigate internally.
- Document findings in a secure log.
- File Suspicious Transaction Reports (STRs) to the Curacao Financial Intelligence Unit (FIU) if necessary.

Examples of reportable suspicious activities:

- Attempts to deposit/withdraw large sums without clear economic purpose
- Structured transactions to avoid reporting thresholds
- Refusal to provide requested documentation

8. Record-Keeping

Records must be kept for a minimum of **five (5) years** from the date of:

- Customer due diligence completion

- Transaction execution
- Suspicious transaction report filing

Records include:

- CDD documentation
- Correspondence and communication logs
- Transaction records
- Internal investigation notes

9. Training and Awareness

- Annual mandatory AML/CTF training for all employees.
- Specialised training for customer-facing roles.
- New employees must complete AML training before interacting with customers.

Training topics include:

- AML laws and regulations
- Identification of suspicious activities
- Reporting mechanisms
- Customer onboarding procedures

10. Third-Party Relationships

- Thorough due diligence is performed on affiliates, payment processors, and any outsourced service providers.
- Outsourced partners must contractually adhere to Olympus' AML standards.
- Regular audits and risk assessments of third-party providers.

Affiliates are required to complete initial KYC verification and periodic re-verification (re-KYC) at minimum every 12 months. Olympus monitors affiliate traffic sources to identify potential exposure to prohibited jurisdictions or VPN/proxy use and requires contractual compliance with Olympus' AML standards.

11. Payment Methods

Accepted payment channels are limited to:

- Verified bank transfers
- Credit/Debit cards from reputable issuers
- Approved e-wallets and payment service providers

Payments are monitored for consistency with customer profiles. No anonymous or prepaid card deposits are allowed unless traceable.

12. High-Risk Jurisdictions

Olympus does not onboard customers from FATF-identified high-risk and non-cooperative jurisdictions. Clients from other higher-risk jurisdictions may only be onboarded after enhanced review and with senior management approval.

13. Independent Audit

- Annual independent review of the AML programme.
- The scope includes testing internal controls, transaction monitoring systems, and compliance with legal requirements.
- Findings are reported to the Board of Directors and the MLRO.

14. Data Protection and Confidentiality

- Customer information is collected and retained securely in accordance with privacy laws.
- Disclosure of information is only made to authorised personnel or regulatory bodies.
- Encryption and cybersecurity measures protect sensitive customer data.

15. Policy Violations and Sanctions

Non-compliance with the AML Program may result in:

- Disciplinary action, including termination of employment
- Regulatory reporting

- Civil or criminal penalties

16. Program Review and Updates

This AML programme will be reviewed and updated:

- Annually
- Upon major changes in business operations
- In response to regulatory changes

Changes must be approved by the Board of Directors and communicated to all staff.

17. Technical Annex: Risk Ratings and System Alerts

Olympus Holdings N.V. has implemented an automated monitoring system that maps identified risk categories to system-generated alerts and thresholds. This ensures timely detection, escalation, and resolution of potentially suspicious activities.

Risk Category Mapping and Alerts:

- High-risk country of residence → automatic onboarding rejection
- Politically Exposed Person (PEP) → MLRO notification and enhanced monitoring
- Large single deposit or withdrawal (> €10,000) → automated alert to compliance team, manual review
- Rapid deposit-withdrawal cycles (≥ 3 cycles within 24 hours) → automated transaction freeze pending review
- Multiple accounts using same payment method → automatic block and fraud team investigation

Threshold Management:

- Standard accounts: transaction alerts triggered at €5,000
- High-risk profiles: transaction alerts triggered at €2,500
- Crypto transactions: alerts triggered at €2,000 or above
- 24/7 automated monitoring with manual review for high-level alerts

Alert Severity Levels:

- Low → automated warning, periodic review
- Medium → compliance team review within 24 hours
- High → immediate MLRO escalation, possible account suspension

Governance:

- Compliance Officer reviews system rules quarterly
- Technical team conducts testing and updates under compliance oversight

18. Sanctions Screening — Scope, Sources, and Systems

Olympus Holdings N.V. ensures robust and comprehensive sanctions compliance through a multilayered screening program covering all relevant relationships and transactions across its operations.

Scope of Screening:

Olympus applies sanctions screening to all entities and individuals interacting with its services, including:

- Customers (retail, VIPs, high-net-worth individuals)
- Affiliates, marketing partners, and third-party introducers
- Vendors, suppliers, and contractors
- Payment processors, wallet providers, and banks
- Shareholders, directors, and senior management

This screening occurs at onboarding, at periodic intervals, and during the lifecycle of the business relationship.

Sources of Sanctions Data:

Olympus screens against a wide range of international and national sanctions lists, including but not limited to:

- United Nations (UN) Consolidated Sanctions List
- European Union (EU) Consolidated Financial Sanctions List
- United States Office of Foreign Assets Control (OFAC) Specially Designated Nationals (SDN) and Sectoral Sanctions Identifications (SSI) Lists
- United Kingdom Office of Financial Sanctions Implementation (OFSI) List
- Financial Action Task Force (FATF) list of high-risk and non-cooperative jurisdictions
- National watchlists from key operational regions (e.g., Curaçao National Ordinance for Games of Chance (LOK) and its implementing directives)
- Local Curacao Financial Intelligence Unit guidance and watchlists

Systems and Tools Used:

Olympus uses a combination of automated systems and manual processes to ensure effective sanctions screening:

- Deployment of a commercial screening solution (e.g., Sumsub)
- Integration of sanctions screening into the core customer onboarding platform
- Daily automated batch screening of the entire customer, affiliate, and vendor database against updated sanctions lists
- Real-time screening of all payment transactions, deposits, withdrawals, and financial flows

Screening Frequency and Triggers:

- **Onboarding:** All customers, affiliates, and vendors are screened before account opening or contract signing
- **Ongoing Screening:** Daily batch scans against updated lists
- **Event-Driven Rescreening:** Triggered when there is a change in ownership, corporate structure, address, or other material customer information

Escalation Process for Positive Matches:

- All potential or confirmed matches are automatically escalated to the Compliance Officer / Money Laundering Reporting Officer (MLRO)
- The MLRO performs a manual investigation, including:
 - Reviewing customer KYC and transactional history
 - Comparing the match to sanctions list details (e.g., date of birth, address, nationality)
 - Consulting additional databases or requesting supporting documents
- Based on the investigation, the MLRO determines the appropriate action:
 - Reject onboarding
 - Freeze accounts or suspend transactions
 - File a suspicious activity or suspicious transaction report (SAR/STR) with the Curacao FIU
 - Notify regulatory authorities where applicable

Audit Trail and Reporting:

- Olympus maintains detailed records of all sanctions screening activities, including:
 - Screening logs
 - Match investigation files
 - Communications with regulators or external parties
 - Final resolutions and actions taken
- Sanctions screening controls and records are included in the scope of:
 - Internal compliance reviews
 - Annual independent AML audits
 - Regulatory inspections by the Curacao Gaming Control Board or other competent authorities

Roles and Responsibilities:

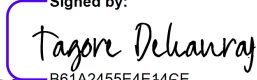
- The Compliance Officer / MLRO has overall accountability for the sanctions screening program

- The compliance operations team ensures system configuration, threshold setting, and timely handling of alerts
- The IT team is responsible for system maintenance, data integrity, and technical integration with onboarding and transaction systems

Continuous Improvement:

- Sanctions screening procedures are reviewed at least annually or when triggered by material events, such as:
 - New business lines, geographies, or products
 - Regulatory changes or updates to sanctions lists
 - Internal or external audit findings
- The compliance team proactively monitors international developments, typologies, and regulatory guidance to keep the program effective and up to date

Approved by: Tagore Hemant Dhanraj

Signed by:

B61A2455E4E14GE...
Board of Directors, Olympus Holdings N.V.

Date: [14.05.2025]

Next Review Date: [14.05.2025]