

BET N PLAY SOLUTION B.V.

COMPLIANCE POLICIES PACKAGE — VERSION 1.1

Registered address: Abraham Mendez Chumaceiro Boulevard 03, Willemstad, Curaçao
Curaçao Chamber of Commerce Number: 163749

Main Domain: GogoRoyal.com

Additional Approved Domains: apuestasroyal.com

Gaming Licence Number: OGL/2024/927/1070

Licence Issue Date: 21-October-2025

Licensing and Supervisory Authority: Curaçao Gaming Authority

Approved by: Managing Directors

Compliance Officer / MLRO: Elias Arturo Rodriguez Parra

Effective Date: 29-June-2026

Next Review Date: 29-December-2026

1. AML/CTF/CPF POLICY — VERSION 1.1

1.1 Policy Statement

Bet N Play Solution B.V. is committed to preventing the use of its gaming platform, player accounts, payment channels, products, services, domains and business relationships for money laundering, terrorist financing, proliferation financing, sanctions evasion, fraud, identity misuse, illegal gambling activity or any other financial crime.

This Policy applies to all domains, brands, platforms, player interfaces, mobile applications, payment channels, employees, directors, officers, outsourced service providers, affiliates, agents and intermediaries used by or under the control of Bet N Play Solution B.V. in connection with licensed remote games of chance.

Bet N Play Solution B.V. shall remain at all times the licensed operator of record and shall retain full regulatory, operational and compliance responsibility.

Nothing in this Policy shall be interpreted as authorising any transfer, lease, sublicense, assignment or third-party use of the Curaçao gaming licence.

1.2 Principal Legal and Regulatory Basis

This Policy is based primarily on the applicable laws, licence conditions, regulations, policies and guidelines of Curaçao, including:

1. National Ordinance on Games of Chance / Landsverordening op de Kansspelen;
2. National Ordinance on Identification when Rendering Services;
3. National Ordinance on the Reporting of Unusual Transactions;
4. Sanctions National Ordinance;
5. Kingdom Sanction Act;
6. Curaçao AML/CTF/CPF Regulations applicable to casinos and online gaming providers;
7. Curaçao Gaming Authority licence conditions, policies, procedures, guidelines and instructions;
8. FIU Curaçao reporting requirements, including goAML reporting.

International standards, including FATF Recommendations, EU AML standards, UN sanctions lists, OFAC, EU and UK sanctions lists, may be used as supplementary standards where appropriate, but they do not replace Curaçao law as the principal legal basis of this Policy.

1.3 Governance and Responsibility

The Board of Directors has ultimate responsibility for the effectiveness of the AML/CTF/CPF framework.

The Compliance Officer / MLRO shall:

1. act independently;
2. report directly to the Board of Directors;
3. have unrestricted access to player data, CDD files, transaction records, payment records and relevant systems;
4. review internal unusual transaction reports;
5. decide whether an external report must be filed with FIU Curaçao;
6. maintain records of unusual transactions, investigations, blocked accounts and reports;
7. design and maintain AML procedures;
8. organise staff training;
9. monitor legal and regulatory developments;
10. prepare periodic AML reports to management;
11. cooperate with CGA, FIU Curaçao, auditors and competent authorities.

No shareholder, director, employee, supplier, affiliate or third party may interfere with the independent decision-making of the MLRO regarding unusual transaction reporting or AML investigations.

1.4 Business Risk Assessment

Bet N Play Solution B.V. shall maintain a documented Business Risk Assessment covering:

1. products and games offered;
2. countries and markets served;
3. player profile and behaviour;
4. payment methods;
5. use of fiat currencies, virtual currencies or tokens;
6. payment intermediaries;
7. software and technology risks;
8. third-party providers;
9. affiliates and marketing partners;
10. fraud and bonus abuse risks;
11. sanctions and high-risk jurisdictions;
12. Venezuela-related risks, where applicable;
13. responsible gaming and vulnerable player overlap;
14. cybersecurity and data risks.

The Business Risk Assessment shall be reviewed at least annually and whenever there is a material change in the business model, domains, payment methods, suppliers, ownership, technology or target markets.

1.5 Customer Risk Assessment

Each player shall be risk-rated at onboarding and during the relationship.

Risk factors include:

1. country of residence;
2. nationality;
3. payment method;
4. use of virtual assets;
5. transaction volume;
6. deposit and withdrawal behaviour;
7. PEP status;
8. sanctions or adverse media;
9. use of multiple accounts;
10. suspicious IP, device or geolocation patterns;
11. unusual gaming activity;
12. source of funds concerns;
13. chargebacks or fraud indicators;
14. responsible gaming concerns that may also indicate financial distress or unusual conduct.

Risk categories shall be Low, Medium and High.

1.6 Customer Acceptance Policy

Bet N Play Solution B.V. shall not accept or shall terminate players who:

1. are under the legal gambling age;
2. are located in prohibited jurisdictions;
3. are subject to sanctions;
4. provide false, misleading or incomplete information;
5. refuse required CDD or EDD documentation;
6. use third-party accounts or payment methods without acceptable justification;
7. are suspected of money laundering, terrorist financing, proliferation financing, fraud or sanctions evasion;
8. are self-excluded or otherwise identified as vulnerable where participation must be restricted;
9. use the platform in breach of applicable law.

1.7 Customer Due Diligence

The Company shall apply CDD on a risk-based basis and in accordance with Curaçao requirements.

At account registration, the Company shall collect at least:

1. full legal name;
2. date of birth;
3. residential address;
4. country of residence;
5. email and/or phone number;
6. acceptance of Terms and Conditions;
7. confirmation that the player is not underage and is not prohibited from gambling.

The Company shall verify identity and apply additional CDD before permitting withdrawals, when regulatory thresholds are met, when risk factors arise, when suspicious or unusual activity is detected, or when otherwise required by law, regulation, internal policy or MLRO decision.

CDD may include:

1. government-issued identity document;
2. proof of address;
3. nationality;
4. place of birth;
5. tax identification number, where applicable;
6. payment method ownership verification;
7. source of funds;
8. source of wealth;
9. PEP, sanctions and adverse media screening.

The Company shall apply the Curaçao AML threshold of NAf. 4,000 or any other applicable threshold issued by the competent authority for CDD purposes. The threshold must be monitored according to applicable Curaçao rules and shall not be replaced by USD thresholds unless expressly permitted by applicable law or regulatory guidance.

1.8 Enhanced Due Diligence

EDD shall apply to:

1. PEPs, relatives and close associates;
2. players from high-risk jurisdictions;
3. players using high-risk payment methods;
4. players using virtual assets;
5. unusual transaction patterns;
6. high-value players;
7. players with inconsistent source of funds;
8. adverse media matches;
9. players linked to fraud, chargebacks or account abuse;
10. any case where the MLRO determines enhanced review is required.

EDD may include:

1. enhanced identity verification;
2. source of funds documentation;
3. source of wealth documentation;
4. senior management or MLRO approval;
5. enhanced transaction monitoring;
6. shorter review periods;
7. restrictions on deposits or withdrawals;
8. termination of the relationship where risk cannot be mitigated.

PEPs are not automatically prohibited unless sanctions, unacceptable risk or other legal grounds apply. However, PEPs require EDD and approval before continuing the relationship.

1.9 Payment Methods, Player Funds and Currency Controls

All payment transactions between the Company and the player shall be carried out exclusively through the player account.

Player funds, including deposits, winnings and balances owed to players, shall be held under appropriate segregation or ring-fencing measures.

If intermediaries are used for player transactions, the Company shall ensure that:

1. the intermediary is identified, verified and approved internally;
2. the intermediary is lawfully permitted to provide the relevant service;
3. the relationship is governed by a written agreement;
4. all transactions are recorded in identifiable accounts;
5. player-level reconciliation is possible;
6. the Company retains access to all relevant records;
7. the intermediary does not act as an operator;
8. the intermediary does not use or represent that it uses the gaming licence;
9. the intermediary does not make final decisions on deposits, withdrawals, account closure, KYC, AML, complaints or responsible gaming;
10. CGA approval or notification is obtained where required.

The Company shall not exchange currencies in the player account or otherwise, unless expressly permitted by applicable regulation. Where fiat or virtual currencies are accepted, the Company shall ensure that the currencies are permitted, traceable and consistent with applicable licence conditions.

Winnings shall be paid in the same currency used to participate in the relevant game, unless otherwise permitted by applicable law and disclosed in the Terms and Conditions.

1.10 Virtual Assets and Venezuela-Related Payment Risk

Where the Company accepts virtual currencies, crypto-assets, stablecoins or payment methods linked to Venezuela or other higher-risk markets, the Company shall conduct a documented risk assessment covering:

1. legality of the payment channel;
2. payment processor or intermediary due diligence;
3. sanctions exposure;
4. source of funds;
5. conversion risk;
6. currency control risk;
7. traceability;
8. wallet ownership;
9. blockchain monitoring, where applicable;
10. reconciliation between the payment received and the player account balance;
11. regulatory notification or approval requirements.

The Company shall not permit informal cash collection, personal accounts, unverified intermediaries, undocumented conversion, or settlement structures that prevent player-level traceability.

1.11 Ongoing Monitoring

The Company shall monitor player activity on an ongoing basis, including:

1. deposits and withdrawals;
2. gaming transactions;
3. payment methods;
4. velocity and frequency;
5. bonus abuse;
6. account changes;
7. IP/device/geolocation;
8. unusual deposits followed by limited play and withdrawal;
9. use of third-party payment instruments;
10. transactions inconsistent with the player's profile.

The Company shall maintain automated and manual controls proportionate to risk.

1.12 Reporting of Unusual Transactions

The Company shall report unusual transactions to FIU Curaçao through the applicable reporting system when required.

The Company shall apply objective and subjective indicators under Curaçao law.

The Company shall apply the Curaçao unusual transaction threshold of NAf. 5,000 or any other applicable threshold issued by the competent authority. The threshold shall not be replaced by a USD threshold unless expressly permitted by law or regulatory guidance.

Internal reports to the MLRO must be made immediately and in any event within the internal reporting timeframe established by the Company.

External reports to FIU Curaçao shall be filed without delay where reporting is required.

1.13 Prohibition of Tipping-Off

No director, employee, officer, contractor, supplier, affiliate or representative may inform a player or any third party that:

1. an internal AML investigation is ongoing;
2. a report has been or may be filed with FIU Curaçao;
3. a player account is under AML review;
4. a competent authority has requested information;
5. a transaction has been classified as unusual.

1.14 Record Keeping

The Company shall retain AML records for at least five years, or longer where required by applicable law.

Records shall include:

1. player identification;
2. CDD and EDD documents;
3. risk assessments;
4. transaction records;
5. payment intermediary records;
6. unusual transaction investigations;
7. FIU reports;
8. sanctions screening;
9. training records;
10. audit reports;
11. management approvals.

1.15 Training

All relevant employees, managers, directors, customer support staff, payment staff, compliance staff, affiliates and contractors shall receive AML training appropriate to their function.

Training shall be provided at onboarding and at least annually.

1.16 Independent Audit

The AML/CTF/CPF framework shall be subject to independent review at least annually or as otherwise required by the CGA or applicable law.

The audit shall assess:

1. policies and procedures;
2. CDD files;
3. transaction monitoring;
4. FIU reporting;
5. sanctions screening;
6. payment intermediaries;
7. record keeping;
8. training;
9. remediation of prior findings;
10. website and Terms and Conditions alignment.

1.17 Website Alignment

The public AML page shall be consistent with this Policy. It shall not present European Union or Belgian law as the principal legal basis of the Company's AML obligations. Those frameworks may only be referenced as supplementary standards where appropriate.



Andres Galperin Gomez
29/06/2026



Michael Balakian Casciani
29/06/2026



Rudsel Lucas o.b.o Dempel Directors B.V.
29/06/2026



Rudsel Lucas o.b.o Waaigat Directors B.V.
29/06/2026