

EDJOWA-GAMING N.V.

ANTI-MONEY LAUNDERING AND COUNTER-TERRORISM FINANCING POLICY

Document / Revision History

EDJOWA-GAMING N.V.	ANTI-MONEY LAUNDERING AND COUNTER-TERRORISM FINANCING POLICY
---------------------------	---

Change control

Revision #	Date	Written by/ Responsible Officer	Approved by	Description of Changes
V1.0	01.09.2024	MLCO Kristina Loseva	Director Andreas Andreou	Initial document created.
V2.0	21.10.2024.	MLCO Kristina Loseva	Director Andreas Andreou	Reference to the PEP definition included, Appendix A amended.
V2.1	28.11.2024	MLCO Kristina Loseva	Director Andreas Andreou	Amendments regarding the PEP/sanctions screening.
V2.2	10.02.2025.	MLCO Kristina Loseva	Director Andreas Andreou	Amendments regarding the updated AML/CFT laws and regulations in Curacao.
V2.3	14.05.2025.	MLCO Kristina Loseva	Director Dmitrijs Volks	Review of the CRA Section and Appendix C, and a general review in accordance with the AML/CFT Policy Template provided by the CGA.

CONTENTS

1. THE POLICY	4
2. DEFINITION OF MONEY LAUNDERING AND TERRORIST FINANCING	5
3. APPLICABILITY AND REGULATORY FRAMEWORK	5
4. COMPANY'S COMMITMENT TO AML/CFT COMPLIANCE	6
4.1. MAIN ML/TF PREVENTION PRINCIPLES	6
4.2. MLCO OBLIGATIONS	6
4.3. RELEVANT STAFF OBLIGATIONS	7
4.4. CONSEQUENCES OF NON-COMPLIANCE	7
5. CUSTOMER RISK ASSESSMENT & CUSTOMER ACCEPTANCE POLICY	8
5.1. GENERAL CUSTOMER ACCEPTANCE POLICY	9
5.2. GENERAL CUSTOMER SCREENING AND RISK EVALUATION PROCEDURES	10
5.3. CUSTOMER RISK LEVELS	10
5.4. SANCTIONS & PEP STATUS SCREENING	12
5.5. SANCTIONED COUNTRIES & HIGH-RISK COUNTRIES SCREENING	12
5.5.1. SANCTIONED COUNTRIES SCREENING ("BLACKLIST")	12
5.5.2. HIGH-RISK COUNTRIES ("GREYLIST")	13
5.6. CUSTOMER IDENTIFICATION	13
5.7. CUSTOMER VERIFICATION	13
5.8. CDD	14
5.9. EDD	14
5.10. ONGOING CDD	15
6. REPORTING OF SUSPICIOUS/ UNUSUAL TRANSACTIONS	16
7. RELEVANT STAFF DUE DILIGENCE	17
8. RELEVANT STAFF TRAINING	17
9. DATA STORAGE	18
9.1. REGISTER AND RETENTION OF SUSPICIOUS OR UNUSUAL TRANSACTION REPORTS	18
9.2. RETENTION PERIOD AND FORMAT OF CUSTOMER RECORDS	19
9.3. EXTENSION OF RETENTION PERIODS	19
9.4. STORAGE OF EMPLOYEE DATA (RELEVANT STAFF)	19
10. RELIANCE ON THIRD PARTIES TO PERFORM CUSTOMER DUE DILIGENCE	19
10.1. PERMITTED SCOPE OF RELIANCE	19
10.2. CONDITIONS FOR ACCEPTABLE RELIANCE	20
10.3. ASSESSMENT AND OVERSIGHT OF THIRD PARTIES	20
10.4. LIMITATIONS AND PROHIBITED RELIANCE	20
10.5. RECORDKEEPING & ACCESS	20
11. REVIEW	21
12. CONTACT INFORMATION	21
APPENDIX A - SANCTIONED COUNTRIES ("BLACKLIST") & HIGH-RISK JURISDICTIONS ("GREY LIST")	
22	
1. SANCTIONED COUNTRIES ("BLACKLIST")	22
2. HIGH-RISK JURISDICTIONS ("GREYLIST")	22

1. THE POLICY

This Policy on Anti-Money Laundering and Counter-Terrorism Financing (“**Policy**”) outlines the general unified standards and procedures of Anti-Money Laundering and Countering Financing of Terrorism (“**AML/CFT**”), which must be adhered by EDJOWA-GAMING N.V. (“**Company**”) and its Relevant Staff.

The term “**Relevant Staff**” refers to individuals or entities who play a role in the execution, oversight, or management of business functions that may involve financial transactions, customer interactions, or services that could potentially be exposed to money laundering or terrorist financing risks. Relevant Staff includes:

1. Directors and Officers: All directors, senior management, and executives who hold decision-making authority or are responsible for implementing Company-wide policies and overseeing the strategic direction, including those who supervise departments or functions that are engaged in financial transactions.
2. Employees: All full-time, part-time, and temporary staff working within any department or function that could be exposed to Money Laundering and/or Terrorism Financing (“**ML/TF**”) risks. This includes employees involved in financial operations, customer onboarding, compliance, legal, risk management, and other relevant business functions.
3. Outsourced Third-Party Providers: Any external entities or individuals that the Company engages through contracts or agreements, including contractors, sub-contractors, consultants, service providers, or any other third-party partners who handle sensitive customer information, financial transactions, or operational duties that could pose ML/TF risks. The Company recognizes the importance of ensuring that any outsourced third-party provider maintains similar standards for AML/CFT compliance and will monitor and assess the third-party's adherence to these requirements.
4. Compliance and Risk Management Personnel: Employees and individuals responsible for overseeing and ensuring adherence to this Policy, including compliance officer in AML/CFT matters (“**MLCO**”), internal auditors, and staff responsible for conducting risk assessments, monitoring financial and gaming transactions, and ensuring the timely reporting of suspicious/ unusual transactions.
5. Customer-Facing Employees: Employees who directly interact with customers and are responsible for verifying customer identities, onboarding customers, and conducting due diligence processes. These employees play a critical role in identifying and preventing potential ML/TF activities at the point of customer interaction.
6. Internal and External Auditors: Individuals or entities who are responsible for evaluating the effectiveness of the Company's AML/CFT controls, ensuring that proper measures are in place, and auditing the Company's compliance with AML/CFT obligations. This includes both internal audit functions (if any) and any external audit firms hired to assess the Company's practices.
7. Senior Management and Board of Directors: Senior management and the board have overarching responsibility for ensuring that the AML/CFT framework is properly implemented across all aspects of the Company's operations. They must ensure that adequate resources, systems, and policies are in place and that staff at all levels are trained and informed of their responsibilities under the Policy.

This Policy shall be communicated to all Relevant Staff. This ensures that all individuals and entities are fully informed of their responsibilities under AML/CFT laws and regulations, as well as the AML/CFT policies established by the Company. Whenever the Policy is updated, it shall be promptly communicated to Relevant Staff to ensure continued compliance.

In any country or jurisdiction where the applicable AML/CFT laws and regulations require the Company to establish higher standards, such country standards must be adhered to.

Compliance with this Policy is mandatory and essential for ensuring that the Company remains fully compliant with applicable AML/CFT laws and regulations of all relevant countries and jurisdictions.

The Company is committed to disrupting illicit activities by fully cooperating with relevant authorities and reporting all suspicious/ unusual transactions to the Curaçao Gaming Authority (“**CGA**”) and the Financial Intelligence Unit of Curaçao (“**FIU**”), as applicable.

2. DEFINITION OF MONEY LAUNDERING AND TERRORIST FINANCING

Money laundering is generally defined as engaging in acts designed to conceal or disguise the true origins of criminally derived proceeds so that the proceeds appear to have derived from legitimate origins or constitute legitimate assets. Money laundering may generally occur in three stages. Cash first enters the financial system at the “placement” stage, where the cash generated from illegal or criminal activities is converted into monetary instruments, such as money orders or traveller’s checks, or deposited into accounts at financial institutions. At the “layering” stage, the funds are transferred or moved into other accounts or other financial institutions to further separate the money from its criminal origin. At the “integration” stage, the funds are reintroduced into the economy and used to purchase legitimate assets or to fund other criminal activities or legitimate businesses.

Broadly, the international AML provisions are aimed at requiring to:

1. Identify customers and suspicious transactions at the placement and layering stages.
2. Keep adequate records which should prevent the integration stage being reached and provide an audit trail for investigators.
3. Report suspicious/ unusual transactions to the relevant regulatory or legislative authority.

Terrorist financing may not involve the proceeds of criminal conduct, but rather an attempt to conceal either the origin of the funds or their intended use, possibly for criminal purposes. Legitimate sources of funds are a key difference between terrorist financiers and traditional criminal organizations. In addition to charitable donations, legitimate sources include foreign government sponsors, business ownership and personal employment. Although the motivation differs between traditional money launderers and terrorist financiers, the actual methods used to fund terrorist operations can be the same or similar to methods used by other criminals to launder funds. Funding for terrorist attacks does not always require large sums of money, such funding could be of cumulative nature over extended periods, and the associated transactions may not be complex.

3. APPLICABILITY AND REGULATORY FRAMEWORK

The Company is bound by the Government of the Country of Curaçao with regards to AML/CFT. The local authorities in charge of the supervision of AML/CFT matters for the gaming sector are the CGA and the FIU.

The following key laws and regulations apply to the Company with regard to AML/CFT:

1. Online gaming laws and regulations:
 - PB 1993, no. 63 | Landsverordening buitengaats hazardspelen (National Ordinance on Offshore Games of Hazard)
 - PB 2024, no. 157 | Landsverordening op de kansspelen (National Ordinance on Games of Chance)
2. General AML/CFT laws and regulations
 - Regulations for the combating of Money Laundering, the Financing of Terrorism and Proliferation of weapons of mass destruction, Applicable to Curaçao casinos and providers of other online games, January 2025
 - GCB Requirements for Compliance Officer Based on NOIS/NORUT, January 2025
3. Identification when rendering services:
 - PB 2017, no. 92 | Landsverordening identificatie bij dienstverlening (GT) (National Ordinance on identification when rendering services (LID))
 - P.B. 2024, no. 41 | Wijziging LMOT/ LID (Amendment of the National Ordinance on Identification when rendering Services (PB 2017, no. 92) and the National Ordinance on the Reporting of Unusual Transactions (PB 2017 no. 99))
 - LB no. 19/0282 | Landsbesluit toezichthouder identificatie bij dienstverlening kansspelsector (Appointment of the GCB as the AML/CFT supervisor for the LID for the gaming industry)
4. Suspicious/ unusual transactions reporting:
 - PB 2017, no. 99 | Landsverordening melding ongebruikelijke transacties (GT) (National Ordinance on the reporting of unusual transactions (LMOT))
 - P.B. 2024, no. 41 | Wijziging LID/ LMOT (Amendment of the National Ordinance on Identification when rendering Services (PB 2017, no. 92) and the National Ordinance on the Reporting of Unusual Transactions (PB 2017 no. 99))

- [LB no. 19/0283 | Landsbesluit toezichthouder ongebruikelijke transacties kansspelsector](#) (Appointment of the GCB as the AML/CFT supervisor for the LMOT for the gaming industry)
 - [PB 2020, 157 | Landsbesluit inzake regels voor melding ongebruikelijke transacties \(Landsbesluit goAML meldportaal\)](#) (Rules for reporting unusual transactions)
 - [PB 2015, 73 | Regeling indicatoren ongebruikelijke transacties](#) (Indicators for recognizing unusual transaction)
 - [PB 2024, 60 | Wijziging van de Regeling indicatoren ongebruikelijke transacties](#) (Amendment of the Indicators for recognizing unusual transactions)
5. The Company also consistently adheres to relevant international standards, including the recommendations of the Financial Action Task Force on Money Laundering (“**FATF**”), the [guidelines and instructions of the European Commission](#), and the [directives of the European Union on AML/CFT](#).
6. Reference is also made to the National and Supranational ML/FT Risk Assessments, in particular to those sections relating to the remote gaming sector:
- [Curaçao’s National Strategy and Action Plan to counter Money Laundering and Financing of Terrorism and Proliferation June 4, 2024](#)
 - [Report on the National Risk Assessment \(on\) Money Laundering Curacao 2020, Published May 2023](#)

4. COMPANY’S COMMITMENT TO AML/CFT COMPLIANCE

The measures, procedures and controls defined in this Policy are kept under regular review so that risks resulting from changes in the characteristics of existing customers, new customers and services are managed and countered effectively.

4.1. Main ML/TF Prevention Principles

1. The Company shall undertake all measures at its capacity to not be used as a facility for ML/TF or assisting others to do so intentionally or otherwise.
2. The Company shall only carry on business relationships with persons whom they have:
 - adequately identified,
 - adequately verified,
 - adequately monitored,
 - in whom there is no suspicion of criminal or terrorist activity (i.e., [sanctions screening](#)), and
 - obtained senior management approval to service the Politically Exposed Persons (“**PEP**”) as defined in the [FATF Guidance politically exposed persons](#) and [Regulations for the combating of Money Laundering, the Financing of Terrorism and Proliferation of weapons of mass destruction](#), Applicable to Curaçao casinos and providers of other online games, January 2025 (i.e., [PEP screening](#)). Senior management are the persons who determine the day-to-day operations or those directly below the level of those determining the day-to-day operations; the approval can also be from the MLCO.
3. The MLCO must investigate, analyse, consult and, if appropriate, report the suspicious/ unusual transactions to the FIU and take any other action considered legal and necessary.
4. The Company must not impede, by action or inaction, any official investigation of ML/TF.
5. The Company shall, as much as possible, follow the relevant 40 + 9 recommendations of the Financial Actions Task Force (www.fatf-gafi.org).
6. The Company shall follow all AML/CFT laws and regulations.
7. The Company shall provide the necessary training for its employees in AML/CFT and fraud procedures.
8. The Company shall keep records of all procedures carried out and suspicious/ unusual transactions reporting effected.

4.2. MLCO Obligations

The Company must designate an MLCO who will be responsible for organizing the implementation of ML/TF prevention measures as specified in the applicable AML/CFT laws and regulations, and for liaising with the FIU. Only a person who has the education, professional suitability, the abilities, personal qualities, experience and impeccable reputation required for performance of the duties of a compliance officer may be appointed as a MLCO.

The MLCO obligations include but are not limited to:

1. Designing, implementing and making necessary changes to the AML program:
 - Establishment of appropriate internal control procedures with the purpose of prevention of monetary operations and transactions related to ML/TF - customer and beneficial owner due diligence (“**CDD**”), submission of suspicious/ unusual reports and information to the FIU, storage of information according to the applicable laws and regulations, risk assessment, risk management (taking into account the type of product, service or transaction, geographical risk, etc.), compliance management and communication;
2. Initial and ongoing Relevant Staff training:
 - Undertaking of appropriate measures so that the Relevant Staff is aware at all times of the provisions currently in force. Such measures shall include participation of the Relevant Staff in special ongoing training programs to help them recognize operations which may be related to ML/TF and provision of instruction to said employees as to how to proceed in such cases.
 - Keeping copies of all training materials. Updated AML training is given annually at minimum plus additional training when the need arises, for example in the case of significant changes in the AML/CFT laws and regulations. Records must be retained of all training sessions including dates, personnel, who received training (name, surname, functions in the Company, their signatures), compliance officer who trained the Relevant Staff (name, surname, functions in the Company, their signatures).
3. Adherence to the applicable AML/CFT laws and regulations:
 - Monitoring all amendments in the AML/CFT laws and regulations, and updating internal instructions according to up-to-date information.
 - Reviewing and controlling overall compliance policy for prevention of ML/TF.
 - Ensuring adequate resources are provided for the proper training of the Relevant Staff and the implementation of risk systems.
 - Remaining informed on the local and international developments on ML/TF and to make suggestions to management for improvements.
4. Transactions monitoring:
 - Analysing transactions and verifying whether any are subject to reporting to the FIU.
 - Reviewing all internally reported suspicious/ unusual transactions for their completeness and accuracy with other sources.
 - Keeping records of internally and externally reported suspicious/ unusual transactions.
 - Executing closer investigation of unusual transactions if necessary.
 - Preparing the external report of suspicious/ unusual transactions.
5. Preparing periodic information on the Company's efforts against ML/TF.

The above-mentioned responsibilities shall be included in the job description of the MLCO. The job description shall be signed off and dated by the officer, indicating his/her acceptance of the entrusted responsibilities.

4.3. Relevant Staff Obligations

All Relevant Staff is responsible for considering the Policy and understanding responsibilities. All Relevant Staff must ensure that the Company procedures are adhered to and must obtain all documentary evidence as outlined within the Policy. In addition, the Relevant Staff must ensure that all suspicious/ unusual circumstances are immediately reported to MLCO.

A dedicated 'Suspicious/ Unusual Transactions' email inbox (legal@planbet.com) is available to Relevant Staff for the purpose of immediately reporting, internally, any accounts or transactions they suspect may involve ML/TF. These reports are submitted to the MLCO, who is responsible for reviewing the information and determining whether a report to the FIU is required. The timeline for reporting to the FIU is set out in this Policy.

4.4. Consequences of Non-Compliance

1. Risks of Non-Compliance. Failure to comply with this Policy exposes the Company to several significant risks, including but not limited to:
 - Legal and Regulatory Penalties. Non-compliance with AML/CFT laws and regulations can result in severe legal consequences, including fines, sanctions, or criminal prosecution. Regulatory bodies such as CGA and/or the FIU may impose substantial penalties on businesses found in

- violation of AML/CFT laws and regulations. These penalties can include heavy fines, restrictions on business operations, and possible loss of business licenses.
- **Reputational Damage.** Non-compliance with AML/CFT laws and regulations can severely damage the Company's reputation. A tarnished reputation can result in a loss of customer trust, reduced business opportunities, and the potential for long-term negative publicity. This could undermine the Company's standing with investors, regulators, and business partners.
 - **Business and Financial Risks.** Failure to identify and report suspicious/ unusual transactions can result in the Company becoming inadvertently involved in illegal activities such as ML/TF. This may expose the Company to financial losses, including the freezing of assets, increased regulatory scrutiny, or even forced liquidation.
2. **Disciplinary Actions for Employees.** Employees found in violation of this Policy may face disciplinary action up to and including:
 - **Verbal or Written Warnings.** For minor or first-time offenses, a verbal or written warning may be issued.
 - **Suspension or Termination of Employment.** For repeated violations or serious breaches, employees may face suspension or termination. Termination may be pursued in cases of deliberate non-compliance or willful negligence that jeopardizes the Company's compliance standing.
 - **Legal Action.** If the violation involves fraudulent activity, deliberate ML/TF, or other criminal acts, the Company may pursue legal action against the employee. This may include criminal charges, civil lawsuits, or reporting to law enforcement agencies.
 3. **Consequences of Non-Compliance by Third-Party Contractors and Outsourced Providers.** Third-party service providers, including contractors, sub-contractors, and outsourced personnel, who are engaged in functions that may expose the Company to ML/TF risk, are also required to comply with this Policy.
 - Non-compliance by third parties may lead to immediate termination of contracts, blacklisting from future engagements, or reporting to regulatory authorities, where applicable.
 - The Company reserves the right to conduct periodic reviews, audits, or assessments of third-party compliance as part of its broader AML/CFT risk management framework.
 4. **Legal and Regulatory Consequences.** Non-compliance with AML/CFT laws and regulations may also trigger significant legal implications for the Company:
 - **Fines and Penalties.** Regulatory authorities may impose substantial fines for non-compliance, which could be both individual (against responsible employees) and corporate in nature. These fines can range depending on the severity of the violation.
 - **Revocation of Business Licenses.** In extreme cases, the Company's ability to operate may be jeopardized through the revocation or suspension of necessary licenses or permits, effectively shutting down business operations until compliance is restored.
 - **Increased Scrutiny and Audits.** Violations of this Policy may result in increased oversight from regulatory bodies, leading to more frequent and invasive audits, investigations, and monitoring by authorities.
 5. **Business Risk and Customer Impact.** Non-compliance can also lead to:
 - **Loss of Business Partnerships.** Many partners and clients conduct business with companies that are compliant with AML/CFT laws and regulations. Non-compliance can result in the termination of business relationships or prevent the Company from entering new partnerships, damaging revenue and growth prospects.
 - **Inability to Conduct Certain Transactions.** Due to regulatory barriers or penalties, the Company may find itself unable to engage in specific transactions, including international trade, banking, or investment activities, which can affect its overall business operations and competitiveness.
 6. **Importance of Reporting and Cooperation.** Employees are encouraged to immediately report any concerns related to potential violations of this Policy or suspicious/ unusual transactions. The Company will not tolerate retaliation against any individual who, in good faith, reports a concern regarding non-compliance or possible illegal activity. All reports will be handled confidentially, and the Company will take prompt action to investigate and address the issue.

5. CUSTOMER RISK ASSESSMENT & CUSTOMER ACCEPTANCE POLICY

For the purpose of the identification, assessment, and analysis of ML/TF risks associated with the Company's principal business activities, the Company shall conduct a comprehensive Business Risk Assessment ("BRA"). The scope and depth of such an assessment shall be commensurate with the nature, scale, and complexity of the Company's operations. The BRA shall be documented, maintained, and treated as a separate and distinct

document forming part of the Company's overall AML/CFT compliance framework. It shall be subject to periodic review and update, in accordance with applicable AML/CFT laws and regulations.

In conjunction with the BRA, the Company shall also conduct a Customer Risk Assessment ("**CRA**") for each customer, with the objective of identifying, categorizing, and managing the level of ML/TF risk posed by individual customers. The CRA shall consider multiple risk factors including, but not limited to, geographic location, customer profile, nature and purpose of the business relationship, transaction behavior, and source of funds. Based on the outcome of the CRA, customers shall be classified under predefined risk categories (e.g., Low, Medium, or High Risk) and subject to corresponding due diligence measures.

Both the BRA and CRA shall collectively inform the Company's risk-based approach to AML/CFT compliance, ensuring that controls are proportionate and effectively targeted to areas of higher risk exposure.

5.1. General Customer Acceptance Policy

The Company's Customer Acceptance Policy ("**CAP**") applies a risk-based approach to customer acceptance, in full compliance with applicable AML/CFT laws and regulations. Customer eligibility is also determined by the Company's internal BRA and predefined risk appetite.

To ensure the integrity of its operations and prevent abuse of its services, access is strictly limited to individuals who meet the Company's legal, regulatory, and risk-based criteria. As such, access to the Company's services is expressly prohibited for individuals who:

1. Attempt to access services through anonymous, pseudonymous, or otherwise unidentified accounts, or fail or refuse to complete the required customer identification and verification procedures. Each player must register using accurate personal information prior to gaining access to the Company's services and must undergo Know Your Customer ("**KYC**") verification upon certain triggers, as defined in this Policy. Gaming accounts may only be operated by the registered individual; third-party access or use is strictly prohibited. The Company actively monitors indicators of linked, duplicate, or fraudulent accounts through system-driven data analysis and identity correlation tools.
2. Are under 18 years of age, or under 21 where a higher minimum legal gambling age is imposed by applicable local laws or regulations.
3. Reside in jurisdictions subject to international sanctions, including but not limited to those imposed by the United Nations, European Union, United States Office of Foreign Assets Control (OFAC), or the FATF. Residency is determined based on customer-submitted documents and geolocation tools.
4. Appear on official international sanctions or watchlists, including those maintained by the UN, EU, UK, OFAC, or FATF. All customers are screened against relevant sanctions, watchlists, and enforcement databases during onboarding and at regular intervals thereafter. Where a positive match is identified, the account is immediately blocked pending further review. If confirmed as a true match, the business relationship will be terminated, and the matter escalated to the MLCO for further assessment and potential submission of a suspicious/ unusual transactions report to the FIU.
5. Are identified as PEPs without the prior written approval of senior management. All customer records are routinely screened against global PEP databases. Where a potential PEP is identified, the individual's risk profile is elevated, and their account may only be approved upon formal review and acceptance by the appropriate senior compliance authority.
6. Are reasonably suspected of involvement in ML/TF, or other predicate criminal activity, as defined under applicable AML/CFT laws and regulations. Where such suspicion arises, either through internal monitoring or adverse media, the Company may suspend the account, conduct Enhanced Due Diligence ("**EDD**"), and escalate the case to the MLCO for formal investigation.
7. Have self-excluded from gambling activities, either:
 - through the Company's own internal self-exclusion procedures, initiated voluntarily by the player or in accordance with responsible gambling protocols, or
 - via a player-initiated self-exclusion mechanism formally recognized under the CGA Responsible Gambling policy, where applicable and effective from the relevant regulatory implementation date.
8. Submit documentation or information that is determined to be false, manipulated, misleading, or otherwise unreliable, whether during onboarding, periodic reviews, or any point in the customer relationship. This includes, but is not limited to, forged identification documents, altered utility bills, or fabricated source of funds evidence.
9. Exhibit a risk profile that exceeds the Company's accepted risk appetite/ threshold, as identified through ongoing monitoring, EDD, or transaction analysis. If a customer's risk level is deemed no longer acceptable — for example, due to emerging financial crime indicators, geopolitical exposure, or

escalated behavioral risks — the Company reserves the right to restrict or terminate the relationship in accordance with its internal procedures.

5.2. General Customer Screening and Risk Evaluation Procedures

Customer screening constitutes a core element of the Company's AML/CFT framework. It is a preventative measure designed to identify and mitigate potential ML/TF, and other financial crime risks presented by both prospective and existing customers. Customer screening is carried out at various stages of the customer lifecycle—at onboarding, during periodic reviews, and on a continuous basis as part of the Company's ongoing monitoring obligations. The objective is to ensure that the Company maintains full compliance with applicable AML/CFT laws and regulations, international standards (including those of the FATF), and licensing conditions imposed by the competent authorities.

1. The Company performs the screening of each customer to assess the customer risk and any changes in the customer risk level.
2. When conducting customer screenings, the Company seeks to achieve 3 main objectives:
 - Conduct a CRA to evaluate potential risks associated with customers and transactions,
 - Ensure compliance with sanctions to avoid violating any applicable sanctions, AML/CFT laws and regulations,
 - Protect against regulatory fines to mitigate the risk of incurring fines and penalties from regulatory authorities.
3. With sanctions & PEP status screening the Company ensures that existing or potential customers are not present in any of the sanctions' lists, banned or wanted lists, are not classified as PEPs and do not have any adverse media data on file.
4. The Company performs customer identification and verification as it is essential for:
 - Compliance with regulatory requirements to meet legal obligations and ensure adherence to AML/CFT laws and regulations,
 - Risk management to assess and mitigate risks associated with fraud and other financial crimes, protecting both the Company and its customers,
 - Maintaining trust to foster a secure and trustworthy environment for all customers by ensuring that all transactions are legitimate,
 - Preventing identity theft to safeguard against the misuse of personal information and reduce the risk of identity theft,
 - Enhancing customer experience to streamline processes and provide better services by verifying customer identities accurately.
5. The Company should regularly, at least once per year, check the risk level of their customers following their screening if the customer is considered as "active".
6. Hence, these methods not only provide comprehensive risk control for the Company but allow them to fulfil AML/CFT obligations effectively.

5.3. Customer Risk Levels

As a result of the BRA, the Company shall classify customer risk into 3 distinct categories as follows:

1. Low risk. Customers classified as Low Risk represent a minimal likelihood of being involved in ML/TF activities. These customers are typically subject to Standard Due Diligence ("**SDD**") procedures. SDD involves the collection, verification, and ongoing monitoring of basic Know-Your-Customer ("**KYC**") information. Customers within this classification will be monitored on an ongoing basis for suspicious/unusual transactions. This monitoring involves assessing the regularity of transactions, consistency with the customer's known profile, and ensuring that transactions align with the expected volume and nature of activity.
2. Medium risk. Customers classified as Medium Risk present a higher likelihood of being involved in ML/TF activities compared to Low-Risk customers. Such customers are subject to increased scrutiny and enhanced monitoring procedures. If a customer fails to provide the requested documentation or information at any stage in the customer lifecycle, especially in situations where documentation has been specifically requested due to certain defined trigger events, the account will be placed under heightened monitoring. Trigger events that could elevate a customer's risk profile include, but are not limited to:

- Unusual or Significant Increases in Transaction Volume or Frequency. Sudden or unexplained increases in deposits, bets, or withdrawals inconsistent with the customer's previous behavior or stated source of funds.
- Frequent Use of Multiple Payment Methods or Payment Instruments. The customer begins using multiple credit cards, e-wallets, or other payment mechanisms, particularly from different jurisdictions.
- Discrepancies in Customer Information. Inconsistencies or contradictions identified in the customer's KYC documentation or personal data, including name, address, or declared occupation.
- Customer Fails to Complete KYC or Verification Process Upon Request. Refusal, delay, or repeated failure to provide identity documents or proof of address when triggered by risk-based thresholds.
- Becoming a PEP. The customer is identified or declared as a PEP or is linked to a PEP.
- Activity Suggesting Use of Third Parties or Proxy Betting. The account activity indicates that the account may be used by or on behalf of another person, including patterns suggesting third-party use or proxy gambling.
- Unusual Patterns of Winnings or Losses. Repeated large wins followed by immediate withdrawal without sustained play, or frequent high losses with continued top-ups from unclear sources.
- Use of High-Risk Geographical Locations. Deposits or withdrawals are made from or to jurisdictions known to have weak AML/CFT controls, be subject to sanctions, or be listed as high-risk.
- Structuring of Transactions to Avoid Reporting Thresholds. Customer conducts multiple smaller transactions in a pattern intended to avoid detection or reporting limits.
- Change in Gaming Behavior. Sudden engagement in higher-risk games (e.g., from low-stakes to high-stakes betting) or increase in bet size without a clear rationale.
- Unusual Login or Access Patterns. Frequent logins from multiple IP addresses, different geographic regions in short succession, or use of anonymizing services such as VPNs.

In such instances, the Company's compliance team, under the direction of the MLCO, will review and assess the customer's transactional activity and related documentation. Where the level of risk is deemed elevated and adequate documentation is not forthcoming, the Company reserves the right to:

- Impose temporary or permanent restrictions on the customer's gaming account;
- Freeze deposits or withdrawals pending investigation;
- Escalate the customer to High-Risk classification and apply EDD; or
- Terminate the business relationship in accordance with the Company's policies and applicable AML/CFT laws and regulations.

3. High risk. Customers classified as High Risk are considered to present a significant or substantial risk of involvement in ML/TF. These customers are subject to EDD procedures, which include a much more in-depth review of the customer's background, financial activities, and sources of funds. Triggers and risk indicators that may lead to a customer being classified as High Risk include, but are not limited to:
 - Suspicious Transaction Patterns or Behaviors. The identification of activity that deviates materially from the customer's declared profile, such as unusually high-value deposits, frequent large withdrawals shortly after deposits, or erratic betting behavior that suggests layering or structuring.
 - Escalation from Medium Risk Following a Trigger Event. A customer previously classified as Medium Risk may be elevated to High Risk due to failure to provide requested KYC documents, persistent inconsistencies in provided information, or the emergence of new risk indicators such as becoming a PEP.
 - Association with High-Risk Jurisdictions or Entities. The customer is found to be located in, or transacting with, countries identified by FATF or local regulators as high-risk, non-cooperative, or under sanctions. This also applies where the customer maintains business or personal links with entities or individuals subject to similar designations.
 - Indicators of Possible Proxy Usage or Fraudulent Account Behavior. Evidence suggesting that the account may be operated by or on behalf of another person, or involvement in collusive behavior, duplicate accounts, or other abuse mechanisms commonly exploited in the gambling sector.
 - Unusual Funding Sources or Methods. Use of complex or opaque funding methods, including frequent top-ups from unrelated third parties, payments from unknown or unverifiable sources, or methods inconsistent with the customer's stated occupation or profile.

- Refusal to Cooperate with EDD Requests. A customer who displays reluctance, delay, or refusal in providing additional information or supporting documentation when requested, particularly after being notified of enhanced review measures.

EDD for High-Risk Customers will typically include, but is not limited to:

- In-depth verification of the customer's identity, business operations, and sources of wealth.
- Detailed analysis of the customer's financial history and transaction patterns, including the identification of the origin and destination of funds.
- Enhanced verification of documents provided, including third-party validation where necessary.
- Ongoing and more frequent monitoring of all transactions and activities, with a focus on large or complex transactions that may deviate from the expected norms.
- The Company may also apply further monitoring or implement other risk mitigation measures, including, if necessary, reporting suspicious/ unusual transactions to relevant authorities, including the FIU and the CGA.

5.4. Sanctions & PEP Status Screening

The Company performs sanctions lists & PEP status screening upon the 1st deposit and repeatedly annually after the initial screening if the customer is considered "active".

An "active" customer is considered such customer whose gaming account is not suspended, closed, terminated or considered inactive, who is not under self-exclusion or ban applied by the customer or the Company, and who has not logged into the gaming account and made the deposit or requested withdrawal regardless of the threshold within a year after the initial/ last screening.

If the customer is considered "inactive", then his/her repeated screening in the context of this Section will be performed immediately upon the gaming account login if the last screening was performed at least a year ago. Sanctions & PEP status screening is done via access to global databases like watch lists, PEPs and sanctions lists (for example, <https://dilisense.com/en>, etc.).

5.5. Sanctioned Countries & High-Risk Countries Screening

In accordance with applicable AML/CFT laws and regulations, the Company implements jurisdiction-based screening measures to prevent engagement with individuals from sanctioned or high-risk countries. This process supports the Company's broader customer due diligence obligations and ensures compliance with global regulatory expectations.

Customers are screened based on their nationality, residency, IP location, and other geographic indicators to identify links to jurisdictions that are either subject to international sanctions ("*blacklisted*") or considered to pose elevated money laundering or terrorism financing risks ("*greylisted*").

The Company distinguishes between:

- Sanctioned Countries, where any customer relationship is strictly prohibited; and
- High-Risk Countries, where EDD and risk mitigation controls are applied before accepting or maintaining a customer relationship.

These jurisdictional assessments are conducted upon onboarding and updated regularly using reliable databases, sanction lists, and FATF guidance.

5.5.1. Sanctioned Countries Screening ("*Blacklist*")

The Company shall be prohibited to perform any actions the performance of which is prohibited by the international sanctions implemented in the Curaçao.

Accordingly, no individual or entity located in or associated with jurisdictions designated as High-Risk Jurisdictions subject to a Call for Action (commonly referred to as "**Sanctioned Countries**" or "**Blacklist Countries**"), as published by the Financial Action Task Force (FATF) (<https://www.fatf-gafi.org/en/countries/black-and-grey-lists.html>), shall be permitted to:

- Register or access a gaming account;
- Maintain or operate an existing gaming account;

- Initiate or receive any form of payment or financial transaction, including deposits, withdrawals, or transfers, through financial institutions, payment processors, or instruments originating from or routed through such jurisdictions.

To ensure enforcement of this restriction, the Company has implemented technical and procedural controls, including:

- IP-based and geolocation blocking affected jurisdictions at registration and login stages;
- Screening of payment instruments and transaction metadata to detect the origin of funds or financial routing through sanctioned or high-risk jurisdictions;
- Real-time monitoring of account activity and transaction behavior for indicators of jurisdictional masking, proxy usage, or circumvention techniques.

Any attempt to register, fund, or operate an account from a Sanctioned Country will result in the automatic denial or suspension of the gaming account and may lead to the submission of a suspicious/ unusual transaction report to the FIU, where applicable.

All customers are checked versus Sanctioned Countries upon the 1st deposit and repeatedly whenever there is a change in the customer's jurisdiction of residence, whenever the Company upon the customer verification process has established that the customer's place of birth or residence is within a Sanctioned Country.

Sanctioned Countries list provided in Appendix A.

5.5.2. High-Risk Countries ("Greylist")

Prospecting customers from countries in which, based on the information officially published by international intergovernmental organizations, ML/TF prevention measures are insufficient or do not correspond to international standards ("**High-Risk Countries**" or "**Greylist Countries**"), and which might lie outside of the business risk appetite might be blocked from registration and/or login, and/or EDD shall be applied to such customers.

The MLCO reviews the list of accepted countries on a regular basis, in line with certified and credible sources of information regarding the level of ML/TF risks, corruption, political unrest, and countries subject to sanctions, embargos or similar measures, countries with no or little AML/CFT laws and regulations, and monitoring by FATF, or countries providing funding and/or support for terrorism.

Greylist Countries list provided in Appendix A.

5.6. Customer Identification

The Company performs identification of the customer upon the gaming account set-up or latest upon the 1st deposit. When identifying the player, at a minimum the following information must be collected:

1. Name, surname,
2. Date of birth,
3. Permanent residential address,
4. Customer's email address and/or phone number,
5. Place of birth,
6. Nationality, and
7. Identity number (if any),
8. Payment details.

However, in low-risk scenarios the Company may limit identification to the personal details set out in (1) to (4). On the other hand, in high-risk situations, it is possible that the Company considers the collection of additional personal details necessary to mitigate the higher risk of ML/FT.

5.7. Customer Verification

The Company performs verification of identity when engaging in financial transactions equal to or in excess of 2000 EUR. This implies that all CDD measures must have been conducted at the time the threshold is reached. The Company endeavours to verify the data supplied by the customers upon the 2000 EUR deposit threshold

and/or upon the 1st withdrawal request (notwithstanding to the amount), through methods and data available depending on country of residence.

The Company verifies the correctness of the data specified by the customer, using information originating from a credible and independent source for that purpose. Where the person has a valid document specified below, or an equivalent document, the person is identified, and the person's identity is verified on the basis of the document or using means of electronic identification and trust services for electronic transactions, and the validity of the document appears from the document or can be identified using means of electronic identification and trust services for electronic transactions, no additional details on the document need to be retained.

1. Required Proof of Identity – Passport or Driving License or National Identity Card.
2. Proof of Address – Utility Bill / Official or Bank Correspondence.
3. Proof of ownership of the linked payment method – Bank Statement or Card Statement (figures may be blocked out).

The documents shall be preferably sent in digital format signed with a person's own digital signature. The Company may ask for these documents also in notarized format (whereby the validity (originality) of the document is confirmed by the notary public).

Customer verification is done either manually by the Relevant Staff by requesting CDD documentation/ information as provided in this Policy from the customer or automatically/ semi-automatically via 3rd party providers (for example, <https://sumsub.com/>, <https://www.alloy.com/>, etc.).

In the event behavioural triggers occur, the Company may ask from the customer presentation of additional documents. In certain situations, it may be necessary to establish the source of funds and the wealth of the customer, or ask for other information in respect of the nature of the transaction, aim of transaction etc. The Company shall use all reasonable efforts to obtain this information.

5.8. CDD

Before establishing a business relationship with the customer, the Company must apply the following due diligence measures:

1. Identification of a customer and verification of the acquired information based on information obtained from a reliable and independent source, including using means of electronic identification and of trust services for electronic transactions.
2. Verification of a customer's residential address by request for provision of secondary document, such as bank statement or utility bill showing residential address.
3. Verification of a customer's e-mail address by sending an email with a verification link.
4. The Company shall be prohibited from establishing business relationships without identification of the customer and sanctions & PEP status screening, and to continue business relationships with the customer when the applicable verification threshold is reached by requesting the customer submit data confirming their identity, or where there is a substantiated suspicion that the data recorded in these documents is false or falsified.
5. The Company shall be prohibited from establishing or continuing business relationships and carrying out transactions when it is not possible to fulfil the due diligence requirements established in this Policy:
 - Where, in the cases established by this Policy, the customer fails to submit the data confirming his identity, or where he submits incomplete data,
 - Where the data are incorrect, where the customer avoids submitting the information required for establishing his identity or the submitted data are insufficient for that purpose,
 - When there are doubts about the veracity or authenticity of the previously obtained identification data of the customer,
 - In any other case, when there are suspicions that the act of ML/TF is, has been or will be carried out.

5.9. EDD

Measures of EDD goes beyond that of the CDD. Enhanced measures are warranted especially in cases identified as high risk. The checks shall cover (but not limited to):

1. Suspicious Transactions.
2. Customers located in High-Risk Countries.

3. Politically Exposed Persons (PEP's).
4. Customers reached a threshold set in Section 5.4.
5. Other customers that the Company considers to be high-risk.

In the case of High-Risk customers, the Company applies the following additional measures to effectively manage and mitigate its risks:

1. Requiring the quality and extent of requisite identification data to be of a certain standard (e.g., documents from independent and reliable sources, certified documents, third person information, documentary evidence).
2. Obtaining additional data and information from the customer, where this is appropriate for the proper and complete understanding of their activities and source of wealth, source of funds.
3. Assessing the individual's history, reputation, and personal and professional background through review of public records – including civil, criminal and bankruptcy / insolvency records, identification of professional affiliations.
4. Search for adverse media and internet research.
5. Applying of ongoing monitoring of High-risk customers' transactions and activities.

The Company shall use all reasonable efforts to obtain this information. All information should be checked against all available databases.

5.10. Ongoing CDD

The Company must apply CDD measures not only in respect of new customers but also in respect of existing ones, having regard to the level of risk, in the event of new circumstances or new information related to the determination of the level of risk posed by the customer, their identification information, activities and other relevant circumstances.

Continuous monitoring is in place to track customer behaviour and where transactions are deemed to be unusual, further investigations are undertaken by the MLCO. These investigations will include, but not be limited to, the following:

1. Inactivity period followed by intense activity.
2. Game type behavior and amounts played.
3. Withdrawals amount against deposits amounts.
4. Transactional behavior.
5. Payment method used.

During the period of cooperation with the customer, the Company is obliged in all cases:

1. To carry out the ongoing monitoring of the customer's activity, used payment methods, including scrutiny of transactions undertaken throughout the course of such relationships, to ensure that the transactions being conducted are consistent with the Company's knowledge of the customer, risk profile as well as the source of funds.
2. To ensure that the documents, data or information submitted by the customer during due diligence are appropriate, relevant, regularly reviewed and kept up to date.
3. To monitor the achievement of the threshold of 2000 EUR deposited into the customer's account, whether in a single transaction or in several transactions that make up the specified amount. The Company calculates 2000 EUR deposit threshold on the basis of a rolling period of 180 days.
4. The Company must pay attention to any activity which they regard as likely, by its nature, to be related to ML/TF, and in particular to complex or unusually large transactions, and relationships or deposits/withdrawals with customers from High-Risk Countries. The Company must examine the basis for and purpose of execution of such operations or transactions and the results of the investigation must be recorded in writing.
5. The Company may, in accordance with internal policies and internal control procedures, refuse to execute the deposits/withdrawals and terminate the transactions or relationship with the customer, where:
 - The customer avoids submitting, or refuses to submit, additional information to the Company, at its request and within the specified time limits,
 - Where there is suspicions or substantial grounds to suspect that ML/TF was, is, or will be performed, or it has been attempted,
 - Where there are suspicions or substantial grounds to suspect that the customer's funds have been obtained from criminal activity,

- Where there is suspicions or substantial grounds to suspect that the transactions or activities are related to terrorist financing.

6. REPORTING OF SUSPICIOUS/ UNUSUAL TRANSACTIONS

The Company must pay attention to any activity which they regard as likely, by its nature, to be related to ML/TF, and in particular to complex or unusually large transactions, and all unusual patterns of transactions which have no apparent economic or visible lawful purpose, and relationships or monetary operations with customers from third countries in which, based on the information officially published by international intergovernmental organizations, ML/TF prevention measures are insufficient or do not correspond to international standards. The Company must examine the basis for and purpose of execution of such operations or transactions and the results of the investigation must be recorded in writing.

The Company must report to the FIU any suspicious/ unusual transactions:

1. Cases where it is aware of, obtains information concerning, has suspicions or has substantial grounds to suspect that ML/TF was/ is/ or will be performed/ or it has been attempted.
2. Cases where they have suspicion or sufficient grounds to suspect that the customer's funds have been obtained from criminal activity.
3. Cases where they have a suspicion or sufficient grounds to suspect that the transactions or activities are related to terrorist financing.

The Company must report suspicious/ unusual transactions to the FIU immediately, but not later than within 2 working days after identifying the activity or facts or after becoming suspicious.

The Company must immediately submit to the FIU all the information available to the Company, which the FIU requested in its enquiry.

Upon establishing that their customer is carrying out a suspicious monetary operation or transaction, the Company must suspend the operation or transaction disregarding the amount of the monetary operation or transaction and, not later than within 1 working day from the suspension of the monetary operation or transaction, report this operation or transaction to the FIU.

Where the postponement of the transaction may cause considerable harm, it is not possible to omit the transaction or it may impede catching the person who committed possible ML/TF, the transaction or professional act shall be carried out or the official service will be provided, and a report will be submitted to the FIU:

1. A report to the FIU is submitted via GoAML reporting portal (link to register in GoAML - https://portal.fiucuracao.cw/goAMLWeb_PRD/Account/LogOn).
2. The data used for identifying the person and verifying the submitted information and, if any, copies of the documents are added to the report.
3. The structural unit of the Company, a member of a management body and any employee are prohibited to inform a person about a report submitted on them to the FIU, plan to submit such a report or the occurrence of reporting as well as about any precept made by the FIU or about the commencement of criminal proceedings. After a precept made by the FIU has been complied with, the Company may inform a person that the FIU has restricted the use of the person's account or that another restriction has been imposed.

The prohibition is not applied upon submission of information to competent supervisory authorities and law enforcement agencies.

The exchange of information must be retained in writing or in a form reproducible in writing for the next 5 years and information is submitted to the competent supervisory authority at its request.

The Company, its employee, representative and/or the person who acted on its behalf are not liable for damage caused to a person or customer participating in a transaction made in economic or professional activities, in performing a professional act or in the provision of a professional service:

1. Upon performance of duties and obligations arising from AML/CFT laws and regulations in good faith, from failing to make the transaction or from failing to make the transaction within the prescribed time limit.
2. In connection with the performance of the duty to report in good faith.

The Company establishes a system of measures ensuring that the employees and representatives of the Company who report of a suspicion of ML/TF to the FIU are protected from being exposed to threats or hostile action by other employees, management body members or customers of the Company, from adverse or discriminatory employment actions.

7. RELEVANT STAFF DUE DILIGENCE

Relevant Staff are at least those persons within the Company who have customer contact or handle and assess customer documents and transactions, who are aware of all activities and risks, irrespective of their level of seniority. All members of the board, (senior) management and the MLCO also have an essential role.

The MLCO has a good knowledge of the risks and can guide the process, but (senior) management should also have a clear understanding of the ML/TF risks. Moreover (senior) management needs to establish the Company's risk appetite.

Relevant Staff due diligence is a procedure used to screen Relevant Staff. The screening procedure aims to identify and minimize business exposure to the ML/TF risk. Relevant Staff's due diligence is based on the risk assessment of the business and the roles within it.

Any employee whose role means they might be able to facilitate ML/TF must be screened. This includes:

1. Prospective employees before they are employed to such a position.
2. Existing employees before they are transferred or promoted to such a position.
3. To screen both current and potential employees the Company should:
 - Identify them,
 - Verify them,
 - Confirm their employment history (e.g., through references),
 - Decide whether they are suitable for the position and do not pose a risk to the Company.

The Company shall take into consideration the knowledge and qualifications necessary for the duties, responsibilities and authorization of the Relevant Staff.

Roles with duties that might make the Relevant Staff a target for collusion with, or coercion by, criminal groups must be subject to a tougher check.

The Company must consider checking whether the employee:

1. Has a criminal record (e.g., through a police check),
2. Is or has been subject to any regulatory, court or legal action,
3. Has used bankruptcy laws to their own advantage,
4. Has lived in high-risk countries or regions.

8. RELEVANT STAFF TRAINING

In providing the specified categories of employees (i.e., the Relevant Staff) with the applicable training, the Company shall take into consideration the knowledge and qualifications necessary for the duties, responsibilities and authorization of the Relevant Staff. The Company shall, within the framework of the training, explain to the Relevant Staff the AML/CFT requirements and provide detailed information on the measures and activities the Relevant Staff are expected to conduct within the framework of their responsibilities.

The Company shall develop and document a staff training plan which contains at least the following programs:

1. An internal training program for the Relevant Staff, which uses internal training resources ("**internal training**").
2. An external training program for the Relevant Staff, which uses external training resources, including participation of foreign experts (a qualified person in the AML/CFT area) ("**external training**").
3. A training program for new Relevant Staff (Relevant Staff members who have just started to perform their duties or changed position at the Company) ("**new Relevant Staff training**").

The Company shall ensure that the information on the conducted Relevant Staff training is saved by documenting the following data:

1. Name of the training.
2. Personal data of the trained Relevant Staff member.

3. Position and structural unit of the trained Relevant Staff member.
4. Training venue.
5. Head and organizer of the training.
6. Time of training.
7. Duration of the training.
8. Result of knowledge tests and certificate obtained, if any.

The Company shall update the training programs in line with any modifications in internal and external regulations and supply of training programs in the market (for provision of external training).

The Company shall, at least once a year, assess compliance and efficiency of the training programs and make any necessary changes thereto.

The Company shall ensure that, in addition to the internal and external training, any Relevant Staff member may obtain the necessary advice from senior employees involved in the AML/CFT risk management, including the MLCO.

The Company shall conduct an appropriate training program before new Relevant Staff starts to perform their duties.

In addition to the internal training, the Company shall ensure extraordinary staff training in AML/CFT issues at least in the following cases:

1. New AML/CFT laws and regulations have come into force and are applicable to the Relevant Staff.
2. New products and/or services have been introduced, which cause changes in the AML/CFT risk exposure.
3. During the performance of his/her duties a Relevant Staff member violates AML/CFT laws and regulations due to insufficient knowledge.

9. DATA STORAGE

In accordance with the AML/CFT legal framework, the Company is required to maintain accurate, complete, and securely stored records relating to CDD, transaction monitoring, internal investigations, and regulatory reporting. Proper recordkeeping is essential to ensuring traceability of financial transactions, facilitating audits and inspections by competent authorities, and supporting the detection, investigation, and prosecution of ML/TF offences.

This section outlines the Company's obligations and procedures regarding the retention, format, and accessibility of records associated with customer identification, suspicious/ unusual transactions reports, and internal compliance reviews. All data shall be retained for at least the minimum period prescribed by law and shall be made available upon lawful request by the FIU, the CGA, or other relevant authorities.

9.1. Register and Retention of Suspicious or Unusual Transaction Reports

The Company shall maintain a secure and up-to-date register of all suspicious or unusual transactions in accordance with applicable AML/CFT laws and regulations of Curaçao, and in line with its reporting obligations to the FIU. This register shall include, at a minimum:

- The nature and description of the suspicious/ unusual transaction;
- The date of internal detection and reporting;
- Customer identification and account information;
- A summary of the reasons for suspicion and risk indicators identified;
- The outcome of the internal review, including the MLCO's decision on whether the transaction was reported externally;
- The date and method of submission to the FIU, where applicable;
- Any follow-up actions taken or correspondence received from authorities.

In addition to maintaining the register, the Company shall retain copies of the full reports submitted to the FIU together with any internal documentation, notes, or investigative records used to support the reporting decision.

All such records, including both the register entries and the underlying reports, shall be stored securely in electronic or durable format for a minimum of 5 years from the date of the report or the termination of the

customer relationship, whichever is later. These records shall be made available without delay upon request by the FIU, the CGA, or any other competent authority.

9.2. Retention Period and Format of Customer Records

All records referred to in this section shall be retained in electronic or durable form for a minimum of 5 years from the date of the termination of the business relationship with the customer, unless a longer retention period is prescribed by applicable laws and regulations, or a competent authority.

Specifically, the following records must be retained:

- Identity Documentation: Copies of official identification documents, verification data, and KYC information collected during customer onboarding and CDD.
- Account and Contractual Records: Copies (or originals, where applicable) of account opening documentation, customer agreements, and other legal instruments.
- Correspondence: All customer-related correspondence, whether conducted via email, in-platform messaging, or physical communication.
- Transactional Documentation: Records evidencing the execution of monetary operations or transactions, including transaction logs, payment confirmations, and source of funds documentation.
- Investigation Records: All internal records relating to investigations of suspicious/ unusual transactions, including internal escalation notes and the MLCO's determination.

9.3. Extension of Retention Periods

The 5-year statutory retention period may be extended upon written requests from a competent authority, such as the FIU, the CGA, or law enforcement agencies. The Company must retain such data for as long as the request specifies, or until the matter under investigation is officially closed.

9.4. Storage of Employee Data (Relevant Staff)

The Company shall retain the personal data of all individuals classified as Relevant Staff, engaged by the Company in roles subject to AML/CFT obligations, for a minimum period of 5 years following the termination of their engagement or employment.

Where applicable labor, data protection, or AML/CFT legislation in the jurisdiction of the individual requires a longer retention period, the Company shall comply with the longer statutory requirement. Personal data shall be stored securely and made available only to authorized personnel for the purposes of compliance monitoring, internal audit, or regulatory inspection.

10. RELIANCE ON THIRD PARTIES TO PERFORM CUSTOMER DUE DILIGENCE

The Company may, under defined and controlled circumstances, rely on third parties to perform certain elements of CDD in accordance with applicable AML/CFT laws and regulations. This reliance does not extend to outsourcing responsibility, as the ultimate accountability for AML/CFT compliance remains with the Company.

10.1. Permitted Scope of Reliance

The Company may engage third parties to assist in carrying out specific CDD obligations, including:

- Customer identification and verification, including the collection of official identification and proof of address;
- Screening customers against relevant sanctions lists, PEP databases, and adverse media sources;
- Ongoing monitoring of customer activity, subject to Company oversight and decision-making.

These third parties may include, but are not limited to:

- Regulated financial institutions or other entities subject to AML/CFT supervision;
- Specialized KYC/CDD service providers;
- Technology vendors offering identity verification, screening, or risk monitoring tools;
- Customer onboarding platforms or affiliated group entities performing onboarding on the Company's behalf.

Licensing or regulatory status is not in itself determinative, provided the third party can demonstrate that it has adequate AML/CFT controls in place and is capable of fulfilling its obligations to the standards required by Curaçao law and the Company's internal policy.

10.2. Conditions for Acceptable Reliance

The Company may rely on a third party only where the following conditions are met:

- A documented arrangement is in place clearly setting out the responsibilities of the third party and the scope of services provided;
- The third party applies equivalent or comparable AML/CFT standards, even if it is not licensed or supervised;
- The Company has immediate access to all CDD data, documentation, and underlying records obtained by the third party;
- The third party is subject to a risk-based due diligence assessment before and during the course of the arrangement.

Where reliance is established, the Company must ensure that:

- The CRA remains the Company's responsibility;
- The final decision to onboard or reject a customer lies with the Company;
- The submission of suspicious/ unusual reports or other regulatory filings cannot be delegated and must be handled internally.

10.3. Assessment and Oversight of Third Parties

Prior to entering into a reliance arrangement, the Company shall conduct a formal assessment of the third party's suitability, including:

- An evaluation of the third party's AML/CFT policies, procedures, and control environment;
- Review of data security measures and information-sharing protocols;
- Confirmation of the third party's operational capability to comply with the Company's requirements;
- Periodic reviews and monitoring to confirm continued adherence to agreed standards.

The MLCO is responsible for:

- Approving reliance arrangements and conducting risk assessments;
- Ensuring the continued availability of CDD records for regulatory inspection;
- Conducting regular oversight and compliance checks;
- Ensuring that reliance does not compromise the Company's ability to detect and respond to ML/TF risks.

10.4. Limitations and Prohibited Reliance

The Company shall not rely on third parties in the following circumstances:

- Where the third party cannot guarantee access to underlying documents and records without delay;
- Where the third party is located in a jurisdiction with inadequate AML/CFT laws, or where supervision is weak or absent;
- For the final risk classification, approval of high-risk customers, or submission of reports to the FIU, which must always be conducted by the Company directly;
- In any case where red flags or inconsistencies have been identified but not adequately resolved.

10.5. Recordkeeping & Access

All data and documentation collected through reliance arrangements must be:

- Available promptly upon request by the FIU, the CGA, or other competent authorities;
- Retained for no less than 5 years after the termination of the customer relationship, or longer where required by applicable laws and regulations;
- Integrated into the Company's own customer files for review, monitoring, and audit purposes.

11. REVIEW

1. This policy will be reviewed at least once every three years.
2. FATF's High-Risk Jurisdictions subject to a Call for Action (i.e., Sanctioned Countries or "Blacklist") and FATF's Jurisdictions under Increased Monitoring (i.e., High-Risk Countries or "Greylist Countries") are checked at least triennially.
3. EU listed high-risk third countries (i.e., High-Risk countries or "Greylist Countries") are checked at least biannually.
4. Basel AML Index and KnowYourCountry ratings are checked at least annually.

However, the Policy will also be reviewed when there are any changes in the Company's business that affect what should be considered in respect of our AML/CFT policies and procedures, when new AML/CFT laws and regulations is enacted.

12. CONTACT INFORMATION

The contact person for matters relating to this Policy is:

Name, surname: Kristina LOSEVA

Email: legal@planbet.com

Any questions, requests for clarification, or concerns regarding this Policy should be directed to the contact person(s) listed above.

APPENDIX A - SANCTIONED COUNTRIES (“BLACKLIST”) & HIGH-RISK JURISDICTIONS (“GREY LIST”)**1. Sanctioned Countries (“Blacklist”)**

Sanctioned Countries are identified by the FATF in the section titled “High-Risk Jurisdictions subject to a Call for Action” (i.e. “black list”): <https://www.fatf-gafi.org/en/countries/black-and-grey-lists.html>, and is reviewed/ followed up by the Company frequently.

2. High-Risk Jurisdictions (“Greylist”)

The Company has established that all jurisdictions (except the Sanctioned Countries) are divided into 3 levels: low risk, medium risk and high-risk countries.

Risk scores are assigned to the countries according to the below:

Assigned tag	FATF “grey list”	EU “grey list”	Basel AML Index	KnowYourCountry
LOW	n/a	n/a	0-4.99	70.01-100
MEDIUM	n/a	n/a	5-6.99	50-70
HIGH	yes	yes	7-10	0-49.99

Countries’ AML ranking is created by the MLCO and updated at least 3 times a year after FATF publishes a list of jurisdictions that have been identified as having strategic deficiencies in their AML/CFT systems.

Assigning the AML ranking, the Company considers:

1. FATF Jurisdictions under Increased Monitoring (i.e., “Greylist Countries”) (<https://www.fatf-gafi.org/en/countries/black-and-grey-lists.html>);
2. EU policy on high-risk third countries (i.e., “Greylist Countries”) (https://finance.ec.europa.eu/financial-crime/anti-money-laundering-and-counter-terror-finance-international-level_en);
3. Basel AML index (<https://index.baselgovernance.org/ranking/>);
4. KnowYourCountry ratings (<https://www.knowyourcountry.com/ratings-table/>);
5. The Company considers countries subject to sanctions, embargoes, or similar measures issued by international organizations, such as the United Nations Security Council, the European Union, or OFAC.

Customer’s residence country/ nationality/ place of birth/ passport issuing country/ device’s IP address is a High-Risk Country, the Company must perform EDD of such customer:

1. The Company must acquire the approval of Company’s senior management or the MLCO prior onboarding such customer.
2. Take adequate measures to establish the source of wealth and source of funds.
3. Conduct enhanced ongoing monitoring of such business relationships.
4. Where applicable, require that the first payment be carried out through a bank account in the customer’s name held with a bank in the EU / EEA or registered in a low risk or medium risk country.

The Company will, at the establishment of the relationship with a prospective customer, take steps to understand where a customer is based, to assess whether they ought to be considered for EDD based on FATF’s list of regimes with poor AML/CFT practices.

APPENDIX B – PLAYER RISK MATRIX

This matrix outlines the risk categorization methodology used by the Company to classify its customers (players) based on four primary dimensions:

1. Nature of the Customer or Behavior
2. Geographic Location
3. Source of Funds / Wealth
4. Transaction Size and Patterns

The matrix supports the application of proportionate CDD or EDD measures and is consistent with the Company's BRA and CRA procedures.

Risk Level	Nature	Geographic Location	Source of Funds / Wealth	Transaction Size / Activity
Prohibited	- Customers listed on sanctions lists (UN, EU, OFAC, UK, etc.) - Individuals failing or refusing to complete mandatory CDD/EDD requirements - Self-excluded persons or individuals on national exclusion registers - Known or suspected identity fraud - Persons impersonating others or using forged documents - Underage individuals (under 18 or under 21, where required by law) - Use of proxies or third party-controlled accounts	- “<i>Blacklist</i>” countries - IPs indicating high-risk geolocation masking (VPNs from high-risk areas)	- Use of unverified third-party funds - Unexplained or unverifiable wealth - Cash deposits without documentation - Funds traced to illegal or unregulated online platforms - Attempt to transact via cryptocurrency services not licensed in FATF jurisdictions	- Any transaction where the customer fails to provide documentation upon reaching reporting thresholds - Attempts to bypass deposit limits via multiple small transactions (structuring) - Transactions flagged by internal systems and CDD refused or incomplete
High Risk	- PEPs, their family members and close associates - Customers with high-volume gambling behavior not justified by known income - High-net-worth individuals with complex structures - Accounts with repeated suspicious activity alerts - Accounts with historical account closures at other platforms for AML/CFT breaches	- “<i>Greylist</i>” countries - Jurisdictions with weak AML/CFT controls - Offshore financial centers known for tax secrecy or anonymity - IP addresses with inconsistent country/account residency details	- Use of more than 5 different payment instruments - Large funds from recently opened offshore bank accounts - Transactions involving digital assets with poor audit trails - Frequent use of third-party or corporate payment sources without justification	- Deposit or withdrawal ≥ 10 000 EUR in a single or multiple related transactions in a 30-day period - Rapid bet-win-withdraw cycles without sustained gameplay - Multiple high-value deposits in short time without activity - Evidence of structuring or layering techniques
Medium Risk	- Customers identified in adverse media or negative online publications - Customers previously categorized as high-risk and now monitored - Public figures with controversial associations - Professional or semi-professional gamblers without clear source of funds - Unusual transaction behavior within acceptable legal limits	- Countries identified by MLCO as posing elevated ML/TF risks - Countries with high levels of corruption, financial secrecy, or political instability - Jurisdictions listed in internal or third-party risk assessments as medium-high risk	- Use of unverified but low-volume payment methods - Inconsistent employment/income vs. gambling activity - Use of funds from business or crypto-related sources without sufficient supporting documents	- Deposits or withdrawals > 2000 EUR in a 30-day period - Multiple transactions just below the EDD trigger thresholds - Transactions involving currency conversions without gambling activity - Sudden increases in volume or frequency compared to customer baseline
Low Risk	- Verified individuals with consistent and expected gambling patterns - No indicators of ML/TF risk- Fully compliant with KYC requirements - No adverse media, PEP, or sanctions match	- Countries fully compliant with FATF recommendations - EU, EEA, UK, Canada, Australia, New Zealand	- Verified personal bank accounts- Debit/credit cards from regulated financial institutions - Licensed and reputable payment service providers	- Deposits and withdrawals within normal limits (e.g., < 2000 EUR monthly) - No unusual gambling or financial behavior

Anti-Money Laundering and Counter-Terrorism Financing Policy

	- Clear ownership and account control	- Stable democracies with low ML/TF risk ratings	- Source of funds supported by employment or savings consistent with profile	- Consistence between customer profile and transaction activity
--	---------------------------------------	--	--	---