



SG-CUR-BP-003

AML and CTF Policy

Internal Document

Version 1.4

March 2025

Copyright YAO Entertainment 2025

1. DOCUMENT CONTROL

Version Control

Date	Version	Version History	Author
2021-08-30	1.1	Initial Draft	JG
2023-08-15	1.2	Monitoring Changes	JG
2024-02-17	1.3	Change to YAO	JG
2025-03-15	1.4	Updates relating to	

Reviewed By

Designation	Name	Signature	Date
CTO	Endrit Haxhaj		19-03-2025

Approved By

Designation	Name	Signature	Date
CEO	James Gibbons		19-03-2025

2. INTRODUCTION

YOUAREON, Anti Money Laundering (AML) and Counter Terrorism Financing (CTF) policy details all of the measures that YOUAREON has taken in order to mitigate the risk of the business being used for criminal purposes (Policy).

This document should be read in conjunction with YOUAREON's AML Risk Assessment

YOUAREON's Anti-Money Laundering & Counter Terrorism (AML/CTF) Policy in accordance with its obligations of:

- Prevention of Money Laundering Act (PMLA)
- Prevention of Money Laundering and Funding of Terrorism Regulations (PMLFTR)
- The Financial Intelligence Analysis Unit (FIAU) Implementing Procedures
- MGA Gaming Act and subsidiary legislation
- EU Anti-Money Laundering Directives

YOUAREON is a remote betting and casino and operator within the online gaming industry and has a legal responsibility to ensure that its gambling facilities are not used for money laundering or to support terrorist financing.

Money laundering and terrorist financing have been identified as major threats to YOUAREON and, indeed, the international gambling community. Malta, similar to

many other countries, has passed legislation designed to prevent money laundering and combat terrorist financing. The legislation, together with the regulations, rules and industry guidance, forms the cornerstone of AML/CFT obligations for Maltese organisations and outline the offences and penalties for failing to comply.

YOUAREON is committed to the highest standards of AML and CFT compliance and requires its management and employees to adhere to these standards in order to prevent use of its services for money laundering or terrorist financing purposes.

Adherence to this AML/CFT Policy is the responsibility of all YOUAREON employees. The AML/CFT Policy and its requirements are formulated and directed by the Money Laundering Reporting Officer (the "MLRO") for YOUAREON. The AML/CFT requirements include client risk assessment, customer due diligence ("CDD")/know your client ("KYC") process (including the requirement to identify and verify the identity of customers), ongoing monitoring, client screening, transaction monitoring, record keeping requirements, the reporting of suspicious activity and training.

3. DEFINITIONS

Definition of Money Laundering

Money laundering is the introduction of money and assets derived from illegal and criminal activities into the legal financial and business cycle and, ultimately, transforming such proceeds of crime into ostensibly legitimate money or other assets.

Typically, money laundering involves three stages; placement, layering and integration. First, the illegitimate funds are furtively introduced into the legitimate financial system. Then, the money is moved around to create confusion, sometimes by wiring or transferring through numerous accounts. Finally, it is integrated into the financial system through additional transactions until the “dirty money” appears “clean”.

The above mentioned stages are not static and can overlap.

Definition of Terrorist Financing

Terrorist financing is the provision of funds or other assets to support a terrorist ideology, a terrorist infrastructure or individual operations. It applies to domestic and international terrorism. While different from money laundering, terrorists often exploit similar weaknesses in the financial system. Terrorist cells exercise several methods to raise and “clean” their money, ranging from illegal activities like organised fraud or narcotics, to legitimate funding sources, including gambling, charitable organizations or legitimate businesses.

4. POLICY

A. Risk Appetite

YOUAREON has no appetite for regulatory or legal censure, fines or prosecution relating to fraud or failing to comply with relevant AML laws and regulation.

YOUAREON has adopted a risk-based approach to AML and CFT, with the aim of managing and mitigating these risks in a proportionate way.

YOUAREON's risk-based approach involves a number of discrete steps in assessing the most proportionate way to manage and mitigate money laundering and terrorist financing risks faced. These steps include:

- identifying the money laundering and terrorist financing risks that are relevant;
- designing and implementing policies, procedures and controls to manage and mitigate these assessed risks;
- monitoring and improving (as appropriate) the effective operation of these controls;

B. Nominated Officer

The Nominated Officer is responsible for this policy ensuring it is current and relevant to the AML/CTF risk posed to YOUAREON and the AML/CTF Risk Assessment from which this policy is derived. The Board of YOUAREON is accountable for the AML/CTF Risk Assessment and Policy and is required to approve these documents and any subsequent changes.

C. AML/CTF Training

All YOUAREON employees must undergo appropriate AML/CFT basic awareness training as a minimum. Initial (online) AML/CFT training must be carried out within three months of an employee joining YOUAREON and subsequent training must take place at least every 12-18 months (but also when there is a change in AML/CFT regulations. The training will include but not limited to:

- What is money laundering/terrorist financing?
- Legislation/regulation relating to money laundering/terrorist financing

- Policies, procedures and controls
- Customer Due Diligence/Enhanced Due Diligence/Customer Monitoring
- The relationship of money laundering to problem gambling
- Politically Exposed Persons/Persons subject to domestic and international sanctions
- The role of senior management
- Who and the role of the Nominated Officer
- What is knowing, suspicion and reasonable grounds to know or suspect
- Staff obligation to report
- What is a suspicious activity report (SAR)
- What is an internal SAR and how to report to the Nominated Officer
- What is a 'request for defence' / how the Nominated Officer will manage
- The risk of tipping off
- The risk of money laundering/terrorist financing in relation to YOUAREON

D. Customer Due Diligence (CDD) and AML/CFT Checks

A fundamental requirement of the AML/CFT regulations is to conduct adequate CDD, including ascertaining a customer's full identification. Therefore, YOUAREON is committed to obtaining adequate evidence of a customer's identity prior to the commencement of any business relationship.

YOUAREON uses automatic electronic verification of the customer's age, name and address during the customer registration process. This is completed through the following automated process:

Step 1 – user uploads a copy of their ID (Driver's license or Passport)

Step 2 – user performs a liveness check using the camera on their device

Step 3 – user may be required to upload a utility bill or bank statement to prove their address information

The customer's details are then verified against the following list of data sources through an automated process using [www.sumsub.com](https://help.sumsub.com/products/external-databases-for-documents-validation). This performs the AML and CFT checks. <https://help.sumsub.com/products/external-databases-for-documents-validation>

Daily checks of the databases are performed to see if any of our active members have been added to any of the databases. In the event that a user has been added to one of these databases, that account is suspended within 24 hours and the customer is investigated by the Nominated Person.

Satisfactory verification will allow for the business relationship to be established (account opened) and for the customer to transact with YOUAREON until the level of their activity triggers a requirement for Enhanced Due Diligence (EDD).

All stages of the CDD process with each customer will be recorded together with any documentation and evidence obtained or provided.

Additionally the backend system will trigger alerts to the Nominated Person in which certain activities may arouse suspicion. Such alerts include but not limited to:

- Multiple failed deposits
- Multiple failed withdrawals
- Changing of payment options

E. Enhanced Customer Due Diligence (EDD)

YOUAREON is required to carry out EDD on clients where there is a higher risk of money laundering and/or terrorist financing or the customer is a politically exposed persons (PEP), or in any other situation when requested to do so by the Compliance department.

EDD will be conducted when:

- Any transaction over 4,000 NAF. and when subsequent additional thresholds are reached. This must be completed within 30 days;
- in any case where alerts have been triggered in respect to responsible gambling;
- the transaction is considered unusual, out of the norm for the customer profile or has hit AML/CTF triggers;
- customers identified as Politically Exposed Persons (PEPs) including family members or known close associate of a PEP whether at the outset of the business relationship or at any time during the business relationship. We need to establish the relationship before allowing them to continue our platform;
- a customer has been flagged by the Commission or any other relevant agency

The EDD minimum standard and measures include:

- establishing the source of wealth of the customer and affordability to maintain level of gambling;;
- where necessary requiring further information regards the source of funds being used for gambling;
- obtaining a detailed financial profile of the customer;
- enhanced monitoring of the customer activity;

F. Politically Exposed Persons (PEPs)

A PEP is defined by the Money Laundering Regulations (MLRs) 2017 as an individual who is entrusted with prominent public functions, other than as a middle-ranking or more junior official. This includes:

- heads of state, heads of government, ministers and deputy or assistant ministers;
- members of parliament or of similar legislative bodies;
- members of the governing bodies of political parties;
- members of supreme courts, of constitutional courts or of any judicial body the decisions of which are not subject to further appeal except in exceptional circumstances;
- members of courts of auditors or of the boards of central banks;
- ambassadors, charges d'affaires and high-ranking officers in the armed forces;
- members of the administrative, management or supervisory bodies of State-owned enterprises;
- directors, deputy directors and members of the board or equivalent function of an international organisation.

A "family member" of a PEP is defined as:

- a spouse or civil partner of the PEP;
- children of the PEP and the spouses or civil partners of the PEP's children;
- parents of the PEP.

A known close associate" of a PEP is defined as:

- an individual known to have joint beneficial ownership of a legal entity or a legal arrangement or any other close business relations with a PEP; or
- an individual who has sole beneficial ownership of a legal entity or a legal arrangement which is known to have been set up for the benefit of a PEP.

During registration our automated verification check will identify and flag whether someone is a PEP. Any PEP that is identified as high or medium will undergo EDD.

Risk categories are identified below:

High

- Heads and members of government
- Members of Parliament
- Head officials of banks/judiciary/military/religious groups/law enforcement
- Prominent political party members

Medium

- Head officials of banks/judiciary/military/religious groups/law enforcement

- Senior members of state agencies, high-rank civil servants
- Commissioners, ambassadors, consuls
- Heads and top ranking-officials of state-owned organizations

YOUAREON acknowledges that customers circumstances may change and PEP's will be searched on a monthly basis. Should a PEP be identified then the above process will be applied. Should an existing PEP be found to be no longer a PEP that person will be treated as a PEP for the following 12 months following the date of status change.

G. Records Retention

Records must be kept of all transaction data and data obtained for the purposes of identification, as well as of all documents related to AML/CFT topics (e.g. documentation on SARs and all AML/CDD onboarding, ongoing monitoring documentation and AML/CFT training). These records must be kept for a minimum of five years beginning from the date a business relationship ends.

Records relating to identification of customers and verification of identify will be kept for 5 years following the cessation of the business relationship. Transaction data will be kept for 5 years following the date of transaction.

Records relating to any AML/CTF investigation will be kept for 5 years following the completion of such investigation and/or review, this includes the submission of any reports to the FIU/law enforcement/Commission. Should there be any subsequent law enforcement enquiry the relevant records will be kept for 5 years from the date of that enquiry.

Upon expiry of the five years retention period, any personal data will be deleted unless YOUAREON is required to retain records for the purpose of any court proceedings, the purpose of other legal proceeding or the customer agrees to the retention of data for any other purpose.

H. Monitoring

All customers will be the subject of ongoing monitoring to ensure that their activity is consistent with the expected business relationship. YOUAREON recognises that money laundering risk can manifest itself in several guises from converting/transferring the proceeds of crime to criminal spend, including spend associated to problem gambling. Monitoring will form part of the process to understand these dynamics and mitigate any risks.

Customers being flagged as a result of monitoring for either the purpose of AML/CTF prevention or problem gamblers will be the subject of further investigation and determine what further action may be taken.

Customer transactions will be the subject to the following:

- level of deposits - are they increasing in value/frequency
- level of losses - are these increasing in value/frequency
- payment methods - has customer attempted to change his payment method and started to use a new device to deposit
- consistency of customer behaviour - has he/she started to complain about deposit limits we have imposed, is he/she increasing his self-imposed limits
- possible collusion to circumnavigate YOUAREON's monitoring procedures

- withdrawal of more than 10,000 NAf. in our transaction or linked transactions i.e. multiple withdrawals in the space of 72 hours
- High risk geographic locations
- Anonymous payment methods, crypto, pre-paid cards etc

Any CDD review should not have a 'shelf life' of more than 12 months. For example, if a customer hit the threshold of 4,000 NAf deposit in 24 hours, does not hit any other thresholds in the next 12 months BUT then hits the same threshold after 14 months, the EDD process should be started again.

In addition, an EDD review should be undertaken when a customer comes to notice through Responsible Gambling triggers/thresholds.

YOUAREON has implemented a 'closed loop' system in relation to customer payments and any subsequent withdrawals, meaning that once a customer has deposited via an accepted payment method, any withdrawal request made by the customer can only be returned to the same deposit method.

If a withdrawal (whether partially or completely) is to be completed back through a payment method that is different from the initial deposit method, (for example, if the initial deposit method is no longer available for use), a risk assessment must be done that should take into account information such as:

- Multiple destinations: YOUAREON will not permit withdrawals to be split into multiple payment mechanisms or bank accounts;
- High risk destinations: YOUAREON will not permit withdrawals to be returned to a country where there is a significant money laundering or terrorist financing concern.

I. Reporting of Suspicious Activities

YOUAREON recognises that the detection and reporting by staff of any suspicion is a key control in the prevention of money laundering and terrorist financing. If an employee or contractor of YOUAREON suspects that a customer may be linked to money laundering or terrorist financing, he/she must immediately report the suspicion to the Nominated Officer. This should be sent by email and contain the identification of the suspected customer and detailed information explaining why the customer was suspected.

It is the Nominated Officer's responsibility to decide whether a report or 'disclosure' about the incident needs to be made to the National Crime Agency (NCA) by making a Suspicious Activity Report (SAR). If a report is necessary, the Nominated Officer will make a report to the NCA as soon as possible.

J. Sanctions and High Risk Jurisdictions

YOUAREON shall screen all customers against the following sanctions lists:

- UN Consolidated Sanctions List
- EU Sanctions Map
- Curaçao-specific national designations

Customers transacting with such countries will be blocked, these include but are not limited to:

Restricted Countries

United States of America, Netherlands, Belgium, France, United Kingdom, Singapore, Australia, Spain, and Curaçao.

Sanctioned or High Risk Countries

Iran, North Korea, Myanmar, Russia, Ukraine, Belarus, Syria, Venezuela, Libya, Sudan, South Sudan, Democratic Republic of the Congo, Central African Republic, Mali, Somalia, Yemen