

GBL SOLUTIONS N.V.

KYC POLICY

This Document is intended only for the following users:

User Types
General Users

Version Control:

<u>Document Version</u>	<u>Document Author</u>	<u>Approved By</u>	<u>Document Purpose</u>	<u>Release Date</u>
1.0	PAVEL EVGRAFOV - UBO	(SMES)Solutions for Management and Employment Support N.V. – Authorized Signatory	Initial Release	02/10/2025

Table of Contents

1. Objectives.....	4
2. General Definitions.....	4
3. Customer Identification and Verification.....	5
3.1. Minimum Information Requirements.....	5
3.2. Verification Documents.....	5
3.3. Timing of Verification.....	6
4. Customer Risk Assessment.....	6
4.1. Risk Categories.....	6
5. Due Diligence Measures.....	6
5.1. Simplified Due Diligence (SDD).....	6
5.2. Standard CDD.....	6
5.3. Enhanced Due Diligence (EDD).....	7
6. Ongoing Monitoring.....	7
6.1. Review Timeframes.....	7
7. Sanctions and PEP Screening.....	7
8. Record-Keeping.....	8
9. Reporting.....	8
10. Training and Awareness.....	8
11. Governance and Responsibilities.....	9

1. Objectives

The purpose of this Know Your Customer (KYC) Policy is to establish the principles, standards, and procedures that GBL Solutions N.V. ("the Company") shall apply to:

- Identify and verify all customers prior to and during the course of a business relationship.
- Prevent the misuse of the Company's services for money laundering (ML), terrorist financing (TF), fraud, or other financial crime.
- Comply with the National Ordinance on Games of Chance (LOK, 2024), the requirements of the Curaçao Gaming Authority (CGA), and applicable international AML/CFT standards (FATF, CFATF, EU Directives).

This KYC Policy operates as a standalone framework and is complementary to the Company's AML/CFT Policy.

2. General Definitions

For the purposes of this Manual, unless the context shall prescribe otherwise:

"Beneficial Owner" means the natural person or natural persons, who ultimately owns or control the Client and/or the natural person on whose behalf a transaction or activity is being conducted.

"Business Relationship" means a business, professional or commercial relationship which is connected with the professional services offered by the Company, and which was expected, at the time when the contact was established, to have an element of duration.

"CDD" — customer due diligence.

"CFATF" - means the Caribbean Financial Action Task Force.

"Client" means any legal or physical person aiming to conclude a Business Relationship or conduct a single transaction with the Company.

"Company" means GBL Solutions N.V., a company which is duly incorporated under the Laws of Curacao and its related companies and entities.

"EDD" — enhanced due diligence.

"European Economic Area (EEA)" means Member State of the European Union or other contracting state which is a party to the agreement for the European Economic Area signed in Porto on the 2nd of May 1992 and was adjusted by the Protocol signed in Brussels on the 17th of May 1993, as amended.

"EU Directive" means the Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and amending Directives 2009/138/EC and 2013/36/EU.

"FATF" — means the Financial Action Task Force

"FIU" — means the Financial Intelligence Unit of Curacao.

"Law" means any Laws and Acts legally enacted from time to time in Curacao, or which are applicable and enforceable in Curacao.

"Money Laundering and Terrorist Financing" or **"ML/TF"** means the money laundering offences and terrorist financing offences defined in the Law.

"Politically Exposed Persons (PEPs)" means the natural persons who have their place of residence in Curacao or any other country and who are or have been entrusted with prominent public functions and their immediate family members or persons known to be close associates of such persons (see also section 9).

"KYC" for Know Your Customer

3. Customer Identification and Verification

3.1 Minimum Information Requirements

At onboarding, the following details must be collected:

- Full name
- Date and place of birth
- Country
- Permanent residential address
- Email address and phone number
- Gender

3.2 Verification Documents

The following must be obtained and verified:

- Proof of Identity: Passport, national ID card, or driver's license (color copy, valid, government-issued).

- Proof of Address: Utility bill, bank statement, or government correspondence (issued within the last 3 months).
- Selfie Verification: To confirm likeness and detect impersonation/fraud.

3.3 Timing of Verification

- No services may be provided to anonymous or fictitious customers.
- Verification must be completed before the first withdrawal or when a cumulative transaction equals or exceeds NAf. 4,000 (or equivalent).
- Additional verification may be triggered by suspicion of ML/TF, high-risk jurisdictions, or unusual patterns.

4. Customer Risk Assessment

Customers are categorized into **Low, Medium, High Risk, or PEP**, based on:

- Jurisdiction of residence
- Product/service type
- Funding methods
- Transaction behavior
- Source of wealth/funds

4.1 Risk Categories

- **Low Risk:** Minimal ML/TF exposure. Eligible for SDD.
- **Medium Risk:** Standard CDD required.
- **High Risk:** EDD mandatory. Requires MLRO approval.
- **PEP:** Treated as high risk. Proof of source of wealth and funds required. Senior management approval mandatory.

5. Due Diligence Measures

5.1 Simplified Due Diligence (SDD)

Applied only to low-risk customers when permitted by law.

5.2 Standard CDD

- Proof of identity and address
- Verification of source of wealth and funds (where relevant)
- Screening against sanctions and PEP databases

5.3 Enhanced Due Diligence (EDD)

Required for high-risk cases, including:

- PEPs
- High-risk jurisdictions
- Unusual transactions or patterns
- Large transactions above regulatory thresholds

EDD may include:

- Certified copies of documents
- Bank statements and reference letters
- Video verification
- Ongoing management approval

6. Ongoing Monitoring

The Company shall conduct continuous monitoring of customer activity, including:

- Reviewing transactions to ensure consistency with the customer profile.
- Detecting unusual or suspicious behavior.
- Screening customers periodically against updated sanctions and PEP lists.

6.1 Review Timeframes

- Low Risk: every 30–36 months
- Medium Risk: every 18–30 months
- High Risk/PEP: every 12–18 months

7. Sanctions and PEP Screening

All customers shall be screened at the point of onboarding and at regular intervals thereafter against relevant international and national sanctions lists, including those issued by the United Nations, the European Union, the Office of Foreign Assets Control (OFAC), and any local Curaçao or Kingdom of the Netherlands authorities. Should a positive match be identified, the case must be escalated without delay to the Money Laundering Reporting Officer (MLRO), who will determine the appropriate course of action. Where required, the matter will also be reported to the Financial Intelligence Unit (FIU) of Curaçao. If the customer is confirmed to be a sanctioned individual, the Company is obligated to freeze any assets under its control immediately and to maintain such freeze pending instructions from the competent authorities.

8. Record-Keeping

The Company is required to maintain all customer identification data, verification documents, and due diligence records for a minimum period of five (5) years, commencing from the date on which the business relationship is terminated or, in the case of an occasional transaction, from the date of that transaction. All records must be stored securely, remain easily retrievable, and be safeguarded in accordance with applicable data protection and privacy laws. In circumstances where an investigation is ongoing, or where legal proceedings require, records may be retained for a longer period as deemed necessary by the MLRO or competent authorities.

9. Reporting

Any suspicion of money laundering or terrorist financing activity identified by employees must be reported immediately to the MLRO. The MLRO will assess the information provided and determine whether there is sufficient basis to file a Suspicious Transaction Report (STR) with the FIU Curaçao. Under no circumstances may employees inform or otherwise disclose to the customer that an STR has been or may be filed, or that an investigation is being undertaken, as doing so would constitute unlawful "tipping off."

10. Training and Awareness

The Company is committed to ensuring that all employees involved in customer-facing activities, compliance, or transaction monitoring receive appropriate training on KYC obligations. Training shall be provided on an annual basis and will cover the identification of red flags, relevant regulatory updates, and internal procedures. In addition, specialized training shall be delivered to members of the Compliance, KYC, and Customer Support teams to ensure they possess the technical knowledge necessary to carry out their functions effectively. Records of all training sessions, including attendance and content, shall be maintained and made available for inspection by regulators or auditors.

11. Governance and Responsibilities

The governance of this KYC Policy rests with the Company's Board of Directors, which is responsible for approving the policy and overseeing its implementation. The MLRO has primary responsibility for ensuring compliance with applicable laws and regulations, for keeping this Policy up to date, and for reporting to regulatory bodies as required. The Compliance Department is charged with the day-to-day execution of KYC procedures, monitoring activities, and reporting obligations. All employees are individually responsible for adhering to the requirements of this Policy and for applying KYC measures consistently in the course of their duties.

Signed by UBO, of GBL Solutions N.V.:

Name: Pavel Evgrafov



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

Managing Director

20.10.2025

Typ hier uw tekst