

Anti-Money Laundering (AML) Policy

BETSSEN

Last Updated: 2025-05-13

1. Policy Statement

BETSSEN, operated by Great BDG Randon Entertainment N.V., is firmly committed to preventing its operations from being used to facilitate money laundering (ML), terrorist financing (TF), or any form of financial crime. This Anti-Money Laundering (AML) Policy applies to all departments, employees, contractors, partners, and customers engaging with BETSSEN services and outlines our obligations and measures to ensure compliance with local and international regulatory standards, particularly under the guidance of the Curacao Gaming Control Board (CGA).

2. Purpose

The purpose of this Anti-Money Laundering Policy is to ensure that BETSSEN's operations are aligned with applicable anti-money laundering (AML) and counter-terrorist financing (CFT) regulations. This policy is designed to:

- Comply with legal and regulatory obligations under the laws of Curacao and relevant international AML standards including EU Directive 2015/849 and FATF recommendations.
- Protect BETSSEN's platform from being exploited for illicit activities.
- Provide a structured framework for implementing preventive, detective, and responsive AML/CFT controls.

3. Audience

This policy applies to all BETSSEN employees, contractors, executive leadership, and any third-party service providers engaged in compliance-sensitive functions.

4. Definitions

- **Money Laundering (ML):** The concealment of the origins of illegally obtained money.
- **Terrorist Financing (TF):** Provision of funds for terrorist activities.
- **PEP:** Politically Exposed Person.
- **CDD/EDD:** Customer Due Diligence / Enhanced Due Diligence.
- **SAR:** Suspicious Activity Report.
- **MLRO:** Money Laundering Reporting Officer.

5. Policy Implementation

5.1 Business Risk Assessment

BETSSEN has conducted a business-wide ML/TF risk assessment considering product types (e.g., slots, tables), geographic exposure, digital currency handling, and transaction flow patterns. Mitigation controls include product-level risk restrictions, enhanced monitoring of high-risk regions, and transaction controls.

5.2 Customer Risk Assessment

CRA is conducted at onboarding and throughout the customer lifecycle. Risk factors include nationality, payment method, gaming pattern, and behavioral shifts. Customers are classified into Low/Medium/High risk tiers based on these inputs.

5.3 Customer Acceptance Policy

Customer acceptance is governed by CRA outcomes:

- **Low Risk:** Standard KYC.
- **Medium Risk:** Additional document validation.
- **High Risk:** Requires SoF/SoW and Compliance approval. PEPs and sanctioned individuals are not accepted.

5.4 Customer Due Diligence

- ID & Address verification
- Sumsu used for KYC automation
- PEP/Sanctions screening
- Freeze and SAR report initiated for any ML/TF suspicion

5.5 Ongoing Monitoring

- **Manual transaction checks** by CS Agents
- Behavioral alerts
- Periodic profile review for high-risk customers
- Human oversight on AI pattern analysis

5.6 Third Party CDD

BETSEN uses Sumsu for identity verification. Final CDD responsibility remains internal. Only vetted PSPs are used for financial processing.

5.7 Reporting of Unusual Transactions

CS agents and staff escalate cases to MLRO. MLRO evaluates and, if necessary, submits SAR via goAML to the Curacao FIU. Tipping-off is prohibited.

5.8 AML Compliance Program

Risk-based and structured program managed by AMLCO and Compliance Department. Includes account blocking, regular audits, and escalation protocols for high-risk behavior.

6. Compliance and Consequences of Non-Compliance

Non-compliance may result in:

- Internal disciplinary actions (termination)
- Regulatory sanctions by CGA
- Legal/criminal prosecution under Curaçao Penal Code (N.G. 2011, no. 48)
- Reputational damage to BETSEN

7. Related Information

This AML Policy is supported and influenced by the following legal and regulatory frameworks, international guidelines, and internal documentation:

a. External Legal & Regulatory Frameworks

- EU Directive 2015/849 on the prevention of the use of the financial system for the purposes of money laundering and terrorist financing
- EU Regulation 2015/847 on information accompanying transfers of funds
- FATF Recommendations on AML/CFT Standards
- Curacao AML Guidelines issued by the Gaming Control Board
- United Nations Sanctions Lists, OFAC Sanctions, EU Consolidated List
- **National Ordinance on the Reporting of Unusual Transactions (NORUT)** (N.G. 2017, no. 99)
- **National Ordinance on Identification when Rendering Services (NOIS)** (N.G. 2017, no. 92)
- **Sanctions National Ordinance** (N.G. 2014, no. 55)
- **Kingdom Sanction Act** (N.G. 2016, no. 54)
- **Regulation Indicators Unusual Transactions** (N.G. 2015, no. 73)
- **National Decree implementing UN Sanctions (Afghanistan/ISIL/ANF)** (N.G. 2015, no. 29)
- **Sanctions Ordinance Libya** (N.G. 2015, no. 28)
- **UN Sanctions Extension Decree** (N.G. 2018, no. 34)
- **National Decree on Kingdom Sanction Law Entry** (N.G. 2017, no. 2)
- **Curacao Penal Code** (N.G. 2011, no. 48)

b. Internal Policies & Procedures

- BETSEN KYC Manual

- Transaction Monitoring SOP
- Suspicious Activity Reporting Flowchart
- Internal Record Retention Policy
- Sumsb Integration & Verification Protocol

Employees may request access to the latest versions of these documents from the Compliance Department.

8. Contact Information

Compliance Department – BETSSEN

Email: help@betssen.com

9. Policy History

Version	Date	Description	Approved By
1.0	2024-03-01	Initial AML Policy Issued	Executive Management
1.1	2025-05-13	Updated per CGA Guidelines and industry best practices	AMLCO & Executive Mgmt
1.2	2025-05-22	Extended Section 7 with full Curaçao legal framework references	AMLCO

Next review scheduled by: **May 13, 2026**

10. Policy URL

<https://www.betssen.com/en/help/109739>

KYC Policy

By accepting the Terms & Conditions, you permit us to conduct any necessary verification checks, including those required by third parties such as regulatory bodies, to verify your identity and contact information (the "Checks"). During these Checks, your ability to withdraw funds from your Account will be restricted.

If any information you provided is false, inaccurate, misleading, does not match your ID, or is otherwise incomplete, we reserve the right to immediately terminate your account and/or restrict your access to our services, along with any other actions we may choose to take.

If we cannot confirm that you meet the Legal Age requirement, we may suspend your Account. If it turns out you were under the Legal Age when you made any gambling or gaming transactions, then:

- Your Account will be closed;
 - All transactions made during that period will be considered void, and any funds you deposited will be refunded;
 - Any winnings accrued during that time will be forfeited, and you will be required to return any funds withdrawn from your Account.
- Accounts that have already been Checked(Verified) will be permitted to withdraw funds.

If there are any changes to your personal information, you must notify us by contacting Support.

Besides the General Verification Checks, the Company will request additional verification from users of its Services in the following situations:

- Suspicions of fraud, money laundering, or criminal activity;
- Doubts regarding the authenticity of submitted documents;
- Breaches of the Company's service usage terms;
- Any other situation deemed appropriate by the Company.

Through this requests, the Company may require a standard set of identification data and documents, along with any additional documents deemed necessary.

The minimum identification data required includes:

- Full name;
- Date of birth;
- Citizenship;
- Permanent residence address;
- Identification number.

The required documents are:

- A valid passport or ID card;
- A document confirming the client's current permanent residence address (e.g., utility bill, bank statement).

Additional documents may include:

- Another form of national ID (e.g., driver's license, military ID);
- A photo of the user holding their passport and a separate paper with a note with their face visible (the document must be clearly readable);
- A photo/screenshot of their payment method. In case of the bank card, front side of it (the first five digits, last four digits, owner's name, and expiry date must be visible).

The Company may also request documentation regarding the source of funds to ensure users provide evidence of the origins of the funds they use for betting or gaming.

Acceptable forms of this information include:

- Proof of income (e.g., payslip, director's remuneration, dividends, pension);
- Bank statements or savings account records showing consistent deposits from identifiable sources;
- A trust deed indicating a consistent entitlement to funds;
- Dated proof of an award or payment made to the user.

Documents provided by the user may be rejected for reasons such as:

- Mismatched name or address on documents compared to the account;
- Illegible documents or copies;
- Unacceptable documents (e.g., a non-accepted form of ID verification or a copy of a mail envelope instead of a utility bill);
- Any other reasons deemed appropriate by Company staff or contractors.

Based on the analysis of the submitted documents, the Company will make a decision in accordance with the Terms and Conditions, Privacy Policy, License Agreement of the Website, and legal requirements.



(SMES)
Solutions for Management
and Employment Support N.V.