

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	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 Curacao AML legislation.

CONTENTS

1. THE POLICY	4
2. DEFINITION OF MONEY LAUNDERING AND TERRORIST FINANCING	4
3. APPLICABILITY AND REGULATORY FRAMEWORK	5
4. THE COMPANY'S OBLIGATIONS	6
4.1. MAIN ML/TF PREVENTION PRINCIPLES	6
4.2. MLCO OBLIGATIONS	7
4.3. RELEVANT STAFF OBLIGATIONS	8
5. CUSTOMER RISK ASSESSMENT.....	8
5.1. CUSTOMER RISKS	9
5.2. CUSTOMER ACCEPTANCE POLICY	10
5.3. CUSTOMER IDENTIFICATION	10
5.4. SANCTIONED COUNTRIES ("BLACKLIST").....	10
5.5. SANCTIONS & PEP STATUS SCREENING	11
5.6. HIGH-RISK COUNTRIES ("GREYLIST")	11
5.6. CUSTOMER VERIFICATION	12
5.7. CDD	12
5.8. ONGOING CDD	13
5.9. EDD	14
6. REPORTING OF SUSPICIOUS MONETARY OPERATIONS OR TRANSACTIONS	15
7. RELEVANT STAFF DUE DILIGENCE.....	16
8. RELEVANT STAFF TRAINING	17
9. OFFENCES AND SANCTIONS	18
10. DATA STORAGE	18
10. REVIEW	19
APPENDIX A - SANCTIONED COUNTRIES ("BLACKLIST") & HIGH-RISK JURISDICTIONS ("GREY LIST")	20
1. SANCTIONED COUNTRIES ("BLACKLIST")	20
2. HIGH-RISK JURISDICTIONS ("GREYLIST")	20
APPENDIX B - RESTRICTED JURISDICTIONS BY THE LICENSE	22
APPENDIX C – PLAYER RISK MATRIX	23

1. THE POLICY

The 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 to by EDJOWA-GAMING N.V. (“**Company**”), its directors, officers, relevant employees and relevant outsourced 3rd party providers (contractors, sub-contractors, etc.,) (if any) (“**Relevant Staff**”).

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 is fully compliant with applicable AML/CFT laws and regulations of respective countries and jurisdictions.

The Company is committed to an annual review and critical reassessment of this Policy considering the Company’s business strategies, goals and objectives on an ongoing basis.

The Company will always seek to disrupt this activity by cooperating fully with the authorities and reporting all suspicious activity to the Financial Intelligence Unit of Curaçao (“**FIU**”).

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 activity or behaviour 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 Curaçao Gaming Control Board (“**GCB**”) and the FIU.

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

- Online gaming regulations:
- PB 1993, no. 63 | Landsverordening buitengaatsse hazardspelen (National Ordinance on Offshore Games of Hazard)
- PB 2024, no. 157 | Landsverordening op de kansspelen (National Ordinance on Games of Chance)
- General AML/CFT 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
- 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)
- 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 I Wijziging van de Regeling indicatoren ongebruikelijke transacties (Amendment of the Indicators for recognizing unusual transactions)

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](#).

The AML/CTF Policy applies to the Company and shall be communicated with all employees of the Company, as well as the subsidiaries and affiliated companies within the group to which the Company outsources some of its operations, to ensure they are aware of their responsibilities under AML/CFT regulations, and the policies set out by the Company. For each version update, the Policy shall be communicated to the Relevant Staff. The Policy shall also be shared with any relevant 3rd party entering into a contract with the Company who has any access to transactional customer data or information which might otherwise present Money Laundering and/or Terrorism Financing (“ML/TF”) risks.

4. THE COMPANY’S OBLIGATIONS

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. The Policy is periodically (at least once a year) updated by the MLCO based on the general principles set up by the Company’s Director in relation to the prevention of ML/TF.

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, analyze, consult **and, if appropriate, report the activity** 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 the laws and regulations relating to AML/CFT.
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 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 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 reports and information to the FIU, storage of information according to the applicable 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 applicable legislation. 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 legislation:
 - Monitoring all amendments in the applicable legislation aimed at prevention of ML/TF and updating internal instructions according to up-to-date information. The internal instructions must be updated at least once a year.
 - 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 according to the indicators mentioned in the Ministerial Decree regarding the Indicators for Unusual Transactions.
 - Reviewing all internally reported unusual transactions for their completeness and accuracy with other sources.

- Keeping records of internally and externally reported unusual transactions.
- Executing closer investigation of unusual transactions if necessary.
- Preparing the external report of 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 circumstances are immediately reported to MLCO.

A dedicated 'Suspicious Transactions' email box has been created which is available to the Relevant Staff (legal@planbet.com). This mailbox is to be used for all Relevant Staff to report accounts they suspect of ML/TF, especially in the cases if behavioural triggers occur. All such suspicious transactions shall be reported internally to the MLCO.

5. CUSTOMER RISK ASSESSMENT

For the purpose of identification, assessment and analysis of ML/TF risks related to the Company's principal activity, the Company conducts business risk assessment ("BRA"). The steps taken to identify, assess and analyse risks must be proportionate to the nature, size and level of complexity of the economic and professional activities of the Company.

As a result of the BRA, the Company maintains the following risk classification:

1. Low risk. Customers who are classified as Low-Risk are subjected to Standard Due Diligence ("SDD") procedures related to the request for Know-Your-Customer ("KYC") documentation and constant monitoring of activities on the account.
2. Medium risk. If the customer fails to provide the requested documentation at a stage where this is required (i.e. when it has been requested due to defined triggers, like change in risk profile from low to medium/high, turns to become a PEP, starts requesting high volume transactions etc.), the account will be under increased monitoring.
3. High risk. Customer activity is the determining factor for the classification of a customer as High-risk. Any customer for which an automated alert has been generated or an inappropriate activity has been detected will be categorized as High-risk, for which an Enhanced Due Diligence ("EDD") procedure is applied.

Customer screening is one of the methods used for risk assessment of the Company's existing or potential customers:

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 Customer Risk Assessment (“CRA”) to evaluate potential risks associated with customers and transactions,
 - Ensure compliance with sanctions to avoid violating any applicable sanctions 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/CTF 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 obligations effectively.

5.1. CUSTOMER RISKS

The Company does not allow anonymous gambling. Every player is required to register and identify themselves with the Company. A gaming account is only allowed to be operated by the registered individual, and the Company does not allow third-party use of an account. The system is regularly scanned for links between accounts in the registered details.

Sanctioned individuals are not permitted as customers. PEPs may become customers of the Company only after obtaining senior management approval to provide services to them. All customers are checked using various methods and if a match is found, the account shall be blocked with immediate effect, to ensure we do not transact with any sanctioned individuals or the PEP prior the senior management approval. Adverse media checks are also conducted regularly.

Any match detected during these checks, where there is a high likelihood of being a true match, shall be evaluated by the MLCO to consider whether there is reasonable ground to submit a Suspicious Activity / Unusual Transaction report to the FIU.

The Company shall not rely solely on open-source information and shall make regular contact directly with any customer identified as potentially risky to verify the customer information provided and obtain further documentation where required.

5.2. CUSTOMER ACCEPTANCE POLICY

The Company's customer acceptance policy is based on what is required under law and in line with the Company's risk appetite and the BRA. Certain types of individuals shall not be accepted as customers, by either being prevented from registering or blocked from using the Company's website:

1. Under 18 (or 21 in some jurisdictions).
2. Residents of Sanctioned Countries.
3. Individuals on FATF, UN, EU, UK or OFAC sanctions lists.
4. Individuals where the Company has reason to suspect involvement in ML/TF or other types of criminal activity.
5. Self-excluded customers, excluded from the Company's websites or any national self-exclusion register available within the license conditions.
6. Individuals who have submitted documentation or information which the Company has reasonable grounds to suspect is fake or fraudulent.
7. Customers where an increased risk level in the customer profile for any reason warranted the Company terminating the relationship.

5.3. 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.

5.4. SANCTIONED COUNTRIES (“BLACKLIST”)

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

No possibility to register or keep the gaming account by customers from High-Risk Jurisdictions subject to a Call for Action (“**Sanctioned Countries**” or “**Blacklist Countries**”) (source: <https://www.fatf-gafi.org/en/countries/black-and-grey-lists.html>) is provided. Technical measurements are integrated into the Company's systems to prevent such registration.

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.

The Company shall be prohibited to accept transactions the execution of which would conflict with international sanctions implemented in the Curaçao. Such transactions concluded after the establishment of the implementation of international sanctions:

- 1. In the manner prescribed by the applicable AML/CTF legislation shall be null and void, and invalid.*
- 2. The fulfilment of the obligations which appeared prior to the Curaçao establishment of implementation of international sanctions in the Curaçao must be terminated immediately or suspended for the duration of the implementation of international sanctions. It shall be prohibited to assume new obligations the fulfilment of which would conflict with international sanctions implemented in the Curaçao.*
- 3. Upon the restriction of availability of accounts to the entities with respect to which international sanctions are implemented, expenses associated with routine holding of such accounts may be deducted from them, and interest as well as payments due under transactions, concluded prior to the commencement of the implementation of international sanctions, may be added only if any deductions or additions shall not be made available to the entity with respect to which financial sanctions are implemented.*

5.5. 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.).

5.6. 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 Regulations and monitoring by FATF, or countries providing funding and/or support for terrorism.

Greylist Countries list provided in Appendix A.

5.6. 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.

5.7. 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.

5.8. 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.

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.

6. REPORTING OF SUSPICIOUS MONETARY OPERATIONS OR 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 or unusual monetary operations or transactions. Suspicious or unusual monetary operations or transactions, including:

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 on unusual monetary operations or 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 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.

For the avoidance of doubt the "Relevant Staff" is considered not only the employees employed by the Company as per the applicable labour laws and regulations, but also include the 3rd parties (contactors, subcontractors, etc.) contracted by the Company, whose duties include the handling of the relevant financial business and/or the relevant activity.

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/CTF 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/CTF 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/CTF 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/CTF issues at least in the following cases:

1. New internal and external regulations governing the AML/CTF 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/CTF risk exposure.
3. During the performance of his/her duties a Relevant Staff member violates the internal and external regulations governing the AML/CTF due to insufficient knowledge.

9. OFFENCES AND SANCTIONS

If the Company does not comply with the compulsory AML/CFT requirements, it is committing an offense, which is an unlawful and punishable act. The way in which an offence is punished depends on the severity of the offence committed. Offences are subdivided into misdemeanours and felonies. Felony refers to a serious offence committed for which the lawbreaker will be tried, judged and sentenced by a court in Curaçao and Sint Maarten.

The Central Bank will report an offence to be criminally investigated or prosecuted by the law enforcement in circumstances where the offender emphatically refuses to comply with the NORUT and/or NOIS. Before proceeding to imposing a fine, the Central Bank shall inform the (financial) institution or individual in writing of its intention to impose a fine, stating the grounds on which the intention is based, and shall offer him the opportunity to redress the omission within a reasonable term.

10. DATA STORAGE

The Company must keep a register of reports of suspicious and unusual transactions.

The Company must keep a register of the customers with whom transactions or relationships were terminated under the circumstances specified in Section 5.8. “ONGOING CDD” of this Policy or under any other circumstances related to violations of the Policy.

Register data shall be stored in electronic form for 5 years from the date of termination of transactions or relationships with the customer.

Copies of the identity documents of the customer, other data received at the time of establishing the identity of the customer and account and/or agreement documentation (originals and/or copies of the documents) must be stored for 5 years from the date of termination of transactions or relationships with the customer.

The correspondence with the customer must be stored in paper or electronic form for 5 years from the date of termination of transactions or relationships with the customer.

The documents confirming a monetary operation or transaction and data or other legally binding documents and data related to the execution of monetary operations or conclusion of transactions must be stored for 5 years from the date of execution of the monetary operation or conclusion of the transaction.

Records of the results of the investigation specified in this Policy shall be stored for 5 years in paper or electronic form.

Time limits for storage may be additionally extended upon receipt of a reasonable request from a competent institution.

The Company must store the personal data of the Relevant Staff referred to in Section 8 “*Relevant Staff Due Diligence*” of this Policy for five years upon termination of employment, unless longer storage is required by applicable Labour laws and regulations in the country of residence of the employee.

10. REVIEW

1. This policy will be reviewed at least annually.
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/CTF policies and procedures, when new AML/CTF legislation is enacted.

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:

<i>Assigned tag</i>	<i>FATF “grey list”</i>	<i>EU “grey list”</i>	<i>Basel AML Index</i>	<i>KnowYourCountry</i>
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://ec.europa.eu/info/business-economy-euro/banking-and-finance/financial-supervision-and-risk-management/anti-money-laundering-and-counter-terror-financing/eu-policy-high-risk-third-countries_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/CTF practices.

APPENDIX B - RESTRICTED JURISDICTIONS BY THE LICENSE

Below is the list of countries/jurisdictions that are subject to limitations of the applicability of the Company's license:

- USA
- Netherlands
- France
- United Kingdom
- Australia
- Spain
- Dutch West Indies
- Aruba
- Bonaire
- Saba
- Statia
- Dutch St Martin
- Curacao

Excluded Territories

Under this license, apart from its own diligence and legalities, the license holder is not authorized to offer its services in the territories of USA, Netherlands, France, United Kingdom, Australia, Spain, Dutch West Indies, Aruba, Bonaire, Saba, Statia, Dutch St Martin and Curacao. It is the responsibility of the licensee to be familiar with the local laws and requirements for the territories which they intend to offer their services. Before reporting such non-compliance, please make sure the license holder is not operating under multiple licenses, allowing the legal operation in the above regions.

The above list may be updated when the Company receives a new seal under GCB regulations, at which point the necessary amendments to this Policy will be made.

APPENDIX C – PLAYER RISK MATRIX

Risk Rating	Nature	Location	Source of funds and wealth	Transaction size
Prohibited	Sanctioned individual A customer that has triggered any of the below qualifiers to become high or medium risk but does not comply with the Company's CDD/EDD requirements	Closed jurisdictions A customer that has triggered any of the below qualifiers to become high or medium risk but does not comply with the Company's CDD/EDD requirements	Cash A customer that has triggered any of the below qualifiers to become high or medium risk but does not comply with the Company's CDD/EDD requirements. Funds appear to be generated or linked to the ML/TF	A customer that has breached any of the below thresholds but does not comply with the Company's CDD/EDD requirements
High	PEPs Professional Gambler Customers that are sporting professional betting on sports High net worth individuals	Named on list of High-Risk Countries	Use of over 5 different payments methods	Deposit or withdrawal of EUR 10,000 in any period
Medium	Public profile raises some form of concern e.g., adverse media, social media activity	Countries which in the opinion of the MLCO represents heightened risk		Deposit or withdrawal or over EUR 2000 (or currency equivalent) or aggregate in excess of EUR 2000 (or currency equivalent) in a 30-day period
Low	Individual	Fully compliant with FATF No AML/CFT concerns	Bank transfer Debit or credit card Approved payment service provider	Under any of the qualifying payment thresholds