

KNOW YOUR CUSTOMER (KYC) POLICY

Version 1.0 – October 2025

Company: Rail Solutions Group B.V.

1. PURPOSE

This policy defines the procedures and requirements for identifying, verifying, monitoring, and managing customers of Rail Solutions Group B.V. in order to:

- Prevent underage gambling
- Prevent money laundering and terrorist financing
- Ensure fair and responsible gambling
- Comply with Curaçao regulations and CGA licensing obligations

2. PLAYER IDENTIFICATION REQUIREMENTS

This policy applies to:

- All customers of betnimbus.com
- Employees responsible for managing customer accounts
- Third-party KYC and verification service providers

3. PLAYER IDENTIFICATION REQUIREMENTS

All players are subject to identification checks before being allowed to withdraw funds, or earlier if risk triggers apply.

3.1 BASIC INFORMATION REQUIRED

Collected during registration:

- Full legal name
- Date of birth
- Country of residence
- Valid email address and phone number
- Confirmation of being 18 years or older (checkbox)

3.2 VERIFICATION DOCUMENTS

Before withdrawals—or earlier if risk-based triggers apply—players must provide:

- Government-issued identification (passport, national ID, or driver's license)
- Proof of address (utility bill or bank statement issued within the last 3 months)
- Selfie verification, if requested, to confirm identity
- Source of funds documentation for high-risk players (e.g., crypto wallet history, salary slips)

Note: Verification is mandatory before the first withdrawal or earlier if triggered by deposit thresholds, flagged behavior, or assessed risk level.

4. AGE VERIFICATION

- Players must confirm they are 18 or older during registration.
- Accounts suspected of being underage are immediately suspended pending investigation.
- Proof-of-age documents must be reviewed before any gameplay or deposits for suspected minors.

5. RISK-BASED KYC TRIGGERS

Verification may be required prior to withdrawal in any of the following cases:

- Cumulative deposits exceed €2,000 (or crypto equivalent)
- High-frequency or high-value transactions
- Use of cryptocurrency
- Suspicious or flagged activity under AML protocols
- Self-exclusion or cooling-off activity

6. PLAYER MANAGEMENT

Rail Solutions Group B.V. maintains a centralized Player Account Management (PAM) system that includes:

- Player registration and verification history
- Risk ratings and behavioral monitoring
- Responsible gambling tool usage (limits, exclusions, cooling-off periods)
- Transaction history and login records
- Communication logs with support and/or the MLRO

Players are segmented by risk tier and monitored accordingly.

7. ACCOUNT SUSPENSION & CLOSURE

7.1 SUSPENSION TRIGGERS

Accounts may be suspended for:

- Suspected underage play
- Incomplete or invalid KYC documentation
- Link to a self-excluded individual
- Fraudulent behavior or multi-accounting
- Chargebacks or payment fraud
- Use of anonymizing tools (VPNs, proxies) to access restricted markets

During suspension:

- Deposits and gameplay are disabled
- Withdrawals are paused pending review

7.2 ACCOUNT CLOSURE TRIGGERS

Accounts may be permanently closed for:

- Verified underage status or falsified identity
- Breach of terms and conditions
- Repeated violations of responsible gambling policies
- Proven fraud or criminal activity
- Closure requested by the player

Upon closure:

- Remaining lawful balances will be refunded
- The account will be flagged to prevent re-registration
- Data will be retained in accordance with legal requirements

8. DATA RETENTION

All KYC records and supporting documentation are retained for a minimum of five (5) years following:

- The closure of the player account, or
- The date of the final transaction — whichever occurs later.

9. USE OF THIRD-PARTY VERIFICATION PROVIDERS

Rail Solutions Group B.V. may engage regulated third-party providers to perform:

- ID document verification
- Biometric or selfie verification
- Database and sanctions screening
- Cryptocurrency wallet screening

All third-party vendors are subject to due diligence to ensure compliance with AML/CFT and data protection standards.

10. REVIEW AND COMPLIANCE

- The Money Laundering Reporting Officer (MLRO) oversees KYC implementation and updates.
- Internal audits are conducted at least annually, or as otherwise required.
- This policy is reviewed and updated periodically to reflect regulatory changes and operational experience.