

Policy Title: Anti-Money Laundering & Counter-Terrorist Financing (AML/CTF) Policy

Effective Date: 15 June 2025

Next Review Date: 15 June 2026

Approved By: Compliance Officer

Responsible Office: Glory Multimedia B.V. Compliance Department

Applies To: All employees, partners, and third-party service providers of Glory Multimedia B.V. and its operated domains

1. Policy Statement

Glory Multimedia B.V. is committed to full compliance with anti-money laundering (AML) and counter-terrorist financing (CTF) obligations under Curaçao regulations. This policy outlines our proactive approach to detecting, preventing, and reporting suspicious activities related to money laundering, terrorist financing, and the financing of weapons of mass destruction across all platforms operated under our company.

2. Purpose

This policy aims to:

- Ensure that Glory Multimedia B.V.'s platforms are not used for illicit financial activities
 - Implement a risk-based approach to AML/CTF in line with Curaçao laws and CGA directives
 - Define responsibilities, procedures, and internal controls to identify and mitigate ML/TF risks
 - Comply with obligations outlined by the Financial Intelligence Unit (FIU) of Curaçao
-

3. Audience

This policy applies to:

- All Glory Multimedia B.V. employees
- Contractors, agents, and affiliates
- Third-party service providers
- Any individual involved in onboarding, payments, or transaction monitoring

4. Definitions

- **ML/TF: Money Laundering and Terrorist Financing**
 - **PEP: Politically Exposed Person**
 - **CDD: Customer Due Diligence**
 - **EDD: Enhanced Due Diligence**
 - **CRA: Customer Risk Assessment**
 - **FIU: Financial Intelligence Unit of Curaçao**
 - **STR/SAR: Suspicious Transaction / Activity Report**
-

5. Policy Implementation

5.1 Business Risk Assessment

We conduct a comprehensive risk assessment of all our brands and delivery channels to identify vulnerabilities to ML/TF, based on product, geography, transaction types, and payment methods.

5.2 Customer Risk Assessment (CRA)

Each customer is profiled at onboarding. Risk indicators include location, payment behavior, PEP status, and source of funds.

5.3 Customer Acceptance Policy (CAP)

Acceptance depends on risk score. PEPs and sanctioned individuals are automatically flagged. High-risk accounts are subject to EDD.

5.4 Customer Due Diligence (CDD)

CDD includes:

- **Government-issued photo ID verification**
- **Proof of address and date of birth**
- **PEP/Sanctions screening**
- **Periodic KYC refreshes and re-verification**

If a suspicious profile is confirmed, customer funds are frozen and an STR is submitted to the FIU.

5.5 Ongoing Monitoring

Automated and manual review tools flag unusual behavior, including:

- Inconsistent or irregular deposits/withdrawals
- Third-party payments
- Cancelled withdrawal requests
- Reversed winnings

5.6 Reliance on Third Parties

Where third parties (e.g., PSPs) are involved, we ensure:

- A written agreement is in place
- AML/CTF standards are contractually enforced
- Access to KYC data and logs is retained

5.7 Reporting Suspicious Activities

STRs are submitted to the Curaçao FIU. Reports are prepared by the Compliance Team and reviewed before submission.

5.8 AML Compliance Program

Our framework includes:

- Designated AML Compliance Officer
- Mandatory annual AML training for relevant staff
- 5-year record retention of CDD and STRs
- Internal escalation procedures and audit readiness
- Immediate freezing of accounts upon valid suspicion

6. Compliance and Consequences

Failure to comply may result in:

- Disciplinary action or contract termination

- Regulatory sanctions
 - Criminal liability for individuals or the company
 - License review or suspension by CGA
-

7. Related Policies & Legal References

- Know Your Customer (KYC) Policy
 - Curaçao AML/CTF Guidelines
 - LOK (National Ordinance for Identification)
 - NORUT (National Ordinance for Reporting of Unusual Transactions)
 - FATF Recommendations and EU 5AMLD Framework
-

8. Contact Information

Compliance Department – Glory Multimedia B.V.

 Email: management@glorymultimedia.com

9. Policy History

- Version 1.0 – 15 June 2025
Initial release based on CGA's 2025 AML/CTF regulatory framework.
-

10. Online Access

This AML/CTF Policy is accessible across all domains operated by Glory Multimedia B.V.

 <https://www.enebet.com/en/help/13904>