

MOMO ENTERTAINMENT B.V.

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

Registered Office

Schottegatweg Oost 10, United 1-9, Bon Bini Business Center, Willemstad, Curaçao

Contact

info@momoentertainmentbv.com

CGA License Number

OGL/2024/940/0485

Document Classification: Internal / Confidential

Version 1.0

Key Information

CGA License Number	OGL/2024/940/0485
Approving Official(s)	Ioannis Kaisarios — Ultimate Beneficial Owner (UBO), Momo Entertainment B.V.
Responsible Office	Compliance Department — AML Compliance Officer (Money Laundering Reporting Officer / MLRO)
Effective Date	18 June 2026
Next Review Date	18 June 2027

Key Information	2
1. Policy Statement	3
2. Purpose	3
3. Audience	3
4. Definitions	4
5. Policy Implementation	5
5.1 Business Risk Assessment	5
5.2 Customer Risk Assessment	5
5.3 Customer Acceptance Policy	6
5.4 Customer Due Diligence	6
5.5 Ongoing Monitoring	7
5.6 Reliance on Third Parties to Perform Customer Due Diligence	7
5.7 Reporting of Unusual Transactions	8
5.8 Anti-Money Laundering Compliance Program	8
6. Compliance and Consequences of Non-Compliance	9
7. Related Information	9
8. Contact Information	9
9. Policy History	10
10. Policy URL	10

1. Policy Statement

Momo Entertainment B.V. (“the Company,” “Momo Entertainment,” or “we”) is committed to conducting its gaming operations with the highest standards of integrity and in full compliance with the anti-money laundering and counter-terrorist financing (AML/CTF) laws and regulations of Curaçao, including the National Ordinance on Games of Chance and the regulations, directives, and guidelines issued by the Curaçao Gaming Authority (CGA) and the Financial Intelligence Unit Curaçao.

The Company has zero tolerance for the use of its products, services, or platforms — whether knowingly or unknowingly — to launder the proceeds of crime, finance terrorism, or finance the proliferation of weapons of mass destruction. This Policy sets out the framework, governance structure, and minimum standards that the Company applies to identify, assess, monitor, and mitigate the money laundering, terrorist financing, and proliferation financing (“ML/TF/PF”) risks to which it is exposed as a Curaçao-licensed gaming operator.

This Policy applies to all products and services offered by the Company under its Curaçao gaming license (License No. OGL/2024/940/0485), including online casino games, live dealer games, and sports betting. It is binding on the entire organization and supersedes any conflicting internal practice.

2. Purpose

This Policy has been developed to:

- comply with the Company’s legal and regulatory obligations under Curaçao AML/CTF legislation and the conditions of its CGA license;
- establish a risk-based framework for identifying and mitigating the ML/TF/PF risks specific to remote gaming;
- ensure that customer due diligence, ongoing monitoring, and reporting obligations are consistently and effectively applied;
- protect the Company, its directors, employees, and players from being exploited for criminal purposes; and
- provide clear guidance and accountability to staff regarding their individual AML/CTF responsibilities.

This Policy gives effect to, among others, the requirements arising from the National Ordinance on Games of Chance (Landsverordening op de kansspelen), the National Ordinance on the Reporting of Unusual Transactions, and the AML/CTF guidelines issued by the Curaçao Gaming Authority.

3. Audience

This Policy applies to:

- all directors, officers, and employees of Momo Entertainment B.V., regardless of seniority or function;
- the designated Compliance Officer / Money Laundering Reporting Officer (MLRO) and any deputy;
- subcontractors, consultants, and third-party service providers engaged in customer-facing, payment, or compliance-related functions on behalf of the Company; and
- any introducer, affiliate, or white-label partner operating under the Company's CGA license, where applicable.

All individuals and entities within scope are required to read, understand, and comply with this Policy and any related procedures referenced in Section 7.

4. Definitions

- Money Laundering (ML): the process by which proceeds of criminal activity are disguised so that they appear to originate from a legitimate source.
- Terrorist Financing (TF): providing or collecting funds, directly or indirectly, with the intention or knowledge that they will be used to carry out terrorist acts.
- Proliferation Financing (PF): providing funds or financial services that are used, in whole or in part, for the manufacture, acquisition, development, or use of weapons of mass destruction.
- Customer Due Diligence (CDD): the process of identifying and verifying a customer's identity and understanding the nature and purpose of the business relationship.
- Enhanced Due Diligence (EDD): additional due diligence measures applied to higher-risk customers or relationships.
- Politically Exposed Person (PEP): an individual who holds or has held a prominent public function, or an immediate family member or close associate of such a person.
- Beneficial Owner: the natural person(s) who ultimately owns or controls a customer, or on whose behalf a transaction or activity is conducted.
- FIU Curaçao / MOT: the Financial Intelligence Unit of Curaçao (Meldpunt Ongebruikelijke Transacties), the authority to which unusual transactions must be reported.
- Unusual Transaction: a transaction or pattern of behavior that deviates from a customer's expected profile, or that otherwise gives rise to a reasonable suspicion of ML/TF/PF, and which must be reported to the FIU Curaçao.
- Risk-Based Approach (RBA): an approach whereby the intensity of due diligence, monitoring, and controls is proportionate to the level of ML/TF/PF risk identified.
- Sanctions Screening: the process of checking customers, beneficial owners, and transactions against applicable sanctions lists (e.g., UN, EU, OFAC, and any Curaçao designations).

- Source of Funds / Source of Wealth: the origin of the specific funds used in a transaction, and the origin of a customer's overall wealth, respectively.
- CGA: the Curaçao Gaming Authority, the regulator responsible for licensing and supervising games of chance in Curaçao.

5. Policy Implementation

The Company implements this Policy through the risk-based components set out in Sections 5.1 to 5.8 below. Overall responsibility for implementation rests with the Compliance Officer, who reports to senior management and the Board on the matters set out in this Section.

5.1 Business Risk Assessment

The Company maintains a documented Business Risk Assessment (BRA), reviewed and updated at least annually and upon any material change to its products, customer base, distribution channels, or the regulatory environment. The BRA identifies and evaluates the inherent ML/TF/PF risks associated with:

- the products and services offered (e.g., online casino, slots, table games, live dealer games, and/or sports betting), including the speed and volume of transactions and any anonymity features;
- delivery channels, including the fact that the Company operates remotely and does not meet customers face-to-face;
- the geographic markets and jurisdictions from which customers are accepted, with reference to FATF lists of high-risk and monitored jurisdictions and the Curaçao National Risk Assessment;
- payment methods accepted (e.g., credit/debit cards, e-wallets, bank transfers, and, where applicable, virtual assets) and their relative ML/TF/PF risk; and
- the customer base, including the proportion of PEPs, high-value players, and corporate or agent accounts.

For each risk category, the Company assigns an inherent risk rating (low, medium, or high), documents the mitigating controls in place, and determines a residual risk rating. The outcome of the BRA directly informs the Customer Acceptance Policy, the customer due diligence measures in Section 5.4, and the resourcing of the compliance function. The Compliance Officer is responsible for maintaining the BRA and presenting its conclusions to senior management and the Board at least once a year.

5.2 Customer Risk Assessment

Every customer is subject to an individual Customer Risk Assessment (CRA) prior to, or at the point of, the establishment of a business relationship (i.e., account registration), and the CRA is updated throughout the relationship. The CRA considers, at a minimum:

- customer risk factors: nationality, country of residence, occupation, PEP status, adverse media, source of funds/wealth, and whether the customer is acting on behalf of a third party;
- product and channel risk factors: the games played, stake sizes, payment methods used, and any use of VPNs or other anonymizing technology; and
- geographic risk factors: country of residence and registration, and the jurisdictions from which funds are received.

Each customer is assigned a risk rating of low, medium, or high based on a weighted combination of these factors. The risk rating determines the level and frequency of due diligence and ongoing monitoring applied under Sections 5.4 and 5.5. Risk ratings are reviewed periodically and upon trigger events, such as a material change in deposit or withdrawal behavior, an adverse media hit, or a sanctions or PEP screening alert.

5.3 Customer Acceptance Policy

The Customer Acceptance Policy (CAP) sets out the conditions under which a prospective customer may be onboarded, restricted, or refused, based on the outcome of the CRA. As a minimum, the Company will not accept:

- customers who are minors or who cannot be verified as being of legal gambling age;
- customers resident in jurisdictions where the Company is not permitted to offer its services, or which are subject to comprehensive international sanctions;
- customers who appear on, or are owned or controlled by an entity on, applicable UN, EU, OFAC, or other relevant sanctions lists; and
- customers who refuse to provide the identification or source-of-funds information requested as part of CDD or EDD.

Customers identified as PEPs, or otherwise rated high-risk, may only be onboarded following Enhanced Due Diligence and the explicit approval of the Compliance Officer or senior management, consistent with the Company's obligations regarding PEPs and sanctions screening. The CAP is applied consistently, irrespective of a customer's expected profitability to the Company.

5.4 Customer Due Diligence

The Company applies CDD measures proportionate to a customer's risk rating, before or as soon as reasonably practicable after the establishment of the business relationship, and in any case before any funds are withdrawn. CDD measures include:

- verification of identity using a valid government-issued identification document, and verification of the customer's residential address;
- screening of the customer's name against sanctions lists (UN, EU, OFAC, and any other applicable list) and PEP databases, both at onboarding and on an ongoing basis;
- where applicable, identification of the beneficial owner(s) and of any person purporting to act on the customer's behalf; and

- for high-risk customers, Enhanced Due Diligence, including verification of source of funds and/or source of wealth, senior management approval to commence or continue the relationship, and more frequent ongoing monitoring.

Where a positive sanctions match is confirmed, the Company will immediately freeze the relevant customer's account and funds, refrain from processing any further transactions on the account, and report the match without delay to the competent Curaçao authorities, including the FIU Curaçao and, where applicable, the relevant designated sanctions authority, in accordance with applicable freezing and reporting obligations. No funds will be released, and no information about the freezing action will be disclosed to the customer, except as permitted by law.

5.5 Ongoing Monitoring

The Company conducts ongoing monitoring of each business relationship to ensure that customer activity remains consistent with the Company's knowledge of the customer, including the customer's risk profile, source of funds, and stated purpose of the relationship. Ongoing monitoring includes:

- automated and manual transaction monitoring to detect deposits, withdrawals, or gameplay patterns inconsistent with the customer's profile (e.g., structuring, rapid deposit-and-withdrawal with minimal gameplay, use of multiple payment instruments or third-party payment sources, or transactions just below internal thresholds);
- periodic re-screening of customers against sanctions and PEP lists, including re-screening following any update to those lists;
- review, and where necessary, update of the customer's CDD information and risk rating at intervals proportionate to risk and upon any trigger event; and
- verification of the customer's continued identity and address information where doubts arise as to the accuracy of previously obtained data.

Alerts generated through monitoring are reviewed by the Compliance Officer, or delegated trained staff, and the outcome of the review — including any decision to escalate, restrict, or report — is documented and retained.

5.6 Reliance on Third Parties to Perform Customer Due Diligence

The Company relies on SumSub, a specialized identity verification and KYC technology provider, to perform certain technical elements of the customer identification and verification process as part of its CDD measures. This includes document authentication, biometric/liveness verification, database checks, and elements of sanctions and PEP screening carried out through the SumSub platform.

This reliance arrangement is subject to the following safeguards: (i) the third party is subject to data protection and operational standards consistent with those expected of a regulated identity-verification provider; (ii) a written agreement is in place with SumSub setting out the respective responsibilities of the parties; (iii) the Company can obtain, immediately upon request, copies of the identification and verification data and any other relevant CDD documentation held by SumSub; and (iv) the Company retains ultimate responsibility for compliance with its AML/CTF

obligations, regardless of the reliance placed on SumSub. The Compliance Officer is responsible for assessing and approving the SumSub arrangement, and for reviewing it periodically thereafter.

5.7 Reporting of Unusual Transactions

All directors, officers, and employees are required to report immediately to the Compliance Officer any transaction, pattern of transactions, or customer behavior that they know, suspect, or have reasonable grounds to suspect may be related to ML/TF/PF (“internal escalation”). Internal escalations are assessed by the Compliance Officer against objective and subjective risk indicators relevant to remote gaming, such as refusal to provide source-of-funds information, third-party funding, structuring of deposits or withdrawals, unusual win/loss patterns, or matches against sanctions, PEP, or adverse-media sources.

Where the Compliance Officer concludes, following this assessment, that a transaction or attempted transaction is unusual within the meaning of Curaçao law, the Company will report it to the Financial Intelligence Unit Curaçao (FIU Curaçao / MOT) without delay and in the prescribed format — regardless of the amount involved, and regardless of whether the underlying transaction was completed, refused, or merely attempted. Employees are strictly prohibited from disclosing to the customer, or to any third party, that a report has been made, is being considered, or has been requested by the authorities (“tipping-off”). All internal escalations and external reports, together with the supporting rationale, are documented and retained in accordance with the Company’s record-keeping obligations.

5.8 Anti-Money Laundering Compliance Program

The Company maintains a risk-based AML/CTF Compliance Program designed to meet, at a minimum, the standards required under Curaçao law and the conditions of its CGA license. The Program includes:

- the appointment of a Compliance Officer (MLRO) with sufficient seniority, independence, and resources to discharge AML/CTF responsibilities, and a deputy to ensure continuity;
- the Business Risk Assessment, Customer Risk Assessment, Customer Acceptance Policy, CDD, ongoing monitoring, and reporting procedures described in this Policy;
- a procedure for the immediate blocking, restriction, or closure of a customer’s account where there is a suspicion of ML/TF/PF, pending further investigation or instruction by the FIU Curaçao or another competent authority; where an account is blocked on this basis, no withdrawal of funds will be permitted, and the matter will be escalated internally and, where appropriate, reported externally, without informing the customer of the underlying suspicion;
- independent testing or audit of the Program at least annually, with findings reported to senior management;
- a documented training program ensuring that all relevant staff receive AML/CTF training upon induction and at least annually thereafter, covering applicable laws, this Policy, red-flag indicators specific to remote gaming, and individual reporting obligations;

- retention of CDD documentation, transaction records, risk assessments, and reports for the minimum period required under Curaçao law, and in any case no less than five (5) years following the end of the business relationship or the date of the transaction, whichever is later; and
- a governance structure ensuring that the Compliance Officer reports periodically to senior management and the Board on the effectiveness of the Program, emerging risks, and relevant regulatory developments.

6. Compliance and Consequences of Non-Compliance

Compliance with this Policy is mandatory for all individuals within its scope. Failure to comply — including failure to escalate a known or suspected unusual transaction, tipping-off a customer, or circumventing CDD or sanctions-screening requirements — may result in disciplinary action, up to and including termination of employment or contract.

Beyond internal consequences, non-compliance with AML/CTF obligations may expose the Company and the individuals concerned to regulatory enforcement action by the Curaçao Gaming Authority, including fines, conditions, suspension, or revocation of the Company's gaming license; criminal liability under Curaçao's AML/CTF and penal legislation; and reputational and financial harm to the Company. Employees who, in good faith, report a suspicion or escalate a concern under this Policy will not be subject to any adverse consequence for having done so.

7. Related Information

This Policy should be read together with the Company's:

- Customer Risk Assessment Procedure and Customer Acceptance Policy;
- Sanctions and PEP Screening Procedure;
- Transaction Monitoring Procedure;
- Record-Keeping Procedure;
- Staff AML/CTF Training Procedure; and
- Business Risk Assessment document.

It is also informed by, among others: the National Ordinance on Games of Chance (Landsverordening op de kansspelen); the National Ordinance on the Reporting of Unusual Transactions (Landsverordening melding ongebruikelijke transacties); the AML/CTF guidelines and directives issued by the Curaçao Gaming Authority; applicable sanctions regulations in force in Curaçao; and the FATF Recommendations as they apply to the gaming sector.

8. Contact Information

For any questions regarding this Policy, please contact:

Company	Momo Entertainment B.V.
CGA License Number	OGL/2024/940/0485
Department	Compliance Department
Address	Schottegatweg Oost 10, United 1-9, Bon Bini Business Center, Willemstad, Curaçao
Email	info@momoentertainmentbv.com
Phone	+306976465522
Compliance Officer (MLRO)	Spyridon Tagkas

9. Policy History

This is the initial issuance of the Company's AML/CTF Policy. Future revisions will be logged below, with version number, effective date, and a summary of the changes made.

Version	Effective Date	Summary of Changes
1.0	18 June 2026	Initial issuance of the AML/CTF Policy.

10. Policy URL

This Policy is made available on the Company's corporate website at <https://momoentertainmentbv.com/>. The Company's CGA license (No. OGL/2024/940/0485) is also displayed on its operating brand website(s), including <https://www.flukyone.com/>.