

MyMoon N.V.

AML- Anti-Money Laundering Policy

Version: 2.0

Contact: admin@mymoonnv.com

Approved on: 26/06/2025

Mymoon N.V., a licensed B2B game provider under the jurisdiction of Curaçao, is committed to maintaining the highest standards of Anti-Money Laundering (AML), Countering the Financing of Terrorism (CFT), and combating the financing of proliferation (CFP). This policy reflects the regulatory requirements established under the Curaçao Gaming Control Board (GCB) "Regulations for the Combating of Money Laundering, the Financing of Terrorism and Proliferation of Weapons of Mass Destruction," effective January 10, 2025 with mandatory compliance by April 10, 2025.

Mymoon N.V., a licensed game provider under the jurisdiction of Curaçao, is committed to upholding the highest standards of Anti-Money Laundering (AML) and Countering the Financing of Terrorism (CFT) compliance in all aspects of its B2B operations. This policy outlines the framework through which Mymoon N.V. identifies, assesses, and mitigates risks related to money laundering and terrorist financing.

Key elements of the policy include:

- **Risk-Based Approach (RBA):** Systematic assessment and classification of business partners and activities based on their inherent AML/CFT risks, ensuring resources are focused on higher-risk areas.
- **Customer Due Diligence (CDD):** Robust verification and ongoing monitoring of all clients, including identification of Ultimate Beneficial Owners (UBOs), screening against sanctions and Politically Exposed Persons (PEP) lists, and applying enhanced due diligence where necessary. This includes checks for proliferation financing and use of the GCB's published sanctions registry.
- **Ongoing Monitoring & Transaction Controls:** Continuous oversight of client activities, usage patterns, and commercial transactions to detect irregularities and prevent misuse of the platform.
- **Training and Awareness:** Comprehensive training programs for employees and contractors to maintain awareness of AML obligations, emerging risks, and internal procedures.
- **Roles and Responsibilities:** Clear allocation of governance, management, compliance, and operational duties to ensure effective implementation and accountability within the organization.
- **Recordkeeping and Documentation:** Secure retention of all relevant AML records for a minimum of five years, ensuring transparency and compliance with Curaçao regulatory requirements.
- **Policy Review and Updates:** Regular review and timely amendment of the AML policy to adapt to evolving legal requirements, business changes, and risk landscapes.

Mymoon N.V. is dedicated to fostering a culture of compliance, integrity, and cooperation with regulators and partners to protect the gaming ecosystem from illicit activities.

1. Regulatory Context and Compliance Commitment

1.1

Legislative

Background

Mymoon N.V. acknowledges the enactment of the National Ordinance for Games of Chance (LOK) and its supplementary AML/CFT/CFP Framework, adopted in April 2024 and entering into effect in 2025, under the supervision of the Curaçao Gaming Control Board (GCB). These reforms align Curaçao's regulatory environment with the Financial Action Task Force (FATF) recommendations and meet international standards for Anti-Money Laundering, Countering the Financing of Terrorism, and combating the Financing of Proliferation (CFP).

Mymoon N.V. acknowledges the enactment of the **National Ordinance for Games of Chance (LOK)** and its supplementary **AML/CFT Framework**, adopted in **April 2024** and entering into effect in **2025**, under the supervision of the **Curaçao Gaming Authority (CGA)**.

These reforms were introduced to align Curaçao's regulatory environment with the **Financial Action Task Force (FATF)** recommendations and to meet international standards for Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT).

Under this legislation, all licensed gaming operators—including **B2B suppliers such as Mymoon N.V.**—are required to establish and maintain effective systems and controls to:

- Detect and deter money laundering and terrorist financing,
- Assess and manage risk using a risk-based approach (RBA),
- Report suspicious or unusual transactions to the appropriate authorities,
- Appoint a designated AML Compliance Officer.

2. Policy Scope & Commitment Statement

2.1 Scope of the AML Policy

This Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT) Policy applies to **Mymoon N.V.**, a private entity incorporated under the laws of Curaçao and operating under a valid online gaming **B2B license** issued by the Curaçao Gaming Authority (CGA).

As a **business-to-business (B2B)** game provider, Mymoon N.V. offers online slot content and associated platform services exclusively to B2C gaming operators. Mymoon N.V. does not interface directly with end-users or individual players.

Despite this operational model, the company acknowledges that it may still be exposed—directly or indirectly—to money laundering or terrorist financing risks through:

- Relationships with business partners operating in high-risk jurisdictions;
- Integration of its software or APIs into environments with inadequate AML controls;
- Use of its infrastructure to mask the origin of criminal funds.

Therefore, this policy applies to:

- **All Mymoon N.V. business relationships**, particularly during onboarding, risk assessment, and ongoing monitoring;
- **All internal departments** (commercial, compliance, legal, and IT) responsible for implementing due diligence, transaction screening, and regulatory reporting;

- **All senior management and employees**, including contractors and third-party service providers who are in a position to identify or report suspicious activities.

2.2 Commitment to Compliance and Ethical Conduct

Mymoon N.V. affirms its **zero-tolerance approach** to money laundering and terrorist financing and is committed to:

- Upholding the requirements of the **National Ordinance for Games of Chance (LOK)** and all AML/CFT directives issued by the Curaçao Gaming Authority;
- Aligning its policies and internal controls with the **Financial Action Task Force (FATF)** standards and best practices for B2B gaming providers;
- Promoting a culture of compliance, integrity, and ethical conduct at every level of the organization;
- Maintaining transparent, auditable relationships with all clients, supported by appropriate **Customer Due Diligence (CDD)** and **risk assessment** procedures;
- Ensuring that all staff receive **regular AML training**, are aware of red flags and reporting obligations, and are encouraged to report concerns without fear of retaliation.

2.3 Continuous Improvement

This AML Policy is subject to **ongoing review and enhancement** in light of:

- Updates to Curaçao's regulatory framework;
- Emerging typologies of financial crime;
- Internal audit findings or compliance issues;
- Feedback from the CGA or other competent authorities.

Mymoon N.V. commits to **updating this policy biannually**, or more frequently as required, and to implementing any necessary changes in a timely and transparent manner.

3. Risk Assessment (Risk-Based Approach - RBA)

3.1 Purpose and Guiding Principles

In compliance with the Curaçao Gaming Authority (CGA) regulatory framework and in accordance with the recommendations of the **Financial Action Task Force (FATF)**, Mymoon N.V. implements a formal **Risk-Based Approach (RBA)** to Anti-Money Laundering (AML) and Countering the Financing of Terrorism (CFT).

The objective of the RBA is to ensure that Mymoon N.V. allocates its resources effectively by identifying and assessing the **specific ML/TF risks** associated with its **B2B operations**, and by applying proportionate controls and mitigation measures.

This includes recognizing:

- That not all customers or transactions present the same level of risk;
- That enhanced measures are required for higher-risk scenarios;

- That simplified measures may be appropriate for low-risk relationships, subject to regulatory limits.

3.2 Risk Assessment Framework

Mymoon N.V. conducts a **comprehensive enterprise-wide risk assessment** (EWRA) at least annually, and whenever there is a material change in operations, markets, products, or the regulatory environment. This assessment includes the evaluation of the following key risk categories:

a. Customer Risk

- Jurisdiction of incorporation and licensing;
- Nature of the customer's operations (e.g., B2C operators serving high-risk jurisdictions);
- Regulatory status and history of compliance;
- Ownership structure and presence of Politically Exposed Persons (PEPs).

b. Geographic Risk

- Country of incorporation or operation of the business partner;
- Sanctions status (UN, EU, OFAC, CFATF, etc.);
- FATF listing (high-risk or non-cooperative jurisdictions).

c. Product & Service Risk

- Integration type (e.g., API access, white-label services);
- Degree of control over downstream operators;
- Customization level and technological complexity (e.g., use of cryptocurrency-ready tools).

d. Delivery Channel Risk

- Onboarding methods (automated vs. manual);
- Communication and contracting (in-person vs. remote);
- Reliance on third-party intermediaries.

e. Transaction Risk

- Transaction value, frequency, and pattern;
- Settlement currencies, especially non-fiat options;
- Cross-border movement of funds.

3.3 Risk Scoring and Classification

Each business partner and operational process is assigned a **risk score** using a weighted scoring model that classifies risk as:

- **Low Risk**
- **Medium Risk**

- **High Risk**

High-risk customers or partners are subject to **Enhanced Due Diligence (EDD)** procedures (see Section 4.4). Risk classification results are documented and reviewed regularly.

3.4 Mitigation Measures

In accordance with risk classification, Mymoon N.V. applies tailored measures, including but not limited to:

- **Standard CDD** for low/medium-risk clients;
- **EDD and approval from senior management** for high-risk cases;
- **Increased frequency of monitoring** and transaction review;
- **Rejection or termination of business relationships** if AML risks cannot be adequately mitigated.

3.5 Periodic Review and Continuous Monitoring

- The enterprise-wide risk assessment is reviewed **annually**, or upon major events (e.g., expansion into new markets or technology changes).

A record of the risk assessments and decision-making rationale is retained for a **minimum of five years**, in accordance with Curaçao's AML laws.

4. Customer Due Diligence (CDD)

4.1 General Principle

Mymoon N.V. applies **Customer Due Diligence (CDD)** measures in accordance with the Curaçao Gaming Authority (CGA) AML/CFT regulations and the FATF Recommendations. CDD is essential for establishing the identity of business partners, understanding the nature and purpose of the business relationship, and assessing the associated risk of money laundering or terrorist financing.

Although Mymoon N.V. operates under a B2B model and does not engage in end-user (player) transactions, it remains responsible for conducting robust CDD on all its clients—primarily B2C gaming operators.

CDD is conducted at the time of:

- Onboarding a new client;
- Reviewing or renewing existing agreements;
- Significant changes in ownership or control;
- Trigger events such as suspicious activity or jurisdictional changes.

4.2 CDD Thresholds and Triggers

Mymoon N.V. performs CDD:

- Prior to entering into any business relationship;
 - Whenever a client's activities exceed a **transactional or value threshold** as advised by the CGA (e.g., Naf. 4,000 / approx. €2,000);
 - In response to any **adverse media, sanctions alerts**, or internal red flags;
 - When there are doubts about the veracity or adequacy of previously obtained information.
-

4.3 Identification and Verification

For all business partners, Mymoon N.V. collects and verifies the following information:

A. Legal Entities

- Full legal name and registered business address;
- Certificate of Incorporation or equivalent legal document;
- Articles of Association or company statutes;
- Valid gaming license(s) and jurisdiction of issuance;
- Tax Identification Number (TIN) or VAT registration;
- Names and verification of directors, legal representatives, and **Ultimate Beneficial Owners (UBOs)**;
- Details of the ownership/control structure (via a corporate chart where applicable).

B. Individual UBOs or Key Controllers

- Full name, date of birth, nationality, and residential address;
- Official identification documents (passport, national ID);
- Proof of address (e.g., utility bill or bank statement not older than 6 months);
- Source of wealth/source of funds declarations when required.

Mymoon N.V. relies on **independent and reliable sources** to verify this data (e.g., government registers, public databases, third-party verification tools).

4.4 Sanctions and PEP Screening

All clients, UBOs, and key personnel are screened against:

- International sanctions lists (UN, EU, OFAC, CFATF, etc.);
- Lists of **Politically Exposed Persons (PEPs)**, close associates, and family members;
- Adverse media monitoring databases.

If a match is found, enhanced due diligence measures are immediately applied, and onboarding may be suspended pending review.

4.5 Enhanced Due Diligence (EDD)

EDD is required when a client is classified as **high-risk**, which may include:

- Operating from or licensed in a high-risk jurisdiction;
- Having complex or opaque ownership structures;
- Use of cryptocurrencies or anonymous payment systems;
- Associations with PEPs or sanctioned entities.

EDD measures may include:

- Obtaining additional corporate or financial documentation;
 - Verifying the **source of funds/wealth**;
 - Requiring senior management approval to commence the relationship;
 - Conducting more frequent ongoing monitoring and audits.
-

4.6 Ongoing Due Diligence and Review

Mymoon N.V. conducts **ongoing monitoring** of its business relationships to ensure:

- Transactions are consistent with the client's known profile;
- Information collected through CDD remains accurate and up to date;
- Risk profiles are revised based on updated intelligence, behavior, or regulatory developments.

Client files are reviewed periodically based on risk level:

- **Annually** for high-risk clients;
- **Every 2–3 years** for medium- and low-risk clients.

All records of due diligence and verification are retained for **at least five years** from the end of the business relationship.

5. Ongoing Monitoring

5.1 Purpose

Ongoing monitoring is essential to ensure that business relationships remain consistent with the customer's profile and declared purpose, and to detect unusual or potentially suspicious activity. Although Mymoon N.V. operates in a **B2B capacity** and does not process individual player transactions, it maintains controls to monitor the **behavior and operations** of its business partners within its platform environment.

6. Training and Awareness

6.1 Objective

Mymoon N.V. is committed to fostering a strong culture of compliance through ongoing training and awareness programs. These initiatives ensure that all employees, management, and relevant contractors understand their AML/CFT responsibilities and are equipped to identify and respond effectively to money laundering and terrorist financing risks.

6.2 Scope of Training

AML training is mandatory for:

- All employees of Mymoon N.V., regardless of role or seniority;
- Senior management and the Board of Directors;
- Contractors and third-party service providers involved in compliance, legal, IT, or operational functions related to AML risk management;
- New hires during their onboarding process.

6.3 Frequency and Delivery

- **Initial training** is provided to all new employees within their first month of employment.
- **Refresher training** is conducted at least annually, with additional sessions as required by regulatory updates or audit findings.
- Training is delivered through a combination of:
 - Interactive e-learning modules;
 - Live webinars or workshops;
 - Internal communications and awareness campaigns.

6.4 Promoting a Compliance Culture

Mymoon N.V. encourages an open environment where employees feel confident to:

- Raise questions about AML policies and procedures;
- Report suspicious activity or compliance concerns without fear of retaliation;
- Participate actively in ongoing compliance efforts.

7. Roles and Responsibilities

7.1 Board of Directors

- **Oversight and Governance:** The Board is responsible for providing overall governance and oversight of Mymoon N.V.'s AML framework, ensuring that adequate resources and support are allocated to compliance functions.
 - **Approval of Policies:** The Board reviews and formally approves the AML policy and any significant updates.
 - **Risk Appetite:** Defines the company's risk appetite related to AML/CFT and ensures that it aligns with regulatory expectations.
-

7.2 Senior Management

- **Implementation:** Senior management is accountable for implementing the AML policy and ensuring its integration into daily operations.
 - **Risk Management:** Ensures that risk assessments are conducted regularly and appropriate mitigation strategies are in place.
 - **Reporting:** Receives regular reports from the AML Compliance Officer on compliance status, risks, and issues.
-

7.3 AML Compliance Officer

- **Designated Officer:** Appointed formally by senior management with clear authority and independence to perform AML duties.
 - **Policy Development:** Maintains, updates, and enforces the AML policy.
 - **Monitoring and Reporting:** Oversees ongoing monitoring activities and escalates suspicious transactions or activities to the Curaçao Financial Intelligence Unit (FIU) and/or CGA as required.
 - **Training Coordination:** Coordinates and delivers AML training programs across the organization.
 - **Regulatory Liaison:** Acts as the primary contact point for regulatory bodies and auditors regarding AML matters.
 - **Recordkeeping:** Ensures documentation of AML activities, decisions, and reports are maintained in compliance with statutory requirements.
-

7.4 Department Heads

- **Compliance Integration:** Heads of commercial, legal, IT, and operations departments ensure that AML requirements are embedded within their teams' workflows.
 - **Risk Identification:** Responsible for identifying AML risks relevant to their operational areas and escalating concerns promptly.
 - **Support to Compliance Officer:** Facilitate AML controls and assist with investigations or audits as needed.
-

7.5 All Employees

- **Compliance Adherence:** All employees are required to understand and comply with Mymoon N.V.'s AML policy and procedures.
 - **Reporting Obligations:** Must remain vigilant for suspicious activity and report concerns promptly through established channels.
 - **Training Participation:** Required to complete AML training and stay informed on compliance updates.
-

7.6 Third-Party Service Providers

- **Due Diligence:** Subject to AML due diligence consistent with their role and risk profile.
- **Compliance Cooperation:** Expected to adhere to Mymoon N.V.'s AML standards and cooperate with monitoring or audits as applicable.

9. Recordkeeping and Documentation

9.1 Purpose

Mymoon N.V. maintains comprehensive records of all AML-related activities to ensure transparency, facilitate audits, and comply with the legal retention requirements stipulated by the Curaçao Gaming Authority (CGA) and applicable laws.

9.2 Types of Records

The following records must be retained in a secure and accessible manner:

- **Customer Due Diligence (CDD) files**, including identification and verification documents of business partners and Ultimate Beneficial Owners (UBOs);
 - **Monitoring logs** and alerts generated through ongoing AML controls;
 - **Suspicious Transaction Reports (STRs)** and correspondence with regulatory authorities;
 - **Training records** evidencing AML awareness and completion by employees;
 - **Internal audit and compliance review reports** related to AML processes.
-

9.3 Retention Period

All AML records shall be retained for a minimum of **five (5) years** from the date of the last transaction or the termination of the business relationship, whichever is later.

9.4 Security and Confidentiality

- Records must be stored securely to prevent unauthorized access, alteration, or destruction.
- Access to AML documentation is restricted to authorized personnel on a **need-to-know basis**.
- Mymoon N.V. complies with all applicable data protection laws in handling personal and business information.

10. Policy Review and Updates

10.1 Purpose

To maintain an effective and compliant Anti-Money Laundering (AML) framework, Mymoon N.V. commits to the regular review and timely updating of this AML Policy to reflect changes in laws, regulations, business activities, and emerging risks.

10.2 Review Frequency

- The AML Policy shall be formally reviewed **at least biannually**.
 - Additional reviews shall be conducted promptly when:
 - There are significant changes to Curaçao's AML/CFT regulations or guidance issued by the Curaçao Gaming Authority (CGA);
 - There are changes to international standards, such as FATF recommendations;
 - The company undertakes significant changes in its business model, services, or customer base;
 - Internal audits, risk assessments, or external regulatory reviews identify material gaps or improvement areas;
 - New money laundering or terrorist financing typologies emerge that may impact the business.
-

10.3 Responsibilities

- The **AML Compliance Officer** is responsible for initiating and coordinating the policy review process.
 - Updates and amendments must be approved by **senior management** and the **Board of Directors** before implementation.
 - All employees shall be informed of material changes and provided with updated training as necessary.
-

10.4 Documentation and Communication

- All versions of the AML Policy shall be documented, dated, and archived.
- Changes to the policy shall be clearly communicated to all relevant staff and stakeholders in a timely manner.
- Compliance with the updated policy shall be monitored and enforced.