

Anti-Money Laundering (AML) Programme

Olympus Holdings N.V.

Operating: www.fireslots.bet | www.casinoempire.com

Effective Date: [10 March 2026] | Next Review Date: [10 March 2027] | Version: 3.0

Companion Document Notice

This AML Programme should be read in conjunction with the Company's Responsible Gaming Policy (Appendix E). The two policies are operationally linked: behavioural monitoring, vulnerable customer procedures, and player escalation pathways described in the Responsible Gaming Policy feed directly into this Programme's customer risk assessment, enhanced due diligence, and suspicious activity reporting frameworks.

Where a customer interaction triggers both Responsible Gaming and AML concerns, the matter must be escalated to the MLRO in accordance with Section 10 of this Programme.

1. Introduction

Olympus Holdings N.V. ("Olympus"), operating www.fireslots.bet and www.casinoempire.com, is committed to the highest standards of anti-money laundering (AML), counter-terrorism financing (CTF), sanctions compliance, and responsible gaming. This AML Programme describes the Company's internal policies, procedures, and controls to prevent the use of its platforms for money laundering, terrorist financing, and other financial crime.

Olympus holds a gaming licence under the Curaçao Gaming Authority (CGA) framework and recognises its obligations under all applicable Curaçao legislation, CGA regulations, and international standards including the Financial Action Task Force (FATF) Recommendations. This Programme has been updated to incorporate: (i) the most recent CGA data localisation and server infrastructure requirements (currently in draft, pending formal commencement); and (ii) the operational controls and escalation pathways set out in the Company's Responsible Gaming Policy (Appendix E).

2. Legal and Regulatory Framework

This AML Programme is developed and maintained in compliance with the following laws, regulations, and standards:

2.1 Curaçao Primary Legislation

- Landsverordening op de Kansspelen (LOK) – National Ordinance on Games of Chance: the primary statute governing gaming operations in Curaçao.
- Landsverordening Identificatie bij Financiële Dienstverlening (LIF) – National Ordinance on Identification for Financial Services: customer identification obligations for regulated entities.

- Landsverordening Melding Ongebruikelijke Transacties (MOT) – National Ordinance on Reporting of Unusual Transactions: mandatory reporting of suspicious or unusual transactions to FIU Curaçao.
- Landsverordening Bestrijding Witwassen en Terrorismefinanciering (LBWT) – National Ordinance on Combating Money Laundering and Terrorism Financing: the core AML/CTF compliance framework.
- Sanctielandsverordening Curaçao – Sanctions Ordinance: implementing UN Security Council and EU financial sanctions.

2.2 Curaçao Gaming Authority (CGA) Regulations

- CGA Regulations and Guidelines issued pursuant to the LOK, including player protection, data management, and technical standards.
- CGA Draft Regulation on Data Localisation and Server Infrastructure (pending formal commencement – see Section 16).
- CGA Licensing Conditions applicable to Olympus Holdings N.V., including responsible gaming obligations.

2.3 International Standards

- Financial Action Task Force (FATF) Forty Recommendations on Money Laundering and Nine Special Recommendations on Terrorist Financing.
- FATF Guidance for a Risk-Based Approach to the Gambling Sector (2021).
- Egmont Group Financial Intelligence Unit standards.

2.4 Data Protection

- Curaçao data protection legislation and applicable privacy frameworks governing the collection, retention, and processing of personal data, including player data stored on the Curaçao-based server infrastructure described in Section 16.

3. Governance Structure

Board of Directors: Ultimate responsibility for the AML Programme, including approval of this policy and all material amendments. The Board receives annual AML and responsible gaming compliance reporting from the MLRO.

Compliance Officer / MLRO: Ms Marwa Tarek Korayem is designated as Compliance Officer and Money Laundering Reporting Officer (MLRO), responsible for implementing and overseeing this AML Programme, receiving internal suspicious activity reports, coordinating responsible gaming escalations with AML implications, and maintaining regulatory relationships with the CGA and FIU Curaçao.

Responsible Gaming Monitoring Team: Responsible for behavioural monitoring, player intervention, and escalation to the Compliance Department where Responsible Gaming concerns intersect with AML or financial risk concerns (see Section 10).

All Employees: Individually responsible for complying with this AML Programme, completing mandatory training, and reporting suspicious activities or responsible gaming escalations to the MLRO promptly.

4. Risk Assessment

Olympus maintains a risk-based AML/CTF framework. Risk assessments are documented, reviewed annually, and updated upon material changes in business activities, regulatory guidance, or emerging typologies identified through the Responsible Gaming monitoring programme. The following risk dimensions are assessed:

- Country / Geographical Risks
- Customer Risks (PEP status, high-risk profiles, source of funds, vulnerability indicators)
- Product / Service Risks (online casino, live gaming, sports betting)
- Transaction Risks (volumes, methods, frequency, and jurisdictional exposure)
- Delivery Channel Risks (online channels, digital payments, crypto assets)
- Responsible Gaming Risk Indicators (see Section 10) that may indicate financial crime exposure

5. Age Verification and Customer Onboarding

Age verification and identity verification are conducted simultaneously during account onboarding and before any financial transactions are permitted. This dual-purpose control satisfies both the CGA's responsible gaming requirements and the AML/CTF identification obligations under the LIF and LBWT.

5.1 Age Verification Controls

- Access to the Company's platforms is strictly prohibited to individuals under the age of 18 years.
- Age verification is conducted during account onboarding, before deposits are permitted, and before withdrawals are processed.
- Accounts are temporarily suspended pending completion of age verification. Deposits and withdrawals are blocked until verification is successfully completed.
- Where an account is identified as belonging to an underage individual, the account is immediately closed and handled in accordance with internal procedures. Any financial transactions are reviewed in line with AML obligations before funds are returned or reported.

5.2 Standard Customer Due Diligence (CDD)

Upon account opening and throughout the customer relationship, Olympus collects and verifies:

- Full legal name, date of birth, nationality, and residential address

- Valid government-issued photo identification (passport, national ID, or driver's licence)
- Screening against global PEP lists, sanctions lists (UN, EU, OFAC, and applicable others), and adverse media databases
- Player account number, country of residence, ID type, and ID number (also recorded for CGA data reporting purposes – see Section 16)

5.3 Enhanced Due Diligence (EDD)

EDD is applied for:

- Politically Exposed Persons (PEPs) and their associates and family members
- Customers from high-risk or sanctioned jurisdictions identified by FATF or the CGA
- Unusually large, complex, or opaque transactions
- Customers exhibiting high-risk behavioural indicators (including those identified through Responsible Gaming monitoring)
- Customers displaying vulnerability indicators as described in Section 10.3

EDD measures include:

- Senior management written approval
- Source of funds and source of wealth documentation and verification
- Enhanced ongoing monitoring with increased review frequency
- Additional evidence of business or economic purpose for unusual activity

5.4 Simplified Due Diligence (SDD)

SDD is considered only for very low-risk scenarios and remains subject to regulatory approval and documented risk justification. SDD does not eliminate the requirement to collect basic identification information.

6. Ongoing Transaction Monitoring

- Continuous monitoring of all customer activity and transactions throughout the customer lifecycle.
- Review of patterns inconsistent with the known customer risk profile.
- Automated alerts for suspicious behaviours, including: rapid deposit-withdrawal cycles, structuring indicators, excessive loss chasing, and unusual payment method switching.
- CGA-mandated daily data points (deposits, withdrawals, bets, balances, losses, and winnings) are monitored, recorded, and stored in accordance with Section 16 of this Programme.
- High-risk customers are subject to enhanced monitoring and reviewed at least annually. Material changes to a customer's risk profile trigger an immediate review.
- Transaction monitoring outputs are reviewed by the MLRO and, where relevant, cross-referenced with Responsible Gaming behavioural monitoring data (see Section 10).

7. Responsible Gaming Tools and AML Relevance

The Responsible Gaming Policy (Appendix E) establishes a suite of player protection tools. Several of these tools produce data points or trigger events that are materially relevant to AML/CTF monitoring and customer risk assessment.

RG Tool / Control	Description	AML / Risk Relevance
Deposit Limits	Players may set daily, weekly, or monthly limits. Reductions take effect immediately; increases require a cooling-off period.	Limit override attempts or rapid limit increases may indicate financial crime. Reviewed by compliance when flagged.
Session Time Limits	Players set maximum session durations. System logs out the player upon expiry.	Extended or unusual session patterns combined with high deposit velocity are AML risk indicators.
Reality Check Notifications	Default 60-minute reminders showing session duration, amount wagered, and net win/loss. Player-adjustable.	Win/loss data feeds into daily CGA reporting and ongoing customer risk profile maintenance.
Cooling-Off Periods	Temporary suspension of 24 hours, 7 days, or 30 days. No access to gaming during the period.	Activation may indicate a customer in financial distress. Funds held during cooling-off are subject to AML review before release.
Self-Exclusion	1 year minimum to lifetime. Irrevocable for the period; marketing stopped; duplicate account creation blocked.	Attempts to circumvent self-exclusion by opening new accounts are a red flag requiring SAR consideration. Funds handled per Section 7.2.

7.1 Funds During Cooling-Off and Self-Exclusion

Where a player activates a cooling-off period or self-excludes and holds an account balance, the following applies:

- The account balance is frozen pending an AML review of the customer's transaction history.
- Withdrawals are processed only after satisfactory completion of the AML review and standard withdrawal verification procedures.
- Where the AML review identifies suspicious activity, the matter is escalated to the MLRO and a SAR/UTR is filed with FIU Curaçao if warranted before any funds are released.

7.2 Self-Exclusion Circumvention

Attempts to create duplicate accounts or otherwise circumvent self-exclusion are treated as a red flag indicator under this Programme. The MLRO is notified immediately and a SAR/UTR is considered. The duplicate account is closed and any deposited funds are held pending investigation.

8. Suspicious Activity Reporting (SAR)

All employees must immediately report suspicious activities to the MLRO using the internal reporting mechanism. The MLRO shall:

- Investigate the reported activity and document findings in a secure, confidential log.
- Determine whether a Suspicious Transaction Report (STR) or Unusual Transaction Report (UTR) must be filed with FIU Curaçao under the MOT Ordinance.
- Maintain tipping-off controls to ensure no subject is informed of a report or investigation. Tipping-off is a criminal offence under the MOT Ordinance.

Reportable suspicious activity indicators include (non-exhaustive):

- Large deposits or withdrawals without clear economic purpose.
- Structuring of transactions to remain below reporting or monitoring thresholds.
- Refusal or inability to provide requested identification or source of funds documentation.
- Inconsistency between the stated customer profile and observed transaction or gaming patterns.
- Use of multiple accounts, jurisdictions, or payment methods in unusual combinations.
- Rapid cycling of funds through the gaming account with minimal betting activity.
- Attempts to self-exclude followed immediately by new account opening – particularly where large deposits are involved.
- Customers in apparent financial distress (identified via Responsible Gaming monitoring) who continue to deposit significant sums.
- Requests for winnings to be paid to a third party or to a different payment method than the deposit source.

9. Record-Keeping

Olympus maintains comprehensive records to demonstrate compliance with applicable laws and to facilitate regulatory inspections by the CGA and FIU Curaçao. Where both AML/CTF obligations and CGA data requirements apply to the same record, the longer retention period governs.

Record Type	Minimum Retention	Legal Basis	Storage Location
Customer Due Diligence (CDD) documentation	5 years from end of relationship	LBWT / LIF	Secure primary system

Record Type	Minimum Retention	Legal Basis	Storage Location
Transaction records	5 years from transaction date	LBWT / MOT	Secure primary system
Suspicious Transaction Reports (STRs/UTRs)	5 years from filing date	MOT	MLRO secure log
Internal investigation notes and MLRO logs	5 years	LBWT	MLRO secure log
CGA-mandated player data (server-stored)	3 years minimum	CGA draft regulation	Curaçao Tier IV server (see S.16)
Responsible Gaming interaction records	5 years	LBWT / CGA	Compliance system
Self-exclusion and cooling-off records	5 years	LBWT / CGA	Compliance system
Training records (attendance and assessments)	5 years	LBWT	HR / Compliance system
Third-party due diligence records	5 years	LBWT	Compliance system

All records are stored securely with access controls, encryption, and audit trails. The CGA server data retention requirement of three years operates alongside, and does not replace, the five-year AML/CTF retention obligations.

10. Responsible Gaming and AML Convergence

Olympus recognises that responsible gaming obligations and AML/CTF obligations share common operational ground. The Responsible Gaming Policy (Appendix E) and this AML Programme operate together to provide a comprehensive customer risk management framework.

10.1 Behavioural Monitoring and AML Indicators

The Responsible Gaming monitoring programme operates manual systems designed to identify indicators of potentially problematic gaming behaviour. The following behaviours, when observed by the Responsible Gaming team, must be assessed for AML risk and escalated to the MLRO where appropriate:

Behavioural Indicator (RG)	Responsible Gaming Response	AML / Compliance Escalation
Increased deposit frequency	RG notification; possible mandatory limits	High deposit velocity is an AML risk indicator – refer to MLRO if threshold exceeded
Repeated failed deposit attempts	Customer contact by support staff	May indicate account testing or structuring – MLRO to assess
Extended gaming session duration	Reality check prompt; session limit	Extended sessions combined with high spend – transaction review triggered
Escalating bet sizes	RG notification; mandatory limit review	Rapid stake escalation inconsistent with profile – EDD triggered
Pattern indicating loss chasing	Direct contact; escalation to compliance	Loss chasing combined with repeated deposits is a red flag – MLRO notified
Emotional distress in communications	Welfare contact; escalation to compliance	Financial distress with continued high deposits – MLRO notified and SAR considered
Borrowing money to gamble	Immediate escalation to compliance	Third-party fund sourcing is a key AML risk indicator – SAR consideration required
Repeated bonus requests during financial difficulty	Compliance escalation	May indicate financial crime or misuse of promotional systems – MLRO review

10.2 Escalation Pathway

The escalation pathway for cases involving both Responsible Gaming and AML concerns is as follows:

- The Responsible Gaming monitoring team identifies a behavioural indicator.
- A Responsible Gaming interaction is conducted and documented in the compliance system.
- Where the interaction reveals AML risk indicators (as set out in the table above), the case is formally escalated to the MLRO.
- The MLRO reviews the customer's full transaction history, CDD file, and Responsible Gaming interaction records.
- The MLRO determines whether enhanced due diligence, additional monitoring, account restriction, or a SAR/UTR filing is required.

- All escalation outcomes are documented in the MLRO secure log.

10.3 Vulnerable Customers

The Company takes particular care when interacting with customers who display signs of vulnerability, financial distress, or loss of control. Vulnerability indicators include:

- Chasing losses across multiple sessions
- Evidence of borrowing money to fund gaming activity
- Emotional distress expressed in customer communications
- Repeated requests for bonuses or credit during apparent financial difficulty
- Sudden large deposits inconsistent with the customer's known financial profile

Where vulnerability is identified, the Responsible Gaming team applies appropriate safeguards per Appendix E. Where the same indicators suggest potential financial crime, the MLRO is notified concurrently. The welfare of the customer and the integrity of the AML programme are pursued in parallel and are not treated as competing obligations.

10.4 Responsible Marketing Compliance

All marketing activities comply with responsible gaming standards (Appendix E) and must not inadvertently facilitate financial crime. The following restrictions apply:

- Marketing communications do not target self-excluded players.
- Promotional offers are not presented in ways that could be used to structure deposits or exploit loyalty programmes for money laundering purposes.
- Bonus terms are clearly explained, and any anomalous use of bonuses (e.g. multi-accounting, bonus abuse patterns) is reported to the MLRO.

11. Payment Methods

Accepted payment channels are limited to:

- Verified bank transfers
- Credit and debit cards from reputable regulated issuers
- Approved e-wallets and payment service providers subject to AML/CTF obligations in their home jurisdictions
- Cryptocurrency payments (where permitted): subject to enhanced monitoring, blockchain analytics wallet screening, and source of funds verification. Anonymous or privacy coins are prohibited.

Payments are monitored for consistency with the customer's known risk profile. Anonymous or untraceable prepaid instruments are not accepted. Withdrawals must, as a general rule, be returned to the same payment method and account used for the original deposit. Requests for third-party payments are treated as red flag indicators and referred to the MLRO.

12. High-Risk Jurisdictions

Olympus does not onboard customers resident in FATF-identified high-risk and non-cooperative jurisdictions or those subject to UN, EU, or applicable Curaçao sanctions. Customers from other elevated-risk jurisdictions may only be onboarded following EDD and with written senior management approval, documented in the risk register. The CGA's jurisdiction guidance is reviewed quarterly and incorporated into the customer onboarding screening process.

13. Third-Party Relationships

- Thorough due diligence is performed prior to engagement of affiliates, payment processors, technology providers, and any outsourced service providers.
- Outsourced partners must contractually adhere to Olympus' AML standards and applicable Curaçao regulations, including CGA data and responsible gaming requirements.
- Regular audits and risk reassessments of critical third-party providers are conducted annually or upon material changes.
- Server infrastructure providers in Curaçao (see Section 16) must be able to demonstrate compliance with applicable CGA technical requirements, including Tier IV facility standards.

14. Training and Awareness

Annual mandatory AML/CTF and responsible gaming training is required for all relevant employees. Training records are maintained for a minimum of five years.

Employee Group	Training Content	Frequency
All employees	AML/CTF laws, suspicious activity identification, reporting obligations, tipping-off prohibition	Annual
Customer-facing / Support teams	CDD procedures, RG tool management, vulnerable customer identification, escalation pathways	Annual + onboarding
VIP Managers	EDD, source of wealth, RG-AML overlap indicators, escalation	Annual
Payments teams	Transaction monitoring, red flag indicators, payment method controls, crypto screening	Annual
Compliance / MLRO	Regulatory updates, SAR filing, CGA data requirements, FATF typologies	Annual + as needed
New employees (all)	AML induction and RG induction before customer interaction	Pre-commencement

15. Independent Audit

- An independent review of the AML Programme is conducted annually by a qualified external auditor or an internal audit function independent of day-to-day compliance operations.
- The audit scope includes: internal controls, transaction monitoring systems, CDD processes, record-keeping, CGA data localisation compliance (Section 16), responsible gaming and AML convergence procedures (Section 10), and sanctions screening.
- Audit findings and management responses are reported to the Board of Directors and the MLRO. Material deficiencies are remediated within agreed timelines with Board oversight.
- The MLRO provides the Board with an annual AML/CTF and responsible gaming compliance report, including metrics on SAR filings, escalations, training completion, and CGA reporting status.

16. CGA Data Localisation and Server Infrastructure Requirements

Pursuant to the CGA’s draft regulation on data localisation (pending formal commencement – the effective date has been postponed pending finalisation of the legislation), Olympus is required to store specified player and transaction data on a server physically located within Curaçao. The requirements set out below have been confirmed by the authorised server provider and are incorporated into this Programme on a best-efforts basis pending formal entry into force.

 Draft Regulation Status

As this regulation remains in draft format, Olympus will implement these requirements on a best-efforts basis. The MLRO is responsible for monitoring legislative developments and triggering a full policy update upon the regulation’s formal commencement date. The implementation obligations set out in Section 16.6 apply from the date of formal commencement.

16.1 Data Required to be Stored on the Curaçao Server

Data Category	Description	CGA Status
Unique Player Identifier	A unique player identification code (non-directly identifiable)	Required
Account Information	Account number, age, country of residence, ID type, and ID number	Required
Daily Deposits & Withdrawals	Total deposits and withdrawals per player per calendar day	Required
Daily Total Bets	Total wagering activity per player per calendar day	Required
Daily Losses & Winnings	Total daily losses and breakdown of winnings per player	Required

Data Category	Description	CGA Status
Daily Account Balances	Opening and closing balance per day, indicating freely withdrawable amount	Required

The data may be stored as a structured report or periodic export; the full primary production database is not required to reside on the Curaçao server. A dedicated table or export containing all required fields will satisfy the requirement.

Note that the account information fields (account number, age, residence, ID type, ID number) required for CGA server storage align with the customer identification data collected under the standard CDD process in Section 5.2 of this Programme. These data fields must therefore be maintained in a format suitable for both AML record-keeping and CGA server reporting.

16.2 Storage Frequency

Data must be uploaded, synchronised, or backed up to the Curaçao-hosted server at a minimum frequency of once per week. Olympus may implement daily synchronisation to support operational resilience and facilitate timely CGA access.

16.3 Server Architecture and Infrastructure

CGA Server Infrastructure Requirements (Confirmed by Server Provider)

- The Curaçao server does not need to be the primary production database. It may serve as a secondary backup, replica, or periodic data store.
- The server must be hosted in a Tier IV data centre facility physically located within Curaçao.
- Primary production infrastructure may remain hosted outside Curaçao, provided that the required critical data is synchronised to the Curaçao server at the minimum weekly frequency.
- The draft regulation does not prescribe specific availability requirements beyond the Tier IV facility standard.
- General best practices for data integrity, availability, and security apply in the absence of additional specific technical standards in the current draft.

16.4 CGA Access and Cooperation

The draft regulation requires cooperation to facilitate CGA access to the stored data, without specifying the technical mechanism. Olympus will ensure that:

- The MLRO and relevant IT and technical personnel are designated as points of contact for CGA data access requests.
- Structured data exports or direct system access can be provided to the CGA within a reasonable timeframe upon receipt of an official request.

- Any access protocols formally prescribed in subsequent regulatory guidance will be implemented promptly.

16.5 Data Retention – CGA Server

In accordance with the draft CGA regulation, data stored on the Curaçao server must be retained for a minimum of three (3) years. This requirement operates alongside, and does not replace, the five-year AML/CTF record-keeping obligations in Section 9. Where the same data is subject to both requirements, the five-year AML retention period governs.

16.6 Implementation Responsibilities

The MLRO, in coordination with the IT Department and Curaçao server infrastructure provider, is responsible for:

- Confirming that a compliant Curaçao-based Tier IV server is in place prior to or upon the regulation's formal commencement.
- Establishing and documenting the data synchronisation or backup process to ensure at least weekly transfer of the required data fields.
- Verifying that all six categories of player data in Section 16.1 are captured accurately, completely, and in a format compatible with CGA reporting requirements.
- Ensuring ongoing compliance with CGA access and cooperation requirements.
- Updating this Programme upon formal commencement of the CGA data localisation regulation or any amendment thereto.

17. Data Protection and Confidentiality

- Customer information is collected and retained in accordance with Curaçao data protection legislation and applicable privacy frameworks.
- Disclosure of customer information is made only to authorised personnel, the CGA, or FIU Curaçao as required by law.
- Encryption, access controls, and cybersecurity measures protect all sensitive customer and transaction data, including data held on the Curaçao-based server described in Section 16.
- Responsible Gaming interaction records, self-exclusion data, and vulnerability assessments are classified as sensitive personal data and subject to the highest level of access control.
- Tipping-off – informing a customer or third party that they are subject to a SAR, UTR, or investigation – is a criminal offence under the MOT Ordinance. All staff are trained on this prohibition.

18. Policy Violations and Sanctions

Non-compliance with this AML Programme may result in:

- Disciplinary action, up to and including termination of employment
- Regulatory reporting to the CGA or FIU Curaçao
- Civil or criminal penalties under applicable Curaçao law
- Reputational consequences and licence sanctions

19. Programme Review and Updates

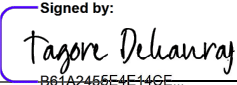
This AML Programme will be reviewed and updated:

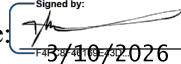
- Annually as a minimum
- Upon major changes in business operations, corporate structure, or gaming platform
- In response to regulatory changes, including formal commencement of CGA data localisation requirements
- Following material audit findings, compliance incidents, or significant typology changes
- When the Responsible Gaming Policy (Appendix E) is materially amended in ways that affect AML/CTF procedures

All amendments must be approved by the Board of Directors and communicated to all relevant staff. Version history is maintained by the MLRO.

Approvals

Approved by the Board of Directors, Olympus Holdings N.V.

Board Signatory:  Signed by: Tagore Dehaanraj Date: 3/9/2026
Sun Reliance Management B.V. 
MLRO: Ms Marwa Tarek

MLRO Signature:  Signed by: 3/10/2026 Date: _____

Next Scheduled Review Date: _____

*Companion Document: Responsible Gaming Policy (Appendix E) – Olympus Holdings N.V.
Version 3.0 supersedes all previous versions of the AML Programme.*