

R BOSTOCK ENTERPRISES B.V.

KNOW YOUR CUSTOMER (KYC) POLICY

KEY INFORMATION

Approving Official(s):	Marios Loukas
Responsible Office:	Compliance Department
Effective Date:	March 3, 2026
Next Review Date:	March 3, 2027
License Authority:	Curacao Gaming Authority (CGA)

1. POLICY STATEMENT

R Bostock Enterprises B.V., licensed by the Curacao Gaming Authority (CGA), is committed to verifying the identity of all customers and maintaining accurate and up-to-date records in accordance with applicable legislation. Under the CGA license and Curacao Anti-Money Laundering and Counter-Terrorist Financing (AML/CTF) legislation, the company implements comprehensive Know Your Customer (KYC) procedures to ensure the integrity of its gaming operations and compliance with all regulatory requirements.

2. PURPOSE

This policy establishes robust and effective customer identification and verification procedures designed to:

- Establish robust customer identification and verification processes in full compliance with CGA regulations and Curacao NORUT requirements;
- Align with international standards for KYC procedures as recommended by the Financial Action Task Force (FATF);
- Prevent identity fraud and verify that customers are who they claim to be;
- Ensure underage individuals are prevented from accessing gaming services;
- Implement comprehensive Anti-Money Laundering and Counter-Terrorist Financing (AML/CTF) compliance measures;
- Maintain accurate customer records and documentation for regulatory inspection;
- Establish risk-based verification procedures appropriate to the customer's profile.

3. AUDIENCE

This policy applies to all employees, contractors, and agents of R Bostock Enterprises B.V. who are involved in any of the following functions:

- Customer onboarding and account registration
- Identity and document verification
- Compliance and regulatory monitoring
- Customer service and account management
- Payments and fund management
- Risk assessment and due diligence

4. DEFINITIONS

Know Your Customer (KYC): Comprehensive processes to verify customer identity and obtain information about customer activities and risk profile.

Customer Due Diligence (CDD): Standard due diligence measures applied to all customers at account opening and ongoing monitoring.

Enhanced Due Diligence (EDD): Enhanced verification procedures applied to high-risk customers, including Politically Exposed Persons (PEPs) and high-risk jurisdictions.

Simplified Due Diligence (SDD): Reduced verification measures for low-risk customers identified through risk assessment.

Identity Verification: Process of confirming that a customer is the person they claim to be through document validation and liveness checks.

Address Verification: Confirmation that a customer's residential address is current and accurate using official documentation.

Source of Funds: Declaration and verification of the origin of customer deposits and funds used for gaming activities.

Source of Wealth: Documentation demonstrating the legitimate source of a customer's overall wealth and assets.

Beneficial Owner: Individual who ultimately owns or controls a customer or entity, or has effective control of the entity.

Politically Exposed Person (PEP): Individual who is or has been entrusted with public functions in any country, or immediate family members of such individuals.

Risk Profile: Classification of customer risk level (Low, Medium, High) based on various risk indicators and verification status.

Ongoing Monitoring: Continuous review of customer accounts and transactions to detect suspicious patterns or changes in behavior.

Document Verification: Process of validating the authenticity of identity and address documents submitted by customers.

Biometric Verification: Use of facial recognition and liveness detection technology to confirm customer identity.

Third-Party Verification Provider: External service provider utilized for identity verification, PEP screening, and sanctions checks.

5. POLICY IMPLEMENTATION

5.1 Customer Identification Requirements

All customers must provide the following information at the time of account registration:

- Full legal name (as it appears on official identity documents)
- Date of birth
- Residential address
- Email address
- Phone number
- Nationality
- Occupation or employment status
- Source of funds declaration

All information provided must be accurate, complete, and verified through appropriate documentation and verification processes. The company reserves the right to request additional information or clarification if documentation is unclear or inconsistent.

5.2 Verification Tiers and Thresholds

The company implements a three-tiered verification system based on account status and transaction thresholds:

TIER 1 - BASIC REGISTRATION (Unverified Account)

- Email address verification required
- Basic customer details collected (name, date of birth, email, phone)
- Maximum deposit cap: €200 total (unverified status)
- Risk Level Classification: BLACK (Unverified)
- Validity: Until customer-initiated verification or deposit threshold exceeded

TIER 2 - STANDARD VERIFICATION (Verified Account)

Required before exceeding €200 or ANG 4,000 threshold:

- Government-issued photo ID (passport, national ID card, or driving license)
- Proof of address document (utility bill, bank statement, or official correspondence) dated within 3 months
- Successful completion of third-party identity verification check
- Biometric liveness verification (facial recognition)

- Risk Level Classification: GREEN or BLUE (Low Risk, Fully Verified)
- Validity: 3 years or until document expiry

TIER 3 - ENHANCED VERIFICATION (High-Risk Customers)

Required for customers meeting any of the following criteria:

- Customer identified as PEP or related to PEP
- Customer from high-risk jurisdiction
- Adverse media flags or sanctions matches
- When deposit thresholds triggered: €2,000/week, €5,000/month, or €10,000 cumulative

Enhanced Verification Requirements:

- All Tier 2 verification documents and checks
- Source of funds documentation (bank statements showing fund origins)
- Source of wealth documentation (employment contracts, property deeds, investment statements)
- Additional beneficial owner verification if applicable
- Enhanced PEP and sanctions screening
- Compliance officer approval required
- Risk Level Classification: ORANGE (Medium Risk) or RED (High Risk)

5.3 Document Requirements

All submitted documents must meet the following standards:

- Clear, legible, and in color
- Unaltered and authentic
- Dated and not expired
- Issued by government or official body
- In English or with certified translation

Acceptable Identity Documents:

- Passport (valid, not expired)
- National ID Card (government-issued with photograph)
- Driving License (government-issued with photograph)

Acceptable Proof of Address (within 3 months):

- Utility bill (electricity, water, gas)
- Bank statement or credit card statement
- Official government correspondence
- Rental agreement or lease contract

Source of Funds Documentation:

- Bank statements showing fund origin and transfer details

- Payslips and employment contracts (for salary sources)
- Property deed or sale documentation (for sale proceeds)
- Inheritance documentation and court orders
- Investment or dividend statements

5.4 Verification Process

The verification process is conducted through the following procedures:

Primary Verification Method - Automated via Sumsub:

- Customer documents uploaded through secure portal
- Automated document verification and quality checks
- Biometric liveness verification through facial recognition
- Real-time identity database cross-reference checks
- Immediate verification result determination

Manual Verification Fallback Process:

- Triggered if automated verification fails or yields unclear results
- Conducted by trained compliance personnel
- Detailed document analysis and authenticity checks
- Customer contact for clarification if needed
- Documented review process

Verification Timeframes:

- Standard verification: 1-48 hours
- Complex or manual review cases: up to 72 hours
- Customer communication: Regular updates on verification status
- Account restrictions: Transaction limits applied during pending verification

5.5 Third-Party Verification Providers

The company engages reputable third-party service providers to conduct identity verification and compliance screening:

Sumsub - Identity Verification and Liveness Checks:

- Global identity verification platform
- Document authentication and validation
- Biometric liveness detection technology
- Real-time verification results
- Comprehensive data processing agreement in place

ComplyAdvantage - PEP, Sanctions, and Adverse Media Screening:

- Global PEP and sanctions database screening

- Adverse media and negative news monitoring
- Ongoing screening for high-risk customers
- Compliance with international screening standards
- Comprehensive data processing agreement in place

Provider Due Diligence and Contractual Requirements:

- Annual due diligence assessment of provider capabilities
- Contractual requirements for data security and privacy compliance
- Service level agreements (SLA) with defined response times
- Fallback procedures if primary provider becomes unavailable
- Data processing agreements compliant with GDPR and local regulations
- Audit rights and regular performance reviews

5.6 Risk-Based Approach to Verification

Customer risk is assessed based on multiple factors and classified into risk categories:

LOW RISK INDICATORS (GREEN/BLUE Classification):

- Successfully verified through automated checks
- No adverse media or PEP flags
- Originating from low-risk jurisdiction
- Standard transaction patterns consistent with profile
- Clear source of funds documentation

MEDIUM RISK INDICATORS (ORANGE Classification):

- Minor document verification issues resolved through manual review
- Moderate jurisdiction risk
- Transaction patterns elevated but not suspicious
- Partial source of funds documentation
- Geographic mismatch or complex business structure

HIGH RISK INDICATORS (RED Classification):

- PEP status or related to PEP
- Originating from high-risk or sanctioned jurisdiction
- Adverse media flags or sanctions matches
- Unusual or suspicious transaction patterns
- Source of funds concerns or unclear origins
- Multiple failed verification attempts
- Beneficial ownership complexity

Risk Color Coding System:

- BLACK: Unverified account (Tier 1 - Basic Registration)

- GREEN/BLUE: Low Risk - Fully Verified (Tier 2 - Standard Verification)
- ORANGE: Medium Risk - Enhanced Review Required (Tier 3 - Enhanced Verification)
- RED: High Risk - Escalated Review and Potential Restriction

5.7 Ongoing KYC Review and Monitoring

Customer information and risk profile must be reviewed and updated on an ongoing basis:

Periodic Re-Verification Schedule:

- Low Risk Customers: Full re-verification every 3 years
- Medium Risk Customers: Full re-verification annually
- High Risk Customers: Full re-verification every 6 months
- Document expiry monitoring and reminders to customers

Trigger-Based Reviews (Immediate Re-verification):

- Significant change in transaction patterns or amounts
- Adverse media alerts or sanctions matches
- Customer change of personal details (address, occupation)
- Regulatory requests or government inquiries
- Failed verification attempts or document issues
- Customer identity concerns or disputes

Continuous Monitoring Procedures:

- Real-time transaction monitoring for suspicious patterns
- Monthly review of high-risk customer accounts
- Quarterly review of medium-risk customer accounts
- PEP and sanctions screening alerts
- Adverse media monitoring through ComplyAdvantage
- Automated alerts for suspicious activities

5.8 Payment Method Verification

The company maintains strict policies regarding payment method usage to prevent fraud and layering:

- Customers must use payment methods registered in their own legal name only
- Corporate, business, or third-party payment methods are strictly prohibited
- No payments via joint accounts unless all account holders are verified customers
- Payment method must match customer registration details
- All payment methods undergo automated verification at deposit

Procedures for Payment Method Mismatches:

- Account flagged for manual review when payment method name does not match customer name

- Investigation conducted by compliance officer
- Customer contacted for explanation or updated documents
- Funds may be returned to source payment method if mismatch cannot be resolved
- Account may be restricted or closed if violation confirmed
- Reporting to Money Laundering Reporting Officer (MLRO) if suspicious activity suspected

5.9 Data Storage and Protection

All customer documents and personal information are stored and protected with the highest security standards:

- All documents stored in encrypted format on secure servers
- Tier-IV certified data center located in Curacao (in compliance with CGA requirements)
- Redundant backup systems for data availability
- Access restricted to authorized compliance and verification personnel only
- Comprehensive audit trails and access logs maintained

Data Retention Policy:

- Minimum retention period: 5 years after end of customer relationship
- Records maintained for regulatory inspection and investigation purposes
- Secure deletion procedures applied after retention period expires
- Customer access and data subject requests handled in compliance with privacy regulations

Information Security Measures:

- Multi-factor authentication for personnel access
- Encryption of data in transit and at rest
- Regular security audits and penetration testing
- Role-based access control (RBAC)
- Segregation of duties in verification process
- Compliance with ISO 27001 information security standards

5.10 Handling of Verification Failures

If a customer fails to complete verification or provided information is determined to be inaccurate, the following procedures apply:

- Customer notified of verification failure with explanation of issues
- Opportunity provided to customers to resubmit corrected documentation
- Maximum 30-day grace period for document resubmission (Tier 1 customers)
- Account restrictions applied: withdrawal functionality suspended, deposits limited
- If verification not completed within grace period, account suspended

Return of Funds Procedures:

- If verification fails and customer does not resubmit documents, funds returned to source payment method
- No refund of gaming losses or wagered amounts - only return of remaining balance
- Return processed within 10 business days of final suspension
- Funds returned at the cost of the customer (transfer fees apply)

Regulatory Reporting:

- Verification failures reported to Money Laundering Reporting Officer (MLRO)
- Pattern of verification failures or false information reported to Financial Intelligence Unit (FIU)
- Suspected identity fraud reported to law enforcement agencies
- Detailed documentation maintained for all failure cases

6. COMPLIANCE AND CONSEQUENCES OF NON-COMPLIANCE

All employees must comply with this KYC Policy. Non-compliance may result in:

- Disciplinary action up to and including immediate termination
- Regulatory fines and penalties by the Curacao Gaming Authority (CGA)
- Suspension or revocation of company gaming license
- Criminal liability for money laundering or terrorist financing violations
- Civil liability for customer claims or regulatory damages
- Mandatory retraining and certification requirements
- Reporting to law enforcement and regulatory agencies

Monitoring and Enforcement:

- Compliance Department conducts regular audits of KYC implementation
- Quarterly compliance reports submitted to management and CGA
- Regular training provided to all staff on KYC procedures
- Whistleblower program available for reporting compliance concerns

7. RELATED INFORMATION

- Curacao Gaming Authority (CGA) KYC Guidelines and Requirements
- R Bostock Enterprises B.V. AML/CTF Policy
- Responsible Gaming Policy
- Information Security Policy
- Data Protection and Privacy Policy
- Curacao NORUT Regulations
- Financial Action Task Force (FATF) Recommendations
- International Sanctions Regulations

8. CONTACT INFORMATION

Compliance Department

R Bostock Enterprises B.V.

For questions or concerns regarding this KYC Policy, please contact the Compliance Department at compliance@rbostock-enterprises.com

9. POLICY HISTORY

Version	Date	Status	Notes
2.0	March 3, 2026	Active	New Policy - Initial Implementation

SIGNATURE AND APPROVAL

This KYC Policy has been reviewed and approved by authorized management of R Bostock Enterprises B.V.

Signed:



Pulkit Totla

Date: March 3, 2026