

MOMO ENTERTAINMENT B.V.

Operational Manual

Online Gaming Operations — All Licensed Platforms

Company	Momo Entertainment B.V.
Document Title	Operational Manual
Applies To	All platforms and websites operated under the Company's CGA licence
Jurisdiction	Curaçao
Regulatory Authority	Curaçao Gaming Authority (CGA)
Version	1.0
Effective Date	January 1, 2025
Next Review Date	January 1, 2026
Owner	Compliance & Operations Department
Classification	Confidential — Internal Use Only

1. Introduction

Momo Entertainment B.V. (hereinafter "the Company") is a licensed online gaming operator incorporated in Curaçao and regulated by the Curaçao Gaming Authority (CGA). The Company operates multiple online gaming platforms and websites under a single CGA licence, offering products and services including casino games, sports betting, live gaming, and related entertainment.

This Operational Manual (hereinafter "the Manual") sets out the policies, procedures, standards, and responsibilities that govern the day-to-day operations of the Company across all its licensed platforms. It is designed to ensure that operations are conducted in a consistent, compliant, fair, and efficient manner, regardless of the specific platform through which services are delivered.

This Manual is a living document and must be read in conjunction with the Company's full suite of regulatory and internal policies, including the AML/CTF Policy, Responsible Gaming Policy, and Player Complaints Policy. All staff, contractors, platform operators, and relevant third parties operating under the Company's licence are required to familiarise themselves with and adhere to the standards set out herein.

1.1 Scope

This Manual applies to:

- All employees, officers, and directors of the Company.
- All platform operators, white-label partners, and affiliated brands operating under the Company's CGA licence.
- All third-party service providers engaged in operations relevant to this Manual, including software providers, payment processors, and KYC/AML solution providers.

1.2 Regulatory Framework

The Company operates under the regulatory framework of the Curaçao Gaming Authority and is required at all times to comply with:

- The CGA Master Licence and all sub-licence conditions.
- The National Ordinance on the Identification of Clients when Rendering Financial Services.
- The National Ordinance on the Reporting of Unusual Transactions.
- All applicable CGA guidelines, circulars, and directives.
- International standards and best practices, including FATF Recommendations.

2. Corporate Structure and Governance

2.1 Company Overview

Legal Name	Momo Entertainment B.V.
Registration Number	160871
Registered Address	Schottegatweg Oost 10, Unit 1-9, Bon Bini Business Center, Willemstad, Curaçao
Contact Email	info@momoentertainmentbv.com
Licence Type	Curaçao Gaming Authority (CGA) Licence
Business Activity	Online Gaming — Casino, Sports Betting, and Related Services

2.2 Governance Structure

The Company is governed by its Board of Directors, which holds ultimate responsibility for the Company's strategic direction, regulatory compliance, and risk management. The Board is supported by the following operational departments:

Department / Function	Primary Responsibilities
Board of Directors	Ultimate accountability for compliance, strategy, and governance. Approval of policies and material decisions.
Compliance & Operations	Day-to-day regulatory compliance, AML/CTF programme, operational oversight across all platforms.
Customer Support	Player onboarding assistance, complaint handling, responsible gaming tool activation.
Finance & Payments	Payment processing, financial reporting, fraud monitoring, invoicing.
Technology & IT	Platform infrastructure, cybersecurity, software maintenance, data integrity.
Marketing	Player acquisition, promotional campaigns, affiliate management, responsible advertising.
Risk & Fraud	Transaction monitoring, player risk assessment, fraud detection and prevention.

2.3 Key Roles and Responsibilities

Compliance Officer

The Compliance Officer is the designated senior officer responsible for implementing and maintaining the Company's AML/CTF programme, overseeing regulatory compliance across all platforms, acting as the primary point of contact with the CGA, supervising KYC and EDD

processes, and ensuring staff training is conducted and recorded. The Compliance Officer reports directly to the Board of Directors.

Platform Operators

Each platform or brand operating under the Company's CGA licence must designate a responsible Platform Manager who is accountable for the operational integrity of that platform, compliance with this Manual and all Company policies, escalation of compliance issues to the Company's Compliance Officer, and timely submission of operational reports.

3. Player Registration and Know Your Customer (KYC)

3.1 Registration Requirements

All players must complete the registration process on a licensed platform before accessing any gaming services or depositing funds. The minimum information required at registration is:

- Full legal name.
- Date of birth (player must be 18 years of age or older, or the minimum legal age in their jurisdiction of residence if higher).
- Residential address.
- Email address.
- Username and secure password.
- Agreement to the platform's Terms and Conditions and this Company's policies, including the Responsible Gaming Policy.

Players are required to confirm that all information provided is accurate, complete, and up to date. Submission of false or misleading information is a breach of the Terms and Conditions and may result in account suspension or closure.

3.2 Age Verification

Age verification is mandatory for all players and must be completed before a player is permitted to make a first deposit or access real-money games. Age verification is conducted through:

- Self-declaration of date of birth at registration (first level).
- Documentary verification as part of the KYC process — the player must provide a valid government-issued photo identification document confirming their date of birth.

Any player for whom age verification has not been completed will have their account restricted to free-play mode only. Real-money deposits and withdrawals will be blocked until verification is completed.

3.3 KYC Procedure

The Company applies a risk-based KYC process to all players. KYC is triggered at account opening and at defined deposit thresholds. The KYC tiers are as follows:

KYC Tier	Trigger	Documents Required
Standard KYC	Account registration / first deposit	Government-issued photo ID (passport, national ID card, or driving licence) + Proof of address (utility bill or bank statement, not older than 3 months)
Enhanced KYC	Cumulative deposits exceed EUR 2,000 or high-risk indicators detected	Source of funds declaration + Additional supporting documentation (e.g. payslip, bank statement)

Full EDD	Cumulative deposits or withdrawals exceed EUR 10,000 OR PEP / high-risk jurisdiction identified	Full source of wealth verification + Senior management sign-off + Periodic review every 12 months
----------	---	---

3.4 Sanctions and PEP Screening

All players are screened against applicable international and domestic sanctions lists and Politically Exposed Persons (PEP) databases at the point of registration and on an ongoing basis. Screening is conducted against:

- OFAC Specially Designated Nationals (SDN) list.
- EU Consolidated Sanctions List.
- UN Security Council Sanctions List.
- Curaçao government-mandated sanctions lists.
- PEP databases including family members and close associates.

Any positive match is escalated immediately to the Compliance Officer. Confirmed sanctions matches result in immediate account suspension, freezing of funds, and reporting to the relevant Curaçao authorities. PEP matches trigger Enhanced Due Diligence and require Board-level approval to proceed.

3.5 Rejected and Restricted Players

Players shall not be accepted onto any licensed platform in the following circumstances:

- The player is under the minimum age requirement.
- The player resides in a jurisdiction listed on the Company's Restricted Countries List.
- The player is identified as a confirmed match on a sanctions list.
- The player has an active self-exclusion on any platform under the Company's licence.
- The player has previously had their account closed for fraud, abuse, or AML-related reasons.

4. Account Management

4.1 Account Opening

Each player is permitted to hold one (1) account per licensed platform. The existence of multiple accounts on the same platform by the same individual is prohibited and may result in the closure of all associated accounts and forfeiture of any bonuses obtained through duplicate accounts.

4.2 Account Verification Status

Player accounts are managed across the following verification statuses:

Status	Description
Unverified	Account registered but KYC not yet completed. Player may access free-play only. Deposits and withdrawals blocked.
Partially Verified	Basic KYC completed. Limited deposit and withdrawal access until full verification is completed.
Fully Verified	All required KYC documentation submitted and approved. Full access to platform features.
Under Review	Account flagged for enhanced review. Access may be restricted pending investigation.
Suspended	Account temporarily suspended pending compliance review, suspected fraud, or investigation.
Closed	Account permanently closed. Player may not re-register on the same platform.

4.3 Account Closure

Players may request account closure at any time by contacting Customer Support. Upon receipt of a closure request, the platform must:

1. Process any pending withdrawal of the player's real-money balance within the standard withdrawal timeframe.
2. Confirm the closure to the player in writing via email.
3. Retain all account data and records for a minimum of five (5) years in accordance with the Company's record-keeping obligations.
4. Flag the account to prevent re-registration where the closure was initiated due to responsible gaming concerns.

5. Payment Operations

5.1 Accepted Payment Methods

The Company and its licensed platforms accept a range of payment methods subject to regulatory approval, KYC status, and jurisdiction restrictions. Accepted methods may include:

- Credit and debit cards (Visa, Mastercard — subject to applicable restrictions).
- Bank transfers.
- Electronic wallets (e-wallets) approved by the Company.
- Cryptocurrency payments where explicitly permitted and subject to enhanced due diligence.

All payment methods must be pre-approved by the Finance Department. Third-party payment processors must be subject to formal written agreements and have undergone appropriate due diligence by the Company.

5.2 Deposit Procedures

All deposits must be made from a payment method registered in the player's own name. Third-party deposits are strictly prohibited. Before processing a deposit, the platform must confirm that:

- The player's account is in good standing (not suspended or restricted).
- The player's KYC status is sufficient for the deposit amount.
- The deposit does not originate from a jurisdiction on the Restricted Countries List.
- The player has not exceeded any self-imposed deposit limits.

5.3 Withdrawal Procedures

Withdrawals are processed in accordance with the following standards:

- Withdrawals are paid to the same payment method used for the corresponding deposit, wherever possible, to prevent money laundering.
- Full KYC verification must be completed before any withdrawal is processed.
- Withdrawal requests are reviewed by the Finance and Risk teams within two (2) working days.
- Withdrawals may be placed on hold pending AML review, additional KYC, or fraud investigation.
- Maximum withdrawal limits per transaction and per period are set by each platform and communicated clearly to players in the Terms and Conditions.

5.4 Fraud Prevention

The Risk & Fraud team monitors all transactions for indicators of fraudulent activity, including:

- Use of stolen or unauthorised payment methods.
- Chargebacks and payment reversals.
- Multiple accounts using the same payment method.

- Unusual deposit and withdrawal patterns inconsistent with the player's profile.
- Collusion or bonus abuse schemes.

Accounts where fraud is suspected will be suspended immediately pending investigation. Confirmed fraud cases will result in permanent account closure, forfeiture of balances where legally permissible, and reporting to relevant authorities.

6. Game Operations

6.1 Game Portfolio

The Company's licensed platforms may offer the following categories of games and products, subject to the applicable licence conditions:

- Online casino games (slots, table games, video poker, specialty games).
- Live dealer casino games.
- Sports betting and virtual sports.
- Other gaming products approved under the Company's CGA licence.

6.2 Game Integrity and Fairness

All games offered on the Company's platforms must meet the following standards:

- Random Number Generators (RNGs) must be certified and regularly audited by an independent, accredited testing laboratory approved by the CGA.
- Game rules, odds, Return to Player (RTP) percentages, and bet limits must be clearly displayed to players within the game interface or accessible documentation.
- No game may be altered, manipulated, or configured in a manner that is deceptive or unfair to players.
- Technical malfunctions must be logged, reported, and investigated. Where a malfunction voids a game round, affected players must be notified and refunded.

6.3 Game Malfunctions

In the event of a game or platform malfunction, the following procedure applies:

5. The platform immediately logs the incident, recording the time, affected game(s), player accounts involved, and nature of the fault.
6. Affected game rounds are voided and bets refunded to player accounts within two (2) working days.
7. The Platform Manager notifies the Compliance Officer and the Technology team.
8. A root cause analysis is conducted, and corrective action is documented.
9. Where the malfunction may have a material impact on game integrity, the CGA is notified.

6.4 Bonus and Promotions

All bonuses and promotional offers must comply with the following requirements:

- All bonus terms and conditions — including wagering requirements, time limits, eligible games, and maximum cashout amounts — must be clearly stated and accessible to players before the bonus is accepted.
- Bonus offers must not be misleading or deceptive.
- Bonuses must not be offered to self-excluded players or players with active responsible gaming restrictions.

- Bonus abuse (including multi-accounting for promotional purposes) is prohibited and may result in account closure and forfeiture of associated winnings.
- All promotional campaigns must be reviewed and approved by the Compliance team before launch.

7. AML/CTF Operational Procedures

This section sets out the operational implementation of the Company's AML/CTF Policy. All procedures below must be read in conjunction with the full AML/CTF Policy document.

7.1 Transaction Monitoring

All platforms operated under the Company's licence are required to implement automated transaction monitoring systems capable of:

- Detecting and flagging deposits, withdrawals, and gaming transactions that meet or exceed defined thresholds.
- Identifying patterns consistent with money laundering typologies, including structuring, rapid cycling, and source-of-funds inconsistencies.
- Generating automated alerts for review by the Risk and Compliance teams.

All alerts generated by the transaction monitoring system must be reviewed and documented. Alerts must be resolved within five (5) working days of generation. Unresolved or escalated alerts must be reported to the Compliance Officer immediately.

7.2 Suspicious Transaction Reporting

Where reasonable grounds to suspect money laundering or terrorist financing are identified, the following steps must be taken:

10. The relevant staff member or platform operator completes an internal Suspicious Activity Report (iSAR) and submits it to the Compliance Officer without delay.
11. The Compliance Officer reviews the iSAR within two (2) working days and makes a determination as to whether to file an Unusual Transaction Report (UTR) with the Curaçao Financial Intelligence Unit (FIU).
12. Where a UTR is to be filed, it is submitted to the FIU in the prescribed format and within applicable statutory timelines.
13. The decision to file or not file is documented and retained on record.
14. The customer must not be informed ("tipped off") that a report has been or may be filed.
15. Where a UTR is filed in relation to a specific account, the account must be placed under enhanced monitoring or suspended, as appropriate.

7.3 Account Freezing

Accounts must be frozen immediately in any of the following circumstances:

- A confirmed match against a sanctions list is identified.
- Credible suspicion of money laundering or terrorist financing has been identified and verified by the Compliance Officer.
- A UTR has been filed and the Compliance Officer determines that continued account operation poses an unacceptable risk.
- A request to freeze funds is received from the Curaçao FIU or another competent authority.

All account freezes must be documented. Frozen account balances must not be disbursed without the written authorisation of the Compliance Officer and, where applicable, the relevant authority.

8. Responsible Gaming Operations

This section sets out the operational implementation of the Company's Responsible Gaming Policy across all licensed platforms.

8.1 Responsible Gaming Tools — Operational Requirements

All licensed platforms must make the following responsible gaming tools available and functional at all times:

Tool	Activation Method	Processing Time
Deposit Limits	Player self-service via account settings or Customer Support	Reduction: immediate. Increase: minimum 24-hour cooling-off period.
Loss Limits	Player self-service via account settings or Customer Support	Reduction: immediate. Increase: minimum 24-hour cooling-off period.
Session Time Limits	Player self-service via account settings	Immediate.
Reality Checks	Player self-service via account settings	Immediate.
Time-Out	Customer Support or account settings	Immediate upon activation. Player notified by email.
Self-Exclusion	Customer Support request	Processed within 24 hours. Applied across all licensed platforms.

8.2 Identifying At-Risk Players

Customer Support and the Risk teams must monitor for the following behavioural indicators and escalate to the Compliance Officer where identified:

- Rapid and repeated deposit and loss cycles within a single session.
- Player communications expressing financial distress or gambling-related problems.
- Requests to remove or increase responsible gaming limits.
- Reversal of previously requested withdrawal ("withdrawal reversal" behaviour).
- Sustained play without breaks, particularly during unusual hours.

Where an at-risk player is identified, Customer Support must proactively reach out to the player, offer responsible gaming tools, and escalate the case to the Compliance Officer for assessment and potential account restriction.

8.3 Self-Exclusion — Cross-Platform Procedure

Self-exclusion requests are applied across all platforms operated under the Company's licence. The procedure is as follows:

16. Player submits a self-exclusion request via Customer Support on any licensed platform.
17. The platform receiving the request processes the exclusion on that platform within 24 hours and notifies the Company's Compliance Officer.
18. The Compliance Officer ensures the exclusion is applied to all other platforms under the Company's licence within 48 hours.
19. All marketing communications to the self-excluded player are ceased immediately.
20. The player's real-money balance is made available for withdrawal.
21. The self-exclusion is recorded and the record retained for a minimum of five (5) years.

9. Customer Support Operations

9.1 Service Standards

Customer Support is the primary point of contact for players on all licensed platforms. The following minimum service standards apply:

Standard	Requirement
Availability	Customer Support must be available at a minimum during standard business hours, five (5) days per week. 24/7 support is strongly recommended for all player-facing platforms.
Contact Channels	At minimum: email and live chat. Telephone support is encouraged.
Initial Response Time	All player queries and complaints must be acknowledged within 24 hours of receipt (or the next working day).
Resolution — Standard Queries	Simple queries resolved within three (3) working days.
Resolution — Formal Complaints	Substantive response within 14 calendar days; final decision within 28 calendar days.
Language	Support must be available in the primary language(s) of the platform's target markets.

9.2 Complaint Escalation

All complaints must be handled in accordance with the Company's Player Complaints Policy. The escalation hierarchy is as follows:

22. First-contact resolution by Customer Support agent.
23. Escalation to Senior Customer Support or Platform Manager for unresolved complaints.
24. Escalation to the Company's Compliance Officer for regulatory or AML-related complaints, or complaints unresolved at platform level.
25. Referral to CGA or ADR body for complaints unresolved within 28 calendar days.

10. Information Technology, Security, and Data Protection

10.1 Platform Infrastructure

All platforms operated under the Company's licence must meet the following infrastructure requirements:

- Hosting on secure, redundant servers with documented uptime SLAs.
- Regular penetration testing and vulnerability assessments, conducted at least annually by a qualified third party.
- Encrypted data transmission (SSL/TLS) for all player-facing interfaces.
- Segregation of player funds from operational funds.
- Regular and verified backups of all player data and transaction records.

10.2 Cybersecurity

The Technology team is responsible for maintaining the security posture of all platforms. Key cybersecurity requirements include:

- Implementation of multi-factor authentication (MFA) for all staff accessing backend systems.
- Role-based access controls (RBAC) limiting system access to the minimum required for each role.
- Regular staff cybersecurity awareness training.
- Documented incident response plan for cybersecurity breaches.
- Notification to the Compliance Officer and CGA in the event of a data breach that may affect player data or platform integrity.

10.3 Data Protection

The Company and all licensed platforms process player personal data in accordance with applicable data protection laws and the Company's Privacy Policy. Key obligations include:

- Collecting only the minimum personal data necessary for the provision of services and compliance obligations.
- Obtaining valid player consent for data processing where required.
- Retaining player data for a minimum of five (5) years following the end of the player relationship, or longer where required by applicable law.
- Responding to player data access, rectification, and erasure requests within applicable legal timeframes.
- Not selling or sharing player data with unauthorised third parties.

11. Marketing and Advertising Standards

11.1 Responsible Advertising

All marketing and advertising activities carried out by the Company or by platforms operating under its licence must comply with the following standards:

- All claims made in marketing materials must be accurate, clear, and not misleading.
- Bonus and promotional terms must be clearly stated, including all material conditions (wagering requirements, time limits, excluded games, etc.).
- Marketing must not be directed at minors or at individuals who have self-excluded.
- Marketing must not exploit vulnerable individuals or encourage excessive or irresponsible gambling.
- Responsible gaming messaging must be included in all promotional materials.

11.2 Affiliate Management

All affiliates promoting the Company's licensed platforms must operate under a formal Affiliate Agreement. Key requirements include:

- Affiliates must comply with this Manual's marketing standards and the Company's Responsible Gaming Policy.
- Affiliates must not direct traffic from restricted jurisdictions.
- Affiliates must not make false or exaggerated claims about winnings, odds, or platform features.
- The Marketing team conducts periodic reviews of affiliate activity and may terminate any affiliate agreement where standards are not met.

11.3 Marketing Approval

All marketing campaigns — including email campaigns, social media posts, paid advertising, and promotional offers — must be reviewed and approved by the Compliance team prior to launch to ensure compliance with regulatory requirements and Company standards.

12. Reporting and Record-Keeping

12.1 Internal Reporting

The following internal reports must be produced and submitted to the Compliance Officer and, where applicable, the Board of Directors:

Report	Frequency	Responsible Party
AML/CTF Compliance Report	Monthly	Compliance Officer
Suspicious Transaction / UTR Log	Monthly (or immediately upon filing)	Compliance Officer
KYC Status Report (by platform)	Monthly	Platform Manager / Compliance
Responsible Gaming Incidents Report	Monthly	Compliance Officer
Player Complaints Log	Monthly	Customer Support / Compliance
Financial & Payment Summary	Monthly	Finance Department
IT Security & Incident Report	Quarterly	Technology Team
AML/CTF Programme Audit	Annual	Independent Auditor
Business Risk Assessment Review	Annual	Compliance Officer

12.2 Record Retention

The Company maintains the following minimum record retention periods:

- Player KYC documentation and identity records: minimum five (5) years following the end of the business relationship.
- Transaction records (deposits, withdrawals, bets, winnings): minimum five (5) years.
- AML/CTF reports and UTRs filed with the FIU: minimum five (5) years.
- Player complaints and resolutions: minimum five (5) years.
- Employee training records: minimum three (3) years following the employee's departure.
- All records must be stored securely and be retrievable within a reasonable timeframe upon request from the Compliance Officer or a competent authority.

13. Staff Training

13.1 Training Programme

All staff in player-facing or compliance-relevant roles must complete mandatory training as follows:

Training Module	Audience	Frequency
AML/CTF Awareness	All staff	On induction + annually
KYC and CDD Procedures	Customer Support, Compliance, Risk	On induction + annually
Responsible Gaming	All player-facing staff	On induction + annually
Fraud Detection & Prevention	Customer Support, Finance, Risk	On induction + annually
Data Protection (GDPR/Privacy)	All staff	On induction + annually
Cybersecurity Awareness	All staff	Annually
Complaints Handling	Customer Support	On induction + annually

Training completion must be recorded and retained. The Compliance Officer is responsible for maintaining training records and ensuring all staff certifications are current.

14. Business Continuity and Incident Management

14.1 Business Continuity

The Company maintains a Business Continuity Plan (BCP) to ensure the continued operation of critical business functions in the event of a disruption. All licensed platforms must implement compatible continuity arrangements covering:

- Server redundancy and automated failover capabilities.
- Data backup and recovery procedures tested at least twice per year.
- Alternative communication channels for staff and player notification during incidents.
- Defined Recovery Time Objectives (RTOs) for all critical systems.

14.2 Incident Management

In the event of a significant operational or security incident, the following procedure applies:

26. The incident is identified and logged by the relevant team (Technology, Finance, Compliance, or Customer Support).
27. The incident is immediately escalated to the relevant Department Head and the Compliance Officer.
28. An incident response team is convened. Immediate containment measures are implemented.
29. The Board of Directors is informed of any material incident within four (4) hours.
30. The CGA is notified of any incident that materially affects player funds, data security, or game integrity, within the timeframe specified by the CGA.
31. A post-incident review is conducted within ten (10) working days, producing a written report with root cause analysis and corrective actions.

15. Compliance, Review, and Consequences of Non-Compliance

15.1 Compliance Obligations

Compliance with this Manual is mandatory for all individuals and entities within its scope. The Compliance Officer conducts periodic reviews of operational compliance across all licensed platforms, including site visits, document reviews, and data audits where applicable.

15.2 Non-Compliance

Failure to comply with the standards and procedures set out in this Manual may result in:

- Internal disciplinary action against employees, up to and including termination of employment.
- Suspension or termination of a platform's operating rights under the Company's licence.
- Regulatory action by the CGA, including fines, licence conditions, suspension, or revocation.
- Civil or criminal liability under applicable Curaçao and international law.

15.3 Manual Review

This Manual is subject to formal review at least annually by the Compliance Officer and senior management. The Manual will also be reviewed and updated promptly following:

- Material changes to the Company's business operations or platform portfolio.
- Changes to applicable laws, regulations, or CGA requirements.
- Significant operational incidents or compliance findings.
- Recommendations arising from independent audits.

16. Related Documents and Contact Information

16.1 Related Documents

This Manual must be read in conjunction with the following Company documents:

- AML/CTF Policy
- Responsible Gaming Policy
- Player Complaints Policy
- Privacy Policy
- Terms and Conditions (per platform)
- Software Services Agreements
- Affiliate Agreements
- Business Continuity Plan

16.2 Contact Information

Company	Momo Entertainment B.V.
Registered Address	Schottegatweg Oost 10, Unit 1-9, Bon Bini Business Center, Willemstad, Curaçao
Email	info@momoentertainmentbv.com
Responsible Department	Compliance & Operations Department

17. Version History

Version	Effective Date	Approved By	Summary of Changes
1.0	January 1, 2025	Board of Directors	Initial issue — new document.

This document is confidential and intended solely for internal use by Momo Entertainment B.V. and its authorised platform operators and personnel. Unauthorised distribution is strictly prohibited.