

Know Your Player (KYC) Policy - Apalonik B.V.

Last updated: 30/07/25

1. Introduction

This Know Your Player (KYC) and Anti-Money Laundering (AML) policy applies to Apalonik B.V., a Curaçao-licensed online casino. We are committed to complying with all applicable laws and regulations related to KYC and AML, including those required by Curaçao's regulatory authorities, international guidelines, and financial institutions. This policy outlines the steps and procedures implemented by Apalonik B.V. to ensure that it does not become involved in illegal activities such as money laundering, terrorist financing, or fraud. All players, regardless of their jurisdiction, must adhere to the KYC/AML guidelines set forth by the casino.

We keep up to date with the NOIS, the NORUT, the Sanction National Ordinance and the Kingdom Sanction Act, to ensure the prevention of illegal activities such as money laundering, terrorist financing, and fraud. The NOIS, the NORUT, the Sanction National Ordinance and the Kingdom Sanction Act contain provisions for service providers to prevent those entities for being used for money laundering, the financing of terrorism and the proliferation of weapons. Different countries act together to combat money laundering and terrorist financing in the Financial Action Taskforce on money laundering (FATF). It was established by the G-7 Summit that was held in Paris in 1989. The Dutch Kingdom is member of the FATF, Curaçao is member of Caribbean Financial Action Taskforce (CFATF). The FATF 40 effective national and international control of financial crime. The FATF members incorporate the FATF Recommendations in their local laws. The most important obligations for the gaming casino resulting from the AML/CFT laws refer to the conducting of Player Due Diligence (CDD) and the reporting of unusual transactions. All this prevents the casino from being used by individuals for the laundering of their criminally acquired funds.

The Regulations for combating Money Laundering, the Financing of Terrorism and Proliferation of weapons of Mass Destruction (ML/FT/FP) are an integral part of the land-based and the online gambling license requirements for the Curaçao jurisdiction. These Regulations are issued in implementation of:

- article 2 paragraph 8 and article 11, paragraph 3, of the National Ordinance on Identification when rendering Services (NOIS) (N.G. 2017 no. 92) and;
- article 22mm, paragraph 3, of the National Ordinance on the Reporting Unusual Transactions (NORUT) (N.G. 2017 no.99);
- Sanctions National Ordinance (N.G. 2014, no. 55);
- Kingdom Sanction Act (N.G. 2016, no. 54).

Key legal requirements include:

- Conducting proper Know Your Player (KYC) procedures.
- Reporting suspicious transactions to the appropriate authorities.
- Ensuring ongoing monitoring of player activity to detect financial crime patterns.

2. Objectives

The primary objectives of this policy are:

- **Player Identity Verification:**

We will verify the identity of players to ensure they are legitimate players and not engaging in fraudulent or illegal activities. This process includes Know Your Player (KYC) procedures, where individuals provide identification documents such as passports, driver's licenses, and proof of address. Proper verification helps prevent identity theft, account takeovers, and the use of fraudulent accounts.

- **Detection and Reporting of Suspicious Activities:**

We will monitor player transactions and behaviors to identify signs of money laundering, fraud, or other financial crimes. This includes detecting unusual betting patterns, rapid deposits and withdrawals, and the use of third-party accounts. If suspicious activities are identified, the casino must report them to the relevant financial authorities through Suspicious Activity Reports (SARs) or other mandatory filings.

- **Regulatory Compliance:**

We will adhere to the laws and regulations established by Curaçao and other jurisdictions where it operates. Compliance requirements include anti-money laundering (AML) protocols, player due diligence (CDD), and enhanced due diligence (EDD) for high-risk players. Ensuring compliance not only protects the casino from legal consequences but also maintains its reputation as a trusted gaming operator.

- **Prevention of Underage Gambling and Illicit Activities:**

To uphold responsible gaming policies, we will implement strict age verification processes to prevent minors from accessing gambling services. Additionally, measures should be in place to prevent fraudulent activities such as bonus abuse, identity fraud, and collusion between players. Casinos should also have robust security protocols to prevent cyber threats and unauthorized access to accounts.

- **Risk Management for High-Risk Players and Transactions:**

We will assess and mitigate risks associated with players from high-risk jurisdictions, Politically Exposed Persons (PEPs), and transactions that exhibit suspicious characteristics. This includes implementing enhanced due diligence (EDD) procedures, continuous transaction monitoring, and risk-based assessments to flag potential threats.

- **Promotion of Responsible Gaming and Player Protection:**

A key priority for us is to encourage responsible gambling by offering self-exclusion programs, deposit limits, and tools that help players manage their spending. Safeguarding player funds is also critical, requiring the segregation of player deposits from operational funds to ensure financial integrity and compliance with licensing requirements.

3. Player Identification and Verification

Apalonik B.V. conducts a player risk assessment for every player to determine their money laundering (ML) and terrorist financing (TF) risk level. This process involves due diligence measures tailored to each player's risk profile to ensure compliance with regulatory requirements and maintain the integrity of the gaming environment.

As part of the Know Your Player (KYC) process, Apalonik B.V. verifies player identity upon account registration. This verification must be completed before players can access specific gaming features, including deposits, withdrawals, and cashouts.

3.1 KYC Documentation Requirements

To verify the identity of a player, the following documents may be requested:

1. Proof of Identity

- A valid government-issued photo identification document, such as:
 - Passport
 - Driver's license
 - National identity card
- The document must be clear, legible, and valid at the time of submission.

2. Proof of Address

- A document verifying the player's residential address, such as:
 - A utility bill (electricity, water, gas)
 - A bank statement
- The document must be issued within the last three months and clearly display the player's name and address.

3. Proof of Payment Method

- To confirm the legitimacy of transactions, players must provide evidence of the payment method used for deposits or withdrawals, which may include:
 - A copy of a credit or debit card (showing only the last four digits)
 - A screenshot or confirmation document from an e-wallet or online banking service
- This step helps prevent fraud, unauthorized transactions, and financial crimes.

4. Source of Funds Declaration

- In cases where a user makes large deposits or exhibits high-risk behavior (e.g., unusually frequent or high-value betting), additional verification may be required.
- Players may need to provide:
 - A declaration of their source of funds
 - Supporting documentation such as bank statements, salary slips, or business income records

3.2 Age Verification

To prevent underage gambling, Apalonik B.V. enforces strict age verification measures. All players must be over the legal age of majority in their jurisdiction before being allowed to play.

The verification process may include:

- Requiring a scanned copy of a government-issued identification document
- Confirmation of the player's age during the registration process
- Additional checks if there is any suspicion of false or misleading information

Failure to meet the KYC and age verification requirements may result in account suspension, restricted access to gaming features, or account closure in compliance with regulatory obligations.

4. Player Due Diligence (CDD)

Apalonik B.V. implements a risk-based approach to due diligence, ensuring that appropriate verification measures are taken based on the level of risk each player presents. This process is categorized into Standard Due Diligence (SDD) and Enhanced Due Diligence (EDD) based on the player's transaction patterns, risk profile, and jurisdiction.

4.1 Standard Due Diligence

For most players, the casino applies standard due diligence (SDD) measures to verify their identity and assess any potential risks. This includes:

- Obtaining and verifying basic identity documents, such as a passport, driver's license, or national ID.
- Ensuring the authenticity of these documents and confirming the player's identity.
- Screening players against international sanctions lists and Politically Exposed Persons (PEP) databases to identify potential risks related to financial crime, corruption, or illicit activities.

For low-risk players, the verification process may be limited to:

- Proof of Identity (government-issued photo ID).
- Proof of Address (recent utility bill or bank statement).

However, for higher-risk players, additional documentation may be required to mitigate potential risks of money laundering (ML) and terrorist financing (TF). In such cases, the casino may also request:

- Proof of Payment Method (to verify the source of deposits and withdrawals).
- Source of Funds Declaration (to confirm the legitimacy of the player's funds).

4.2 Enhanced Due Diligence (EDD)

Enhanced Due Diligence (EDD) is conducted for players or transactions that present a higher risk.

This includes, but is not limited to:

- High-value deposits or withdrawals that exceed predefined risk thresholds.
- Players from high-risk jurisdictions or countries associated with financial crime, weak regulatory oversight, or sanctions.

- Transactions exhibiting unusual or suspicious patterns, such as rapid deposits and withdrawals, use of multiple payment methods, or third-party transactions.

For such cases, the casino will implement additional verification measures, which may include:

- Requesting further identity verification beyond standard KYC documents.
- Requiring additional proof of the player's source of funds, such as bank statements, payslips, or business income records.
- Conducting a deeper assessment of the business relationship, including identifying the purpose and intended nature of the transactions.
- Ongoing monitoring of account activity to detect any signs of financial crime.

If a player fails to provide satisfactory documentation, we reserve the right to:

- Restrict or suspend account access until the necessary documents are provided.
- Block certain transactions that appear suspicious or non-compliant.
- Report the activity to relevant regulatory authorities if necessary.

5. Monitoring and Reporting of Suspicious Activities

Apalonik B.V. is committed to detecting, preventing, and reporting any activity that may indicate money laundering (ML), terrorist financing (TF), or fraud. In compliance with Curaçao's licensing requirements and Article 11 of the NORUT, we will immediately report any suspicious activity to the relevant Curaçao authorities, including the Financial Intelligence Unit (FIU).

5.1 Monitoring Transactions

Apalonik B.V. will continuously monitor player accounts and transactions for any suspicious activities. This may include:

- Unusually large deposits or withdrawals.
- A series of rapid and high-value bets.
- Any transactions that appear inconsistent with the player's usual behavior.

Suspicious activities will be flagged, investigated, and reported to the relevant authorities if necessary.

5.2 Reporting Suspicious Transactions

If any suspicious activity is detected that could indicate money laundering, terrorist financing, or fraud, we will immediately report it to the relevant Curaçao authorities such as the FIU in compliance with the Curaçao licensing requirements, as per article 11 of the NORUT.

- All suspicious transaction reports (STRs) will be filed and retained in accordance with local and international regulations.

- If a player is suspected of being involved in illegal activity, their account may be frozen, and further investigation will take place.

The following transactions or intended transactions are deemed unusual:

- a) Transactions which in connection with money laundering or terrorism financing are reported to the Police or to the Department of Justice;
- b) Transactions by or on behalf of a natural or legal person, a group or an entity, who is named on a list, adopted by virtue of the Sanctions National Ordinance (N.G. 2014 no. 55);
- c) Transactions in the amount of NAf. 5,000 or more, regardless whether the transaction is through electronic or other non-physical means.

This includes but is not limited to:

1. A cashless transaction in the amount of NAf. 5,000 or more. A cashless transaction is a transfer from a bank account of the casino to a local or international bank account, at the request of the client.
2. Accepting or releasing a deposit in the amount of NAf. 5,000 or more at the request of the client;
3. Sale to a player of chips in the amount of NAf. 5,000 or more. "Chips" include but is not limited to tokens and credits.
4. A cash out in the amount of NAf. 5,000 or more;

These transactions are flagged for further review due to their potential link to illicit activities such as money laundering or terrorism financing and will be scrutinized accordingly.

6. Record Keeping

Apalonik B.V. is committed to maintaining comprehensive records in compliance with Curaçao's regulatory requirements and international anti-money laundering (AML) and counter-terrorism financing (CTF) standards.

Retention Period and Scope

- All Know Your Customer (KYC) and AML documentation, including:
 - Customer identity verification records
 - Proof of address, proof of payment method, and source of funds documentation
 - Transaction history and records of financial activity
 - Suspicious Transaction Reports (STRs) and any related communications

- These records will be retained for a minimum of five (5) years after the termination of the business relationship with the customer.

Availability and Compliance

- All retained records will be securely stored and made available to regulatory authorities, including the Financial Intelligence Unit (FIU) of Curaçao, upon request.
- We will ensure data integrity and confidentiality by implementing secure storage measures in line with applicable data protection laws.

By maintaining robust record-keeping practices, Apalonik B.V. ensures compliance with legal obligations while supporting regulatory investigations and audits when necessary.

7. Anti-Money Laundering Training and Awareness

All relevant staff members at Apalonik B.V. will receive regular AML training to ensure they understand their roles and responsibilities in detecting and preventing money laundering and other illegal activities.

- Training will be conducted annually and include guidance on how to identify suspicious activities and report them to the appropriate authorities.
 - Staff will also be informed about changes to laws and regulations to ensure ongoing compliance.
-

8. Risk Assessment and Risk-Based Approach

Apalonik B.V. implements a risk-based approach (RBA) to Know Your Player (KYC) and Anti-Money Laundering (AML) compliance. This means that the level of due diligence applied to each player is determined by their individual risk profile, ensuring that regulatory efforts and resources are allocated effectively.

8.1 Risk Factors Considered

The casino evaluates multiple risk factors to assess the potential risk a player poses, including:

- Country of Residence – Players from jurisdictions with weak AML regulations, high corruption records, or sanctioned regions may be subject to Enhanced Due Diligence (EDD).
- Player History and Behavior – Past account activity, prior compliance concerns, and betting patterns may indicate potential risk.
- Payment Methods Used – The use of anonymous, high-risk, or third-party payment methods (e.g., prepaid cards, cryptocurrency wallets, or multiple accounts) may require additional scrutiny.
- Transaction Size and Frequency – Large or frequent deposits and withdrawals, particularly those inconsistent with typical gaming behavior, may indicate potential money laundering risks.

8.2 Effective Resource Allocation

By adopting a risk-based approach, Apalonik B.V. ensures that:

- Low-risk players undergo standard due diligence (SDD) with minimal verification requirements.
- High-risk players and transactions are subject to Enhanced Due Diligence (EDD), including additional document requests and ongoing monitoring.
- Suspicious activity is identified and reported promptly to prevent financial crime and ensure compliance with regulatory obligations.

This structured approach enhances security, mitigates financial crime risks, and ensures compliance with Curaçao's AML regulations while maintaining a seamless player experience.

9. Player Privacy and Data Protection

Apalonik B.V. is committed to safeguarding all player data collected as part of the Know Your Player (KYC) and Anti-Money Laundering (AML) process. We ensure that personal data is handled with the highest level of confidentiality and in full compliance with applicable data protection laws, including the General Data Protection Regulation (GDPR) where applicable.

9.1 Purpose of Data Collection

Player data is collected solely for the following purposes:

- Verifying the player's identity as required by KYC regulations.
- Ensuring compliance with AML and counter-terrorism financing (CTF) laws.
- Preventing fraud, money laundering, and other illicit activities.

9.2 Data Confidentiality and Security

- Personal data will not be shared with third parties unless required by law, regulatory authorities, or with the player's explicit consent.
- All collected data will be stored securely using industry-standard security protocols to prevent unauthorized access, loss, or misuse.
- Access to personal data is strictly limited to authorized personnel responsible for compliance and regulatory matters.

9.3 Compliance with Data Protection Laws

- Apalonik B.V. adheres to all applicable data privacy regulations, including the GDPR, ensuring that player rights regarding data privacy and protection are upheld.
- Players may exercise their data protection rights, including requesting access, correction, or deletion of their personal data, as permitted by applicable laws.

By implementing stringent data protection and confidentiality measures, Apalonik B.V. ensures regulatory compliance while protecting the privacy and trust of our players.

10. Independent Audits & Regulatory Inspections

Apalonik B.V. is committed to maintaining transparency, accountability, and compliance with all applicable anti-money laundering (AML) regulations and Curaçao Gaming Authority (CGA) requirements. To ensure the effectiveness of our AML compliance program, we implement regular independent audits and remain fully cooperative with regulatory inspections.

10.1 Independent AML Audits

- Apalonik B.V. conducts annual independent audits to assess the effectiveness of its AML policies, procedures, and risk management framework.
- These audits evaluate compliance with regulatory obligations, identify potential vulnerabilities, and recommend corrective actions where necessary.
- In addition to internal audits, the casino will engage external AML compliance specialists to provide an objective review and ensure alignment with best practices.

10.2 Regulatory Inspections by the Curaçao Gaming Authority (CGA)

- The Curaçao Gaming Authority (CGA) has the authority to inspect the casino's records, policies, and procedures to ensure compliance with AML and responsible gaming regulations.
- The casino must provide full access to relevant documentation and systems upon request from the CGA or other authorized regulatory bodies.

10.3 Consequences of Non-Compliance

Failure to comply with AML regulations or regulatory requirements may result in:

- Corrective actions imposed by regulatory authorities.
- Financial penalties for non-compliance.
- License suspension or revocation in cases of severe or repeated violations.

By implementing rigorous internal audits and independent compliance reviews, Apalonik B.V. ensures adherence to legal obligations, industry best practices, and regulatory expectations while fostering a secure and transparent gaming environment.

11. Compliance Oversight

Apalonik B.V. is committed to maintaining a robust compliance framework to ensure full adherence to KYC (Know Your Customer) and AML (Anti-Money Laundering) regulations. The following measures have been implemented to ensure effective compliance oversight and timely reporting of suspicious activities:

11.1 Appointment of a Compliance Officer

Apalonik B.V. has appointed a dedicated Compliance Officer responsible for overseeing all aspects of KYC and AML compliance, including:

- Overseeing KYC implementation: Ensuring that all customer identification, verification, and monitoring processes are in place and adhered to, in line with legal and regulatory requirements.
- Liaising with regulatory authorities: The Compliance Officer will serve as the main point of contact for regulatory bodies such as the Curaçao Gaming Authority (CGA) and other relevant agencies, ensuring transparent communication and timely submission of required reports.
- Ensuring the submission of Suspicious Activity Reports (SARs): The Compliance Officer will be responsible for submitting SARs for any suspicious transactions or behaviors, as required by law, and ensuring that these reports comply with local and international regulations.

11.2 Internal Audits

Apalonik B.V. will conduct periodic internal audits to evaluate the effectiveness of its KYC and AML measures. These audits are designed to:

- Assess the compliance status of the casino's KYC processes and identify any gaps or weaknesses.
- Ensure that all regulatory requirements are being met and that the internal procedures are up to date and fully effective in preventing financial crimes.
- Provide recommendations for improvement and enhancement of the compliance framework to address emerging risks or changes in regulations.

11.3 Training Programs

To ensure that all employees are well-versed in the requirements and responsibilities of the KYC and AML processes, Apalonik B.V. will implement comprehensive training programs that cover:

- Identifying fraudulent documentation: Training employees to spot fake or altered identification documents and prevent identity theft or fraud.
- Recognizing red flags for money laundering (ML) and terrorism financing (TF): Ensuring staff can identify suspicious patterns or activities that may indicate illegal financial activity, such as unusual transaction amounts, rapid fund transfers, or inconsistent betting behaviors.
- Reporting obligations under Curaçao's regulatory framework: Educating employees on their role in reporting suspicious activities, submitting SARs, and adhering to the legal obligations set out by Curaçao's laws and international standards.

12. Penalties for Non-Compliance

Apalonik B.V. takes any breach of KYC/AML regulations seriously and has a strong policy in place to deal with non-compliance. Any failure to adhere to KYC obligations may result in the following penalties:

12.1 Administrative Penalties

- **Fines:** Failure to meet KYC requirements may lead to significant administrative penalties, including monetary fines. These fines are imposed to ensure that the casino adheres to the legal and regulatory standards and serves as a deterrent against non-compliance.
- **Corrective Actions:** In addition to financial penalties, non-compliance may result in the implementation of corrective actions to rectify any deficiencies or weaknesses in the KYC procedures. These actions may include increased oversight, re-training of staff, or revising existing procedures.

12.2 Referral for Criminal Investigation

- **In cases of serious non-compliance or where fraudulent activity or money laundering is suspected,** referral for criminal investigation may be required. This may lead to criminal charges being filed against individuals involved in illicit activities, such as fraud, identity theft, or terrorism financing.
- **Cooperation with authorities:** The casino will fully cooperate with law enforcement and regulatory bodies during any criminal investigations related to non-compliance with KYC/AML laws.

By maintaining strict compliance oversight and a zero-tolerance policy for non-compliance, Apalonik B.V. ensures a secure and transparent gaming environment that adheres to all legal obligations and regulatory standards.

13. Policy Review & Updates

Apalonik B.V. has compiled an AML compliance program that involves the following:

1. A system of internal policies, procedures and controls;
2. A designated compliance officer with day-to-day oversight over the AML program;
3. An employee screening program and ongoing employee training program; and
4. An independent audit function to test the AML program.
5. This policy is reviewed and updated annually to ensure compliance with new AML regulations.
6. Employees and relevant stakeholders will be informed of any policy changes.
7. New regulatory developments and technological advancements should be incorporated into the policy framework.

Apalonik B.V. is fully committed to complying with the KYC and AML requirements to protect its players and the broader gaming community from financial crime. We will continue to review and

improve our KYC/AML processes to ensure full compliance with Curaçao regulations and international standards.
