



**Anti-Money Laundering ,
Combating Financing of Terrorism and Financing of Proliferation
of weapon and mass destruction (AML/CFT/CFP) Policy**

Legal Entity: PP Solutions N.V.

May 1st, 2025

Version: 2025.1.0.



Anti-Money Laundering (AML) and Counter-Terrorism Financing (CTF) Policy Summary ***(Aligned with Curaçao Licence 8048/JAZ2023-031 requirements)***

Popiplay is committed to operating in strict compliance with Curaçao's anti-money laundering (AML), counter-terrorism financing (CTF), and counter-proliferation financing (CPF) regulations, including NOIS, NORUT, the Sanctions National Ordinance, the Kingdom Sanction Act, and the FATF Recommendations.

The policy outlines the company's approach to:

- Business Risk Assessment and Customer Risk Assessment to identify and mitigate financial crime risks.
- Customer Due Diligence (CDD), including verification of identity, beneficial ownership, and ongoing monitoring.
- Sanctions and PEP screening to prevent exposure to sanctioned entities or politically exposed persons.
- Reporting of Unusual Transactions to the Financial Intelligence Unit (FIU) Curaçao via the goAML portal.
- Employee training, independent audits, and the appointment of a Compliance Officer to maintain program effectiveness.

Non-compliance with this policy can result in internal disciplinary actions, reputational harm, and regulatory penalties.

This policy will be reviewed annually and updated to reflect regulatory or operational changes.



Anti-Money Laundering (AML) and Counter-Terrorism Financing (CTF) Policy Template

1. Policy Statement

PP Solutions N.V. is committed to conducting its business in accordance with all applicable Anti-Money Laundering (AML), Counter-Terrorism Financing (CTF), and Counter-Proliferation Financing (CPF) laws and regulations in the jurisdiction of Curaçao, including compliance with the National Ordinance on Identification when rendering Services (NOIS), the National Ordinance on the Reporting of Unusual Transactions (NORUT), the Sanctions National Ordinance, the Kingdom Sanction Act, and adherence to FATF and CFATF standards. This policy applies to all employees, contractors, third-party suppliers, and agents.

The Company will not continue established relationships with participants whose conduct gives rise to suspicion of involvement with illegal activities. The company will seek to terminate any participant relationship where the participant's conduct gives reasonable cause to believe or suspect involvement with illegal activities. Any such termination shall follow the reporting of the suspicion to the Curacao Financial Intelligence Unit (FIU) and thereafter shall be undertaken in conjunction with the relevant Government of Curacao authorities and in accordance with Curacao custom and practice to avoid any risk of the Company committing a tipping-off offence.

2. Purpose

This policy aims to prevent PP Solutions N.V. from being connected to or used for money laundering, terrorist financing, and proliferation financing activities. It ensures that we adhere to the applicable legal, regulatory, and international standards, protecting our reputation and the integrity of the global financial system.

3. Audience

- All employees
- Contractors and consultants
- Subcontractors
- Third-party service providers and agents

4. Definitions

Definitions have been aligned with Curaçao Regulations.

- Casino: Land-based and online casinos.
- FATF: Financial Action Task Force
- CFATF: Caribbean Financial Action Task Force
- Financial Transaction: Deposit, withdrawal, or transfer involving monetary value.
- FIU: Financial Intelligence Unit Curaçao
- Politically Exposed Person (PEP)
- Source of Funds and Source of Wealth
- Beneficial Ownership
- Unusual Transaction

5. Policy Implementation

5.1 Business Risk Assessment (BRA)

- Conduct a documented BRA annually.
- Identify ML/TF/FP risks linked to products, services, geographical locations, delivery channels, and technologies.
- Update risk assessments based on changes in products, services, technology, or regulation.



5.2 Customer Risk Assessment (CRA)

- Conduct CRA at the time of account creation or first transaction.
 - CDD process for all UBOs and responsible persons/signatories
 - If CDD process shows any irregularities, the decision is negative
 - If CDD process shows inconsistencies, the customer is asked to provide additional information, If additional information is satisfactory, we proceed, if not, the decision is negative.
- Assign a risk category (low, medium, high).
 - Risk category is connected to the country or origin in question, jurisdiction of a legal entity as well as UBOs' jurisdictions. Each customer will be assigned a category, and depending on the level, it will be monitored more or less frequently (every 3 (three) or every 6 (six) months)
- Consider factors such as customer profile, country of origin, product usage, payment methods (banking).

5.3 Customer Acceptance Policy (CAP)

- Define acceptance criteria based on CRA outcomes.
- Refuse service where high-risk criteria cannot be mitigated.
- Special scrutiny for PEPs, high-risk countries, and anonymous funding methods.

5.4 Customer Due Diligence (CDD)

- Identification and verification of customer identity is done through the CDD procedure, documents are collected and securely stored, all documents are requested in English, or in original with an official translation in English.
 - Compliance Form: We provide our future customers with a Compliance Form to be filled in and signed by an authorized person. The Form also lists documentation, which is part of the CDD. All listed documents must be provided, or CDD will not have been completed.
 - Company check:
 - Following documentation is collected before any contract is signed with the customer (Note: all documents have to be less than 3 (three) months old): Excerpt from the Official Business Registry, MoA/AoI,



Certificate of Good Standing or a similar document, Shareholder Register, signed and dated, Proof of Domain ownership, connected to either a UBO or the legal entity, Authorized Signatories List, License Certificate;

- Personal check:
 - The following documentation is collected before any contract is signed with the customer (Note: all documents have to be less than 3 (three) months old): Official notarized copies of UBO Passports or ID cards, Official notarized copies of UBO utility bill, Official notarized copies of Director Passports or ID cards, Official notarized copies of a Director's utility bills.
- Sanctions and PEP screening before and during the relationship (if it is established)Enhanced Due Diligence (EDD) for high-risk customers. If for any reason, above CDD check returns unfavorable information, we may request additional documentation, and comments from customer on the findings. Depending on the results, we may designate a customer to be acceptable, but monitored monthly, or not acceptable, in which case CDD is not accepted.

5.5 Ongoing Monitoring

- Monitor transactions and behavior throughout the business relationship. Transactions need to match the Invoiced amounts, which is prior confirmed by both sides. Transactions need to match the sender's details. If any of the two is not met, the transaction is rejected and returned to the sender. Our back office us used for tracking.
- Refresh CDD documentation every 6 (six) months for no risk/low risk customers. For high-risk customers, CDD documentation will be requested every 3 (three)months.
- Identify and report unusual patterns or deviations via portal

5.6 Reliance on Third Parties for CDD

- Permissible only with regulated third parties.
- Maintain full responsibility for compliance.
- Formal agreements to guarantee availability of CDD documentation.

5.7 Reporting of Unusual Transactions



- Report transactions equal to or greater than XCG. 5,000 or suspicious activities to the FIU Curaçao without delay via the goAML portal.
- Internal escalation and documentation of all suspicious findings.
- Strict prohibition against tipping off customers.

5.8 AML Compliance Program

- Risk-based AML program approved by senior management.
- Appointment of an independent Compliance Officer.
- Ongoing employee training and screening.
- Annual independent audit of AML processes.
- Procedures for freezing accounts based on suspicion of ML/TF.

6. Compliance and Consequences of Non-Compliance

Failure to comply with this policy may result in:

- Internal disciplinary action.
- Termination of employment or contract.
- Regulatory fines, sanctions, and/or criminal prosecution.
- Reputational damage to Popiplay.

7. Related Information

- National Ordinance on Identification when rendering Services (NOIS)
- National Ordinance on the Reporting of Unusual Transactions (NORUT)
- Sanctions National Ordinance
- Kingdom Sanction Act
- FATF 40 Recommendations

8. Contact Information

For questions about this policy, please contact:

- **Compliance Officer:** Lydia Obispo
- **Email:** Lydia.obispo@allyant-group.com
- **Phone:** +5999 4652559

9. Policy History

- New Policy - Effective 01/05/2025.
- Next Review Date: 01/05/2026, or sooner due to regulatory changes.

10. Policy URL (if applicable)

- www.popiplay.com

End of Document

Lydia Obispo

MLRO obo Allyant Group B.V.

May 30, 2025



Philip M. Humme

Managing Director obo Allyant Group B.V.

May 30, 2025

Philip M. Humme
