

AML Manual

NVRB B.V.

VERSION HISTORY

Version Number	Version Date	Author	Summary of Changes
V1.0	1/12/2025	Gabriela Xuereb	Initial Draft

APPROVALS

Name	Title	Date of Approval	Version Number

DISTRIBUTION

Name	Title	Date of Issue	Version Number
V1.0	1/12/2025	Gabriela Xuereb	Initial Draft

Contents

Purpose	3
Definitions and Abbreviations	3
What is Anti-Money Laundering and combating the financing of terrorism?	4
Key Policy Points	4
Key Points of AML/CFT Procedures	4
Roles and Responsibilities	5
Registration Process	6
Client Acceptance Policy (CAP)	7
The Risk Assessment	9
Customer Risk Scoring.....	10
Channel Risk Scoring	10
Geographical Risk Scoring	11
Other Risk Scoring	12
High Risk Source of Funds	12
Identification of Risks	13
Design and implementation of measures and procedures to manage and mitigate the risks.....	15
Player Name Screening & Sanctions Screening Procedures.....	16
Politically Exposed Persons – PEPs.....	16
Policy Applicability	17
Reporting Concerns	17
Information on the purposes and intended nature of the business relationship.....	19
Legal and Regulatory Framework	19
Final Provisions	19
KYC Procedure	20
KYC Verification Flow	20
Due Diligence Procedures on Natural Persons	22
CDD Procedure	22
Enhanced Due Diligence	24
Ongoing Monitoring Process.....	25
Retention Policy	26
Funds Management	27
Training and Awareness.....	27

Purpose

The purpose of this AML policy internal working procedure is:

- a. To make available the general legal provisions, the terms used, the necessary forms, the instructions to be followed, the activities and operations required by law with reference to the specific economic activity of the company, namely, the provision of services according to the registered NACE codes, generically called support activities for a third party;
- b. To establish in general terms the working method for applying the provisions of the legislation on anti-money laundering and combating the financing of terrorism with specific particularities taking into account the activities carried out.

Definitions and Abbreviations

- a. **FIU** – Financial Intelligence Unit. Regulatory Body for combating Money Laundering and Funding of Terrorism.
- b. **Compliance Officer** - person appointed in relation to the CGA, whose names are communicated in writing to the MGA together with the nature and limits of the said responsibilities in preventing Money Laundering and Funding of Terrorism.
- c. **AML (anti money laundering)** - refers to the activities that the reporting entity issuing this procedure carries out to meet legal requirements for the purpose of combating money laundering, terrorist financing and international sanctions.
- d. **GDPR** - Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of Personal Data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) and as may be amended from time to time (the “GDPR”)
- e. **CFT** - activities that the reporting entity issuing this procedure carries out to meet legal requirements for the purpose of combating terrorist financing and international sanctions.
- f. **KYC (Know Your Client)** - is an abbreviation for "know your client".
- g. **AML&FT Law** – Prevention of Money Laundering Act Cap.373
- h. **PEP** - Publicly Exposed Person, an individual who holds or has held an important public office: heads of state, heads of government, ministers and deputy ministers or secretaries of state, members of parliament or similar central legislative bodies, members of governing bodies of public parties, members of supreme courts, constitutional courts or other courts , members of governing bodies of courts of auditors or members of governing bodies of boards of central banks, ambassadors, chargés d'affaires and senior officers in the armed forces, members of boards of directors and supervisory boards and persons holding managerial positions in autonomous companies, companies with majority state capital and national companies, directors, deputy directors and members of the board of directors or members of the governing bodies of an international organization. Publicly exposed persons are persons who are or have recently been in important public positions, or who are relatives or friends of persons who also hold such positions.

What is Anti-Money Laundering and combating the financing of terrorism?

- **Money laundering** - is the process of making illegally obtained proceeds appear legal to hide their true origin and avoid detection.
- **Terrorist financing** - is the provision of financial support for terrorist activities. The source of these funds may be legitimate or criminal

Key Policy Points

Our policy is to meet and, where possible, exceed legal and regulatory obligations to prevent money laundering and terrorist financing, and this includes the following:

- a. Ensuring that only registered and verified customers can use Company services
- b. Carrying out our duties in a way that minimizes the risk of the Company being used to launder funds associated with criminal activity or terrorist financing;
- c. Customers' accounts will be closed if their behavior gives reasonable grounds to believe or suspect that they are involved in illegal activities;
- d. Require all NVRB B.V. and service providers to meet all their regulatory obligations;
- e. If our checks indicate that there are suspicions about a potential or existing customer, this will be reported confidentially to the Compliance Officer .
- f. The policy and its associated procedures are based on the legal and regulatory framework detailed below and on best practices.

Key Points of AML/CFT Procedures

The AML/CFT procedures set out the minimum standards to be followed and include:

- a. Establish and maintain a risk-based approach to assessing and managing the money laundering and financial fraud risks faced by the company;
- b. Appoint a Compliance Officer with responsibility for overseeing compliance with relevant anti-money laundering (AML) and combating the financing of terrorism (CFT) legislation, regulations, rules and sectoral guidelines;
- c. All persons doing business with the Company are registered customers and have been properly identified, verified and, where applicable, sufficient information is collected and recorded to allow the company to "Know Your Customer" (KYC) and know their expected and evolving games of chance;
- d. Client activities are regularly reviewed to ensure that they are consistent with what The Company knows about them, particularly in relation to large or unusual transactions.
- e. In 2024, we will establish specific thresholds when it comes to deposited amounts in order to identify accounts that will be reviewed by the AML Team.

- f. The AML Team will also look into large cash transactions made either in person (physical casinos) or via Wallets.
- g. In case of high-risk customers or PEP customers, EDD measures will be applied and additional documentation will be requested such as source of funds and/or source of wealth, fiscal residence, etc.
- h. Furthermore, a more thorough investigation will be conducted by the AML team from a wider variety of sources such as adverse media and the account/s will be kept under close monitor.
- i. empowering employees to confidentially report suspicious activity to the Compliance Officer , for these internal reports to be investigated by the Compliance Officer or, if necessary, a deputy, and for relevant cases to be reported to law enforcement authorities;
- j. Provide online, face-to-face and awareness sessions for all relevant employees on AML and CFT, enforcement activities and best practices;
 - i. Provide information to senior management and directors to enable them to oversee the AML/CFT program, the Due Diligence process and its effectiveness; and
 - ii. Review the effectiveness of the AML/CFT program so that improvements can be made where Necessary.

Roles and Responsibilities

Board and Senior Management	• Providing the necessary "tone at the top" and a culture of ethics and integrity from all staff • Day-to-day compliance with AML/CFT obligations in their areas of responsibility. • Supporting staff in their AML/CFT activities • Promptly notifying the Compliance Officer of any unusual/suspicious activity. • Supporting the Compliance Officer in carrying out its tasks, ensuring that it has full autonomy, independence and the resources to assess incoming suspicious activity reports. • Empowering staff to raise any concerns and confidentially report suspicions to the Compliance Officer.
Compliance Team and Management	• Assist in overseeing the effectiveness of the AML/CFT program on behalf of administrators and senior management. • Assessment of management information on the AML/CFT program
Compliance Officer	• Develop policies, procedures, training and education of staff on AML and CFT. • Representing the company to external agencies and third parties on AML and CFT related questions. • Receipt of internal reports on suspicious activities and assessed, deciding whether or not to report them to the relative regulatory bodies

	• Provide the necessary support to all stakeholders to comply with legal and regulatory obligations in relation to AML/CFT and monitor the effectiveness of the overall program. • Ensuring robust records of AML/CFT activities undertaken are kept for law enforcement agencies in any investigation. Drive and continuously improve the AML/CFT program and its associated policies • and procedures
All staff	• Stay alert to ML/CFT risk • Prompt reporting to the Compliance Officer of any known or suspected ML/CFT. • Comply with all AML/CFT obligations, including assisting the compliance team with client identification, monitoring, record keeping and reporting. • Timely completion of all AML/CFT training

Registration Process

An individual must register personally by submitting an application for registration. Players who do not register themselves will not be allowed to play. As part of the application, the player needs to provide the following information:

- date of birth;
- player's first and last name;
- player's full residential address;
- player's valid email address; and
- a username and a password

In addition, the Company may ask the user to provide further information to ensure the user's true identity. The user will not be able to make use of the Company's services until such information is required. The user is required to provide the Company with their email address or any other means of contact so that the Company may contact the user if necessary.

After registration, the Company will ask further information, such information may include but is not limited to:

- Place of Birth
- Nationality
- Do you have multiple Citizenships? If so, please provide details.
- Current Country of Residence
- Please list any country in which you have a vested interest. Note: this includes any country which you have ties with, or your wealth is generated within such countries, or you own businesses in such countries.
- Your Mobile Phone Number

Client Acceptance Policy (CAP)

The client acceptance policy defines the criteria for accepting new clients (players) and defines the client categorisation criteria which shall be followed by The Company.

The company shall onboard players on two levels:

Level 0: Unregistered Players

Unregistered Players will not be able to place any stakes on the websites owned by The Company.

Level 1: Before €2000 threshold is reached.

At this level, the company shall ask the player to provide at least the information listed in the Registration Process.

The company will then monitor the transactions of the player and his or her behaviour such as changes in the betting behaviour, deposit behaviour, changes in funding methods and games being played. Furthermore, the company shall monitor the total deposits of the player (excluding bonuses and winnings) in a rolling period of 180 days and ensure the total deposit does not meet the €2000 threshold. The total deposit threshold shall be calculated across all platforms the company is offering under its MGA license. The company will only remit withdrawals to the same account from which the player's funds have originated. If this is not possible, the company will verify an alternate method of remitting the player's withdrawals and confirm that the destination is secure and belongs to the player. If the threshold is met, then Level 2 of the onboarding will be initiated as noted below. Cash deposits or withdrawals will not be affected.

Level 2 – After €2000 threshold is reached

Once the €2000 threshold is reached by the player, the company shall initiate the following procedure:

- a. The account of the player is blocked from further deposits or withdrawals as the player is provided 30 days to provide the requested information.
- b. The compliance team shall provide the player with a set of due diligence questions through the "Player Onboarding Questionnaire" which shall include:
 - Additional personal details including the Nationality, place of birth, countries having vested interest in, and whether the player has any additional citizenships.
 - Details about the source of wealth and the income of the player. This includes the source of how the wealth was accumulated, the employment situation of the player, the current occupation, the annual income of the player and whether this is derived from a single or multiple source. Furthermore, an estimate of the overall net worth of the player is asked to be provided through the selection of specific categories. Further information on the wealth is obtained by requesting the types of assets forming such wealth. The player is also asked to provide whether his wealth is derived from certain high risk

- sources such as cash intensive activities, arms trade, defense or mining activities or cryptocurrencies.
- The Player is also asked to provide the expected amounts he or she is expecting to deposit with the company on a monthly basis.
 - The player is asked to confirm whether he/she or the immediate family members is/are considered as a PEP.
 - Furthermore, the player is requested to confirm a set of declarations to ensure he or she is of good repute and to ensure the player confirms the information provided is full, correct, and complete.
 - The player is to confirm that he or she is not representing a third party.
- c. The Client Risk Assessment (CRA) is performed to assess the risk classification of the customer based on the information provided as noted in 'b' above.
- d. If the CRA classifies the customer (player) as 'high risk', then the compliance team shall initiate Enhanced Due Diligence procedures. This will also require supporting wealth documentation from the player.
- e. If the player does not provide the due diligence requested within a 30-day period, the company shall suspend and terminate the player from its platform. The company shall return the funds on account to the customer's bank account, ideally through the same channels such funds were received, if possible, unless there are suspicions or knowledge of ML/FT.
- f. Terminated customers shall not be re-onboarded unless approved by the Compliance Officer .
- g. Further to the above, once the player who reached the €2000 deposit threshold within 180 days provides the onboarding questionnaire, the following procedure is to be followed:
- The Compliance Team shall ensure that the questionnaire is completed;
 - The Compliance team shall ensure that the questionnaire is translated to English and such translation is kept on file;
 - The following documents are to be sent to the Compliance Officer for his feedback:
 - a) The original questionnaire as received from the player
 - b) The translated questionnaire (if applicable or required)
 - c) The risk classification of the player
 - d) Any wealth supporting documentation provided by the player
 - The Compliance Officer shall provide feedback to the team
 - The team shall then communicate with the player and obtain further information as recommended by the Compliance Officer
 - Any updated documentation shall be provided the Compliance Officer once received.
 - If the said documentation is not received by the player, the team shall inform the Compliance Officer accordingly;
 - It is being highlighted that the player's account shall remain blocked until otherwise instructed by the Compliance Officer.

The client acceptance process involves:

- All staff must be aware of the business's policies and procedures especially with regards to Prevention of Money Laundering and funding of terrorism Regulations;
- Before accepting or continuing servicing a client, the compliance team shall obtain the necessary due diligence to enable them to assess the client and engagement within the 2nd level of onboarding as noted above and basic identification information as noted in the 1st level of onboarding;
- The company must also obtain information on the nature of services to be provided – which by nature is known since the service will always be related to the provision of gaming services;
- Where necessary, the compliance team or the Compliance Officer shall enquire on the client's bankers, legal advisors and any other business relationships;
- The documentation gathered will be documented within the customer's file;
- Once the €2000 threshold is reached, the engagement will be terminated if the full due diligence documentation in line with Enhanced Due Diligence procedures, is not received within 30 days;
- The Company shall perform EDD when the client is classified as High Risk through the CRA after the €2000 threshold is met or if there is suspicion of ML/FT at any time;
- The company use the following risk indicators when onboarding a client:
 - (a) Customer risk
 - (b) Product/Service risk
 - (c) Interface risk (Channel Risk)
 - (d) Geographical risk
 - (e) Transaction Risk
 - (f) Complexity of the Structure
 - (g) National and/or supranational risks (if any)

The Company shall classify clients into 3 categories:

- 1. Low-risk clients,**
- 2. Medium-risk clients, or**
- 3. High-risk clients.**

The Risk Assessment

The risk model of The Company provides a detailed risk assessment. The below information provides a detailed explanation of the logic behind the risk model (Customer Risk Assessment).

The final risk score of a player shall be based on the following after taking into consideration the average risk across all risk types.

Total Score	Risk Level
0 – 50	LOW RISK
51 – 69	MEDIUM RISK
70 +	HIGH RISK

Customer Risk Scoring

The Company applies the following combinations when providing scoring for customer risk. This takes into consideration the PEP status, adverse media, sanctions as well as the nationality of having a local resident or otherwise a non-resident. It also takes into consideration the override function for certain types of risks such as sanctions and PEPs as noted below:

Customer Type	Score
Client is PEP	50
Client not PEP	10
Client Sanctioned	50
Client not Sanctioned	10
Client has Adverse Media	50
Client has no Adverse Media	10
Authenticity issues noted	50
No Authenticity Issues noted	10
Single source of income	10
Multiple sources of income	13
Reluctant to provide Due diligence	50
Wealth from High risk sources ¹	50
Wealth not from High Risk Sources	10

Channel Risk Scoring

The company uses the following scores for interface/delivery channel risk:

¹ Please refer to section 6.3.7

Type	Score
Non-Face-to-Face	20
Non-Face-to-Face but using digital ID-V verification systems (AI)	10

No override settings exist in this type of risk assessment

Geographical Risk Scoring

Countries are scored as follows:

Country Classification	Score
Nationality is Low Risk country	10
Nationality Medium Risk country	13
Nationality is High Risk country	20
Nationality is non-reputable country	50
Residency in low risk country	10
Residency in medium risk country	13
Residency in high risk country	20
Residency in non-reputable country	50
Vested interest in low risk country	10
Vested interest in medium risk country	13
Vested interest in high risk country	20
Vested interest in non-reputable country	50

Since the company identifies several different country risk profiling methods within a client, the highest geographical risk score will be used for the calculation of the final risk score, namely:

- Country of Residency of the player;
- Nationality of the player;
- Countries in which the player declared a vested interest.

One should also note that countries which have been listed on the FATF's 'Grey List', that is, countries under increased monitoring [<https://www.fatf-gafi.org>] and/or countries listed under the EU list of countries having weaknesses in their AML Regime [<https://ec.europa.eu/info/business-economy-euro/banking-and-finance/financial-supervision-and-risk-management/anti-money-laundering-and->

counter-terrorist-financing/eu-policy-high-risk-third-countries_en], have an 'override' condition attached to them, and therefore, when these countries are involved, the player will always be considered as 'High Risk' and this would ensure EDD is performed, subject that the €2000 threshold is reached. Furthermore, Iran, Myanmar and North Korea are considered as non-reputable jurisdiction with an international 'call for action' status, also known as 'black list'. **The company shall not onboard / register players being exposed to Iran, Myanmar or North Korea.**

Other Risk Scoring

The Company shall ensure the following risk exposures are captured within the customer risk assessment:

Risk Factor	Score
Attempt to use fake documentation	50
Attempt to open multiple accounts from same location	50
Abnormal betting pattern identified	50
Deposit/withdrawal requests without explanation	50
Attempted payment by third party	50
Multiple payment methods (3 or more);	50
Use of Funds emanating from DLT Assets	50

High Risk Source of Funds

Upon reaching the €2000 deposit threshold, a player is asked to verify his or her source of income. The customer risk pillar takes note on whether the player's income is derived from high risk sources. The below is the list of sources which is considered as 'high risk' by the company:

- Adult entertainment industry
- Oil & Gas industry
- Manufacturing or Printing of Currencies
- Providing a service to the Military
- Manufacturing of Weapons
- Sale or promotion of weapons
- Cryptocurrency or Blockchain
- Cash intensive businesses

Should a player's income be derived from any of the above, this will override the player's risk classification to 'High risk'. In such a scenario, EDD shall be performed within 30 days from when the

€2000 threshold is met or from when the company notes such exposure and updated with risk classification.

The Company shall revise and amend these risk assessments from time to time to ensure that the Company is up to date from all risk assessments.

Identification of Risks

The risk-based approach of the CDD adopted by the Company involves the identification, recording and evaluation of the risks that have to be managed. The CDD includes the client due diligence systems and procedures of The Company and is used during the implementation of the client acceptance policy and on-going monitoring, including an annual review of clients where high risk is noted.

The Company shall assess and evaluate the risks the business faces for the use of their Gaming services for the purpose of money laundering or terrorist financing. The Company shall be, at all times, in a position to demonstrate to the relevant authorities that the extent of measures and control procedures it applies (whether in the CDD or otherwise) are proportionate to the risk it faces for the use of its services for the purpose of money laundering and terrorist financing.

A more detailed and separate document on the risks of the business has been drafted. This report shall be kept up to date with at least an annual update. The document shall be referred to as the 'Business Risk Assessment' and includes the identification of all risks, how these are being mitigated and their likelihood of taking place. The Business Risk Assessment report can be made available to competent authorities upon request.

Business risks

The following, inter alia, are sources of risks which The Company faces with respect to money laundering and terrorism financing, and which must be taken into account in assessing the risk posed by a particular player and/or business relationship. The final risk assessment will be case-specific, taking into account a holistic view of the risks posed by the player and the specific circumstances of the business relationship, as well as the high-risk categories as prescribed at law, which require the application of EDD measures. The following risks are being captured by the risk model. A more detailed information about the risks of The Company business may be found in the 'Business Risk Assessment' report.

Customer risk - risks based on the client's nature:

Below is a non-exhaustive list of customers whose activities may pose a higher risk:

- Whether the player is a Politically Exposed Person (PEP);

- Whether the player is a Sanctioned individual;
- Whether the player is mentioned in adverse media;
- Whether this is a doubt about the authenticity of the documents provided;
- Whether the source of wealth is related to high risk sources;
- Whether the player benefitted or is a prospective applicant of citizenship or residency by investment schemes;
- Whether the player was reluctant to provide due diligence documentation;
- Whether the player has a multiple source of income.

Channel Risk - the channels through which a business relationship is established and through which transactions are carried out:

Non face-to-face clients;

- Non-Face-to-Face but using digital systems to identify and verify players
- Due to the nature of the business, face-to-face relationships are not expected. In fact, the company expects all customers to be considered as non-face-to-face.

Funding Method Risk

The company accepts payments via PSPs, bank transfers, bank cards and E-Wallets.

Cash payments are not acceptable.

Payments by cheques are not acceptable.

Payment by anonymous sources are not acceptable.

The payment shall be from a source in the name of the player. Transfers between players are also not allowed by the company.

Product risk - some gaming products are inherently more risky than others and are therefore more attractive to criminals. The company shall offer four main types of products, namely, casino games, sports betting, lotteries and live casino games. Both products are considered as remote gaming and are expected to have an inherently low ML/FT risk.

Jurisdiction risk - the risk posed by the geographical location of the business/economic activity and the source of wealth/funds of the business:

- Players from high-risk countries or countries known for high-level of corruption or organised crime or drug trafficking;
- Countries subject to sanctions, embargoes or similar measures issued by international organisations;
- Countries identified by credible sources as lacking appropriate AML/CFT laws, regulations and other measure;
- Countries identified by credible sources as providing funding or support for terrorism;
- Activities that have designated terrorist organisations operating within them; and
- Countries identified by credible sources as having significant levels of corruption, or other criminal activity.

Specifically, in relation to geographical risk, The Company carries out country risk assessments with respect to jurisdictions from which the player lives or jurisdictions which are somehow linked to the wealth generation of the player. A reputable jurisdiction is any country having legislative measures for the prevention of ML/FT, taking into account that country's membership of, or any declaration or accreditation by, any international organisation recognised as laying down internationally accepted standards for the prevention of money laundering and for combating the funding of terrorism, and which supervises natural and legal persons subject to such legislative measures for compliance therewith.

For the purpose of determining whether a jurisdiction is reputable or otherwise, the Compliance Officer shall consider reports and other publications issued by the FATF, the European Commission, IMF, World Bank and Transparency International, amongst others. The Compliance Officer will review the jurisdictional assessment from time to time in line with developments.

The Company also takes into account national and supranational risks by taking into consideration several reports on jurisdictions which are available to the public when assessing such a risk.

(a) Other Risks

Players may expose the company to other types of ML/FT risks which are considered as 'high'. In fact, these risks mentioned below are loaded with a scoring which would override the player to an overall risk classification to 'High', hence triggering EDD. These are the following scenarios:

- Attempt to use fake documentation;
- Attempt to open multiple accounts from the same location;
- Abnormal betting patterns identified;
- Abnormal Deposits or withdrawals patterns;
- Attempted deposit/payment by a third party on behalf of a player.

Design and implementation of measures and procedures to manage and mitigate the risks

Taking into consideration the assessed risks, the Gaming Company shall determine the type and extent of measures it will adopt to manage and mitigate the identified risks in a cost-effective manner. These measures and procedures include:

Adoption of the client due diligence procedures in respect of players in line with their assessed money laundering and terrorist financing risk, following meeting of the €2000 deposit threshold within a 180-day rolling period;

Requirement for the quality and extent of identification of data for each type of client to be of a certain standard (e.g. documents from independent and reliable sources, third person information, and documentary evidence, where possible. One should note that player identity verification procedures will take place within a 30-day period from the moment the €2000 threshold is met;

Obtaining additional data and information from the player, where this is appropriate and applicable for the proper and complete understanding of their activities and source of wealth, and for the

effective management of any increased risk emanating from the particular business relationship or the occasional transaction. This is performed for high risk players following the €2000 threshold is met or before if there is a suspicion of ML/FT;

Ongoing monitoring of player transactions and activities from the initialisation of the business relationship to ensure that:

- The player is not using multiple accounts from the same IP Address in order to avoid the CDD threshold;
- The player is not using fake identification details;
- The player is not indicating abnormal betting patterns;
- The player is not indicating abnormal deposit or withdrawal patterns or activities;
- The player is not playing from an IP/Geo Location which differs from the declared country of residency; and
- The player is not showing any abnormalities or suspicious behaviour during his or her usage of our services.

Should there be a suspicion or knowledge of ML/FT, then please refer to section 10.1 for the internal reporting procedures of the company.

Whether or not to accept a player will depend on the risk factors outlined in the Business Risks above and on other factors such as whether the €2000 threshold is met and name screening results. Once these risk elements are considered thoroughly, a decision has to be taken whether to accept the client or not in accordance with the client acceptance policy.

If a player is considered to present a high risk of ML/FT, the player could be accepted under higher monitoring or refused. Players who are considered to pose a 'high-risk' must be subject to enhanced due diligence procedures if such players have exceeded the €2000 threshold.

Player Name Screening & Sanctions Screening Procedures

The Company shall screen the player for PEP, Sanctions, adverse media and for financial crime at the following situations:

- a) Upon initial registration (before the €2000 deposit threshold is reached);
- b) Within 30 days after the €2000 deposit threshold is reached;
- c) At any time if there is a suspicion of ML/FT;
- d) On an ongoing basis in line with the risk-based policy as noted in section 9 subject that the €2000 deposit threshold has been reached;
- e) On a regular basis in relation to 'Sanctions Screening/Monitoring' to ensure that all players are not sanctioned.

Politically Exposed Persons – PEPs

The Company shall ask the player whether he, she, or their immediate family members are classified as a PEP.

The term 'politically exposed persons' is broad and generally includes all persons who fulfil a prominent public function. Regulation 11(7) states that a natural person who is, or has been, entrusted with a prominent public function shall include:

- (a) Heads of State, Heads of Government, Ministers and Deputy and Assistant Ministers and Parliamentary Secretaries;
- (b) Members of Parliament;
- (c) Members of the Courts or of other high-level judicial bodies whose decisions are not subject to further appeal, except in exceptional circumstances;
- (d) Members of courts, Audit Committees or of the boards of central banks;
- (e) Ambassadors, charge d'affaires and other high-ranking officers in the armed forces
- (f) Members of the administration, management, or boards of state-owned corporations; and where applicable, for the purposes of (a) to (e), shall include positions held at the community or international level.

The Company adopts the following additional measures in relation to PEPs:

Upon registration, the company shall screen the player for a PEP. It is being noted, that whilst the company opted to screen at the initial level of registration, the implementing procedures part-2 (remote gaming) defines such obligation to be initiated within 30 days from when the €2000 deposit threshold is reached. At each level (Level 1 and Level 2 as described in the Client Acceptance Policy (CAP), the following procedure shall be followed by all staff:

- The Compliance Officer shall be notified and approves to deal with such a PEP before the player is allowed to continue utilising the company's services;(for both level 1 and level 2) and
- Take adequate measures to establish the source of wealth and the source of funds together with supporting documentation; (only at level 2) and
- Conduct enhanced ongoing monitoring (only at level 2).

Policy Applicability

- a. The policy applies to all directors and employees at all levels of the company as well as its agents, contractors, consultants and agency workers.
- b. Failure to comply with the policy and its associated procedures may result in fines, imprisonment and will also be considered an act of gross misconduct and may result in summary dismissal from the company.

Reporting Concerns

- a. Please notify the Compliance Officer if you know or even suspect that someone is involved in AML/CFT or any form of criminal activity. Even if you are unsure, you should report this as it is a criminal offence not to inform the Compliance Officer of known or suspected AML/CFT. Please see below a list of scenarios of suspicious activities that will need to be submitted for further review:
- Deposits over 5k in the last 24 hours
 - The client has deposited over 5k euro and mail doesn't match the name of the client
 - The client has deposited with 3 different payments methods (credit cards) in 1 hour
 - Clients that change the email address 2 or more times in the last 24 hours
- b. The Internal Suspicious Activity Report can be easily accessed in the Compliance, AML section of You Manage (internal employee system). Employees of the company shall submit an internal STR to the Compliance Officer of the company immediately after detecting a suspicious transaction. The STR shall be sent directly to the Compliance Officer via email and shall be considered highly confidential. The employee who submitted the STR shall not disclose such information with persons outside the company. **The STR shall be sent to the Compliance Officer on the same day it was raised.** STR or any other concerns regarding AML/CFT procedures need to be sent via email to Armine Gasparyan In case of absence, the Compliance Officer will action the duties of the Compliance Officer. The mentioned email address can be accessed only by the Compliance Officer.
- c. The Compliance Officer is expected to file an STR when and if she has a suspicion of ML/FT after receiving and reviewing an internal STR.
- d. The Compliance Officer shall consider reports made by employees for the purpose of determining whether or not the information or other matter contained in the report does give rise to a knowledge or suspicion of money laundering or the funding of terrorism.
- e. If, for any reason, a report cannot be accessed, you can report your suspicion by contacting the Compliance Officer directly by phone or email.
- f. Under no circumstances should you discuss your suspicion with anyone other than the Compliance Officer
- g. The Company shall not carry out a transaction that is suspected or known to be related to ML/FT until the Compliance Officer has informed the FIU
- h. In the unlikely event that the company is not in a position to refrain from carrying out a transaction which is known or suspected to be related to ML/FT in view of the fact that such action is impossible because of the nature of the transaction or such action is likely to frustrate efforts of investigating or pursuing the beneficiaries of the suspected ML/FT operations, the company shall carry out the transaction and the Compliance Officer inform the FIU immediately.
- i. All measures should be taken not to tip-off customers regarding:
- i. the submission of STRs to the FIU,
 - ii. any information demanded by or transmitted to the FIU within the context of ML/TF analysis and
 - iii. any ML/TF investigations on a customer.
- j. If you have any questions, concerns or ambiguities about the AML/CFT, requests for additional relevant training, or are unsure of how the policy or procedures should be applied in a particular situation, please contact the Compliance Officer.

Information on the purposes and intended nature of the business relationship

Once the applicant for business (the player) has been identified and verified, The Company shall also obtain information on the intended nature of the business relationship in order to be able establish the business and risk profile of the applicant for business. Due to the nature of its business, one can easily note that the intended nature of the business relationship shall always be to utilise the betting services provided by the company.

Such procedure shall be triggered upon the player reaching the €2000 deposit threshold as described in more detail in CDD Procedure. Upon reaching such threshold, the company shall obtain the following information from the player within a 30-day period from when such threshold was reached. If the player's account is due to become inactive, the licensee will inform the player 30 days before the account is considered to be inactive.

Legal and Regulatory Framework

The Company policy and procedures are regularly reviewed to incorporate any relevant laws and best practices. The key requirements, obligations and sanctions underpinning our policy and procedures are contained in:

- i. Prevention of Money Laundering Act Cap.373
- ii. FIU Implementing Procedures Part I and Part II – Remote Gaming Sector
- iii. Prevention of Money Laundering and Funding of Terrorism Regulations (S.L.373.01)

Final Provisions

- a. All communications between The Company and competent authorities such as the MGA, FIU, law enforcement, etc. are mediated by our appointed legal representative. In case of direct requests of information on behalf of the authorities mentioned above, they will be escalated to our appointed Compliance Officer.
- b. Personal data and information of all customers will be stored and protected as per General Data Protection Regulation (Regulation (EU) 2016/679, GDPR).
- c. the company keeps customer data for a minimum of five years upon the end of a business partnership or illegal transaction.
- d. The dissemination of this procedure will be done electronically (email) to all departments of the company directly involved.
- e. Acknowledgement of the contents of the procedure will be made by signature (Annex 1);
- f. By processing it, The Company means reading it and discussing it with the line manager.
- g. In case of any discrepancies with the real situation, an e-mail with the necessary explanations will be sent to the risk department;
- h. For new employees in other departments to which this procedure is addressed, this procedure will be presented and processed by the director of the department/direct manager to which

he/she belongs, after which he/she will sign for its insertion using the table presented in Annex 1.

- i. This revised procedure is effective from the date of its revision, any amendments, additions, revisions to it will be communicated by the risk department

KYC Procedure

All documents are reviewed once uploaded by users in the Verification section of their account. The ONLY case where we can check IDs on Chat (includes Facebook conversations) or Email is when the account is locked because ID verification was not completed within 30 days from the first deposit date (Audit section- AV failed - age verification failed - Account is closed with status Other and is listed as AV failed in Audit)- customer cannot upload document on his account as it is locked - verification can only be done on chat or email.

KYC Verification Flow

1. The customer is identified in the database using the email address or username/user id.
2. Check that the document sent by the customer meets the following criteria:
 - It is a valid document, accepted by The Company:
 - ❖ Identity card (new format only, we do not accept voter cards or temporary documents);
 - ❖ Passport;
 - ❖ Driving license;
 - ❖ Temporary residence permit (front and back);
 - ❖ Provisional identity card is not accepted.
 - The document is valid (check expiry date)
 - The name on the document corresponds to the name on the The Company customer account.
 - The document is framed entirely in the photo (all four corners must be visible, in the case of a passport both pages must be included, and in the case of a residence permit there must be double-sided photos of the document);
 - The camera's flash light should not cover the essential details of the document (name, surname, CNP, address, expiry date, ID number, the two alphanumeric series at the bottom of the document.
 - No xerox copies are accepted
 - No blurred or digitally edited photos are accepted.
 - We ONLY accept the following formats :pdf, jpeg, png, img.
 - We do not accept IDs of underage persons. The account will be closed with Underaged status and the user will be informed by email
3. Customer account details to be checks as follows:
 - i. CNP check - we make sure it matches with the information provided by the customer at registration.

- ii. Name and surname - if the name is incomplete, it is necessary to fill in the details manually. The name must not contain diacritics or special characters (-, ` , etc). Make sure that the surname is under Surname and the first name (all) under First name.
- iii. Date of birth – We check that the date of birth corresponds to the date of birth in the ID Card and correct it if necessary- we DO NOT accept underage customers
- 4. The documents are automatically saved in the CMS – Document Verifications section after being uploaded by the customers (see the below picture) in order to be verified by RISK agents
- 5. List of roles used on customer's account:

Roles	Functionality	Details
New Basic Verified Identity	Role added when player's ID is successfully verified	This role gets replaced with New Complete Verified when player also sends POA
New Complete Verified Identity	Role added when player's ID + POA are successfully verified. KYC Role, can deposit is after 900RON/200EUR limit, also can request withdrawals	
IDH Approved	Role added when player's IDH is successfully	Selfie with identity card in hand
Full Docs Verified	Role added when all of the player's documents are verified (ID + POA + Payment methods + IDH)	
Withdraw Block	Role added to a player that has suspicious activity or has over 2K EUR lifetime Deposits or lifetime Withdrawals. Customer has to send additional documents to fully verify the account (missing payment methods, POA etc.)	This role is removed once requested additional documents are successfully verified
POA Requested	Proof of Address Requested	This role gets removed after he sends POA and its approved
Paysafe proof requested	Paysafe proof requested	This role gets replaced by Paysafe proof Approved
Paysafe proof approved	Paysafe proof approved	
1/2/3/4/5 CC approved	This role is added according to the nr of cards used for deposits	It shows how many active credit cards with deposits are verified and approved in the account
Skrill/Neteller proof Approved	Skrill/Neteller proof Approved	
IDH requested	Selfie with ID in hand requested. We request this type of document for 3rd parties payment methods mostly	Replaced by IDH Approved when the request document is approved

Due Diligence Procedures on Natural Persons

The Company shall obtain the following information to ascertain the true identity of the natural persons:

- (a) Official full name;
- (b) Date of birth;
- (c) Permanent residential address;

Before the €2000 deposit threshold is reached, and within 30 days after the €2000 deposit threshold is reached:

- (a) Identity reference number were available;
- (b) Place of birth; and
- (c) Nationality

Following the reaching of the €2000 deposit threshold, the identity of the player shall be verified. The company may decide to verify the identity through technological means before the €2000 threshold at its discretion.

CDD Procedure

Full access to our online gambling platform and its' features requires the completion of an onboarding process which is mandatory for all customers. This will enable us to obtain and verify the identity of each new customer and minimize the level of risk.

Essential information such as full name, date of birth, address, and a valid government-issued identification document (e.g., ID card, passport) will be mandatory to fill in and provide in order to have full access to all the features of our product. Additional information/documentation may be required in order to complete customer onboarding process. This includes documentation which would confirm customer's current address such as a bank statement/utility bill or documentation that would justify customer's overall depositing/wagering behaviour such as Source of Funds (SOF).

Depending on the player's account situation, for various reasons, additional checks are made, and certain documents are requested from the customer, in order to remove suspicions of fraud and also to comply with the law as well as with the casino's Terms and Conditions.

1. We list a few possible cases in which additional documents are requested from the customers:
 - a) The player has lifetime deposits of at least EUR 2,000.
 - b) The total amount of successful withdrawal transactions or pending withdrawal transactions totals at least EUR 2,000- this applies only for customers verified only with the ID.
 - c) There are attempts or successful transactions with payment methods registered in a name other than that of the account holder (3rd party)
 - d) There is a minimum of one clear duplicate account.
 - e) There are relevant links or details in common with other accounts registered on the site

- f) There is suspicion that someone else is using the player account and not the account holder
 - g) The account holder is over 60 years old
 - h) The account holder registers an e-mail address that contains totally different details from his name, e.g. Vasile Ion registers on the site with the e-mail address oana.popescu@gmail.com
 - i) Customer tries to avoid close loop withdrawal (makes deposits with one payment method and withdrawals are requested to another payment method repeatedly, e.g. deposits are made with the Paysafe Card method, but withdrawal transactions are only requested to the Card method).
 - j) There are suspicions that the customer exploits/abuses certain technical bugs in the system to his advantage
 - k) The payment methods registered or the player's e-mail address are on the payment processor's negative list
 - l) Payment methods used for deposits are registered with insufficient details (incomplete information on name on card sections), possible 3rd party
 - m) The player withdraws to a newly registered payment method in the account that has not been verified, even if previous payment methods have been verified in the past.
 - n) The customer also submits documents (e.g. ID) that are not registered in his/her name during the basic account verification (KYC) or later when additional documents are requested (CDD), which indicate that someone else is using the account or that he/she has more than one account on the site.
 - o) The player gives us information through various communication channels (live chat, e-mail, phone, etc.) that the payment method on the account does not belong to him or that he uses multiple accounts.
2. Types of additional documents required for security reasons:
- a) Proof of address which can be a bank statement, utility bill or a letter (document received by postal service or courier service) from any state institution (town hall, police, etc.), not older than 6 months
 - b) A selfie photo in which the ID is held up to the face, with the arm and face visible in the photo, including all details on the ID visible
 - c) Front and back photographs of the cards registered in the player's account, with the first 6 and last 4 digits of the card, the name of the cardholder and the expiry date visible)
Proof that a payment method belongs to the account holder, e.g. card used for transactions, proof can be requested from the bank issuing the card in question
 - d) A bank statement for a certain period
 - e) Proof that the account holder has changed his/her name, this can be a marriage certificate or divorce decree, or an identity card with the new name
 - f) A summary of transactions on the Paysafe Card account plus a screenshot of the Paysafe account details

Enhanced Due Diligence

The Company shall apply EDD in situations which, by their nature, present a higher risk of ML/FT after the €2000 deposit threshold is reached. Such measures ensure that higher risks are better monitored and managed to avoid involvement in ML/FT.

The Company applies EDD when the risk classification of the player is 'High Risk' after taking into consideration all the risks involved. Furthermore, the company has designed its customer risk assessment to take into consideration situations where the player will always be classified as 'high risk' due to:

- (a) Being a Politically Exposed Person; or
- (b) Being a sanctioned entity or individual; or
- (c) Individual residing or is a citizen of a set of countries considered by The Company to represent a higher risk than 'high risk' countries or jurisdictions; or
- (d) The player has its wealth being derived from high risk sources;

In such 'High Risk' cases, the company may apply one, or more, of the following measures as a means of EDD:

- 1) Establish the identity of the applicant for business by using additional documentation and information

In such cases a bank reference and professional reference may be obtained. Where such documents do not provide proof of residential address, an additional utility bill or bank statement containing residential address may also be produced.

- 2) Verify or certify the documentation supplied using supplementary measures.

This involves certification for the purposes of verification of identity by a legal professional; notary; accountancy professional; a person undertaking relevant financial business; or a person carrying out an activity equivalent to relevant activity carried out in another jurisdiction. In other high-risk circumstances, the Compliance Officer will decide on the most appropriate EDD measures.

- 3) Ensure that the first payment of transaction into the account is carried through an account held by the player in his or her name with a credit institution authorised under the Banking Act or otherwise authorised in another member state of the community or in a reputable jurisdiction.

The Company shall always obtain supporting documentation on the source of wealth / source of funds when the player has reached the €2000 deposit threshold and the risk classification of such player is 'high risk'. The company shall also ensure that the source of wealth description provided by the player is detailed.

The Company will also ask the player to provide the following information, which should include evidence supporting it.

- Nature of and details concerning the customer's business/occupation/employment
- Any other activity from which the customer derives his/her wealth
- The expected source and origin of funds to be used throughout the business relationship

- The expected value and frequency of transactions. That is to be undertaken throughout the relationship

Ongoing Monitoring Process

Due to the nature of the business, The Company is expected to have business relationships which would trigger the on-going monitoring obligations.

The below ongoing monitoring obligations are triggers upon reaching the €2000 deposit threshold:

- High Risk: At least once Yearly
- Medium Risk: Once every 2 years
- Low risk: Once every 3 years

Ongoing due diligence may be conducted more frequently than the timeframes mentioned above if it merits on a case-by-case basis or/and if it is requested by the Compliance Officer. Furthermore, such ongoing monitoring on a player would cease should the player be terminated or if the player's account is turned into an 'inactive' status.

It is the company's policy to perform an enhanced review of the player when suspicious transactions or activity are detected. The review shall be performed with immediate effect following flagging of suspicious activity, irrespective of the planned review date of such player.

Following the initial risk assessment of the player after reaching the threshold, ongoing monitoring will enable to identify unusual transactions which may involve money laundering or funding of terrorism. It is noted that certain transaction monitoring is performed since registration and are not linked to the said threshold.

Once a customer has successfully completed the onboarding process, they will be categorized based on the overall risk level that they represent for our business. We will have low, medium and high-risk customers.

A customer's risk level can vary over time depending on documentation provided or changes in overall behavior. A customer's risk level can increase or decrease, certain account restrictions could be applied or eliminated based on the latest findings.

We will closely and continuously monitor each customer's overall activity, with particular interest towards the higher risk customers. This phase is crucial to identify potential unusual or suspicious activity.

The amount of information gathered on a specific customer is essential as it will aid us in establishing a specific baseline when it comes to their overall behavior. In case there's a clear deviation from this baseline, the account will be investigated thoroughly in order to establish the reason behind this change in behavior.

Ongoing monitoring includes:

- a. Scrutiny of transactions undertaken throughout the course of the relationship to ensure that the transactions are consistent with the company's knowledge of the player and his or her risk

profile including, where necessary, the source of funds and source of wealth. Information on the source of wealth and source of funds should be determined initially (within 30 days of reaching the €2000 threshold) and on an ongoing basis after applying a risk-based approach; and

- b. Verifying that the documents, data or information which the company holds are kept up to date; and
- c. The Company must ensure that the risk status of the player did not change; and
- d. Other ongoing monitoring procedures

Special attention will be taken on any large, unusual complex transactions or unusual patterns of transactions. Activities which are not in line with the risk profile of the player must be brought to attention of the Compliance Officer immediately to ensure that proper action is taken.

Retention Policy

It is the policy of the company to maintain records of identification (where applicable) and any other documents related to the player in electronic form with the internal database system for the entire period that it is providing a service to the player and for 5 years after such service has been completed or relationship terminated. Record-keeping is also important for the competent authorities who are responsible for the analysis, investigation, and analysis of the possibility of ML/FT. Such records may also be requested by the FIU.

The Company shall retain a written record of all internal and external STRs. This should include any determination by the Compliance Officer when deciding to not make a disclosure to the FIU.

When the company ceases to provide the service to the player, all information related to the player needs to be archived. This information should be destroyed after 5 years from such termination of service with the player in line with the retention policy of The Company which is part of the privacy notice provided to players as per GDPR obligations.

Each transaction record should include the date, time, amount, and customer identification details. Records must be kept for a minimum of 5 years from the date of the transaction or the end of the customer relationship, whichever occurs at a later stage.

The following records need to be maintained:

1. All transactions, deposits, withdrawals, bets and registration details of all players, irrespective of whether the €2000 threshold was reached;
2. Electronic versions of the due diligence documents including evidence of identity and business relationship in respect of all players who reached the €2000 deposit threshold;
3. Records of details relating to the business relationship and all transactions carried out in the course of the business relationship;
4. Records of the findings of the examination of the background and purpose of the relationship and transactions carried out;
5. Evidence of ongoing monitoring of players (where applicable);
6. Evidence of the management of and monitoring of compliance with internal controls;

7. Player and Employee Screening Records
8. Employee Training records, this includes all types of training taken place

Funds Management

The Company shall only accept payments made from accounts held within a licensed financial institution or through a licensed payment provider which have been notified to the Authority. All funds deposited by the players or owned by the Company shall be credited to the player's corresponding account.

The Company will be making use of Lidion bank as the Company's financial institution, which will maintain all player accounts and funds. Moreover, the Company will also be making use of Nuvei, a Payment Service Provider which will manage and process all payments.

The Backend System shall be generating two dated reports on the last day of each month, one regarding jackpot funds and the other regarding players' accounts.

The player Accounts report shall be capable of presenting the cashable balances in the players' accounts, open bets, chips in play and any participation fees which are part of an open prize pool. Such information shall be presented according to currency and all separately identifiable within the report. The report shall also include any unprocessed withdrawals which have been deducted from the player's cashable balance, however, have not yet been remitted by the Company to the player's deposit method (Such as a wallet/bank/card etc.). The Backoffice shall be capable of identifying and distinguish between player funds information falling under the Maltese license as well as any other foreign license the Company may obtain in the future. Such report shall exclude test account balances and transactions.

Training and Awareness

Awareness of money laundering threats and mitigating measures is essential for the Company to safeguard the business from being exploited by financial criminals.

Financial crime vulnerabilities may arise in any aspects of the business – be it customer onboarding, while executing transactions or at the time of settling the payments. Support from every single employee of the company is crucial to building a robust shield against these threats. AML training is the foundation to any organization's overall AML/CFT framework.

Thus, it is essential to provide regular training to all employees on AML risk factors, the risk assessment process, and how to identify and report suspicious activities.

Training should be tailored to the roles and responsibilities of employees, ensuring that they understand the specific risks related to their functions. The training sessions should be mandatory for all members of staff, especially the ones in customer relationship management roles.

The AML Team is responsible for developing the training programme, keep the modules up to-date, oversee AML/CFT training of the entire staff and maintain the training register.

Training must be imparted at reasonable intervals, at least annually, to refresh some of the most important concepts around AML/CFT. This is also necessary to ensure that employees are trained in recent updates in AML /CFT regulations or the development of new money laundering techniques. Any new employee that joins a customer relationship management role, adequate AML training must be imparted as soon as possible.