

Anti-Money Laundering Policy

Anti-Money Laundering (AML) Policy

1. Introduction

BG8 Entertainment NV is committed to the highest standards of ethical conduct and compliance with all applicable laws and regulations designed to combat money laundering, terrorist financing, and other financial crimes. This Anti-Money Laundering (AML) Policy establishes the framework within which the company operates to prevent the misuse of its services for illicit activities.

2. Purpose

The purpose of this AML Policy is to:

- Prevent BG8 Entertainment NV from being used as a conduit for money laundering, terrorist financing, or other financial crimes.
- Comply with applicable AML laws and regulations, including European Union's AML Directives, FATF Recommendations.
- Protect the integrity of BG8 Entertainment NV's business and reputation.

3. Scope

This policy applies to all employees, officers, directors, agents, contractors, and third-party vendors associated with BG8 Entertainment NV, as well as its subsidiaries and affiliates worldwide.

4. Legal Framework

BG8 Entertainment NV adheres to all AML laws, regulations, and directives in jurisdictions where it operates, including:

- National AML legislation and regulations.
- International standards set by the Financial Action Task Force (FATF).
- Sanctions issued by relevant bodies, such as the United Nations, European Union, and the U.S. Treasury Department's Office of Foreign Assets Control (OFAC).

5. Definitions

Policy Definitions used in this document:

- **Money Laundering (ML):** The process of disguising the origins of illegally obtained funds to make them appear legitimate.
- **Terrorist Financing (TF):** The provision of funds to support terrorist activities or groups.
- **Know Your Customer (KYC):** Procedures to verify the identity of customers and assess the risk of financial crime.
- **Politically Exposed Person (PEP):** An individual who holds or has held a prominent public position and may pose a higher risk due to potential involvement in corruption or bribery.
- **Sanctions List:** A list of individuals, entities, or countries subject to economic sanctions or restrictions.

The laws that address the money laundering offences cover a range of activities and offences in relation to money laundering. According to such laws, the money laundering offence may be committed by anyone by:

- Concealing, disguising, converting or transferring criminal property or removing it from Cyprus; or
- Entering into or becoming concerned in an arrangement which you know or suspect facilitates the acquisition retention, use or control of criminal property by or on behalf of another person; or
- Acquiring, using or possessing criminal property; or
- Failure to disclose knowledge or suspicion of another person(s) involvement in money laundering; or

- Tipping off or making a disclosure which is likely to prejudice an investigation being carried out by the law enforcement authority, knowing that such investigation is in progress.
- These offences cover a range of activities, which do not necessarily need to involve money or cash, regarding the proceeds of crime or criminal property. Criminal property in these cases may be a person's benefit from criminal conduct, received directly or indirectly, even if only in part. The conduct, activity or criminal property can be take place or be located in Cyprus or overseas.
- Potentially any director, employee or consultant of the Company, irrespective of what sort of work activity or service they undertake or provide for or on behalf of the Company, could commit an offence if they become aware of, or suspect the existence of criminal property, irrespective of the size or amount in question, the criminal conduct or activity, and fail to report their concerns.
- Where someone suspects money laundering, reports it, or is aware that someone else has reported it, they must exercise caution in what is discussed with others.

6. Roles and Responsibilities

- Individuals within the company:
 - **Board of Directors:** Ultimate oversight of the AML program.
 - **Compliance Officer:** Designated individual responsible for implementing and enforcing the AML program, including monitoring compliance and reporting suspicious activity.
 - **Employees:** Responsible for adhering to the AML Policy and reporting suspicious activity to the Compliance Officer.
- You must ensure that you read, understand and comply with this policy. If you are unsure about whether a particular act or activity constitutes money laundering, report to the board of directors or the director of the holding company, Sheermore Holding Limited.
- It is important to note that you will not be committing an offence of prejudicing investigation if you report your suspicions of possible money laundering according to this policy. The Company commits to ensure that your report is confidential, and you are not subject to any form of detrimental treatment because of making a report.

7. Key AML Program Components

7.1 Risk-Based Approach

BG8 Entertainment NV adopts a risk-based approach to identify, assess, and mitigate money laundering and terrorist financing risks. Customers, transactions, and services are categorized as low, medium, or high risk, with appropriate controls applied accordingly.

7.2 Customer Due Diligence (CDD)

Before establishing a business relationship, the company will:

- Verify the identity of customers using reliable and independent documentation.
- Obtain information about the nature and purpose of the business relationship.
- Perform Enhanced Due Diligence (EDD) for high-risk customers, such as PEPs or customers from high-risk jurisdictions.

7.3 Enhanced Due Diligence (EDD)

The company will perform additional Enhanced Due Diligence under the following circumstances:

EDD is initiated when a player exhibits one or more of the following risk factors:

- **High-Risk Behaviour:** Significant deposits, high-stakes wagers, or irregular spending patterns.

- **Source of Funds Concerns:** Unclear or suspicious origins of the money used for gambling.
- **Politically Exposed Persons (PEPs):** Individuals in influential positions or connected to potential corruption risks.
- **Geographical Risk:** Customers located in high-risk regions.
- **Suspicious Activity:** Red flags such as attempts to bypass limits, unusual transaction patterns, or irregular withdrawals.

Key Elements of Enhanced Due Diligence

- 1. Customer Identification and Verification**
 - Confirming the customer's identity through official documents (e.g., passport, driver's license).
 - Checking against sanctions lists, PEP databases, and adverse media reports.
- 2. Source of Funds (SoF) and Source of Wealth (SoW) Verification**
 - Requesting evidence of the origin of the funds (e.g., bank statements, payslips, or tax records).
 - Evaluating if the customer's gambling behaviour aligns with their financial circumstances.
- 3. Ongoing Monitoring**
 - Tracking transactions for suspicious activity, such as rapid deposits, withdrawals, or irregular betting behaviour.
 - Investigating transactions that exceed set thresholds.
- 4. Customer Risk Profiling**
 - Analysing factors such as income, gambling frequency, and behavioural patterns to determine the customer's risk level.
 - Assigning risk scores to inform necessary actions.
- 5. Additional Information Requests**
 - Seeking further documentation to address concerns about the legitimacy of the customer's activity.
 - Conducting interviews or follow-up communications when needed.
- 6. Relationship Analysis**
 - Identifying third parties who may be funding the customer's gambling activities or are otherwise connected.

7.4 Ongoing Monitoring

The company continuously monitors transactions and customer activity to:

- Identify unusual patterns or red flags.
- Ensure that activities align with the customer's profile and expected behaviour.
- Detect and investigate potential suspicious activities.

7.5 Suspicious Activity Reporting (SAR)

The Compliance Officer will file Suspicious Activity Reports (SARs) with the appropriate regulatory authority if any suspicious activities are detected. Examples include:

- Transactions that appear inconsistent with a customer's profile.
- Structuring of transactions to avoid reporting thresholds.
- Transactions involving sanctioned individuals or entities.
- Rapid deposits and withdrawals.
- Funding or withdrawals involving third parties.

The process for filing SARs with the relevant Financial Intelligence Unit (FIU) of the jurisdiction is as follows:

- **Internal Escalation and Review**
 - Once suspicious activity is identified, staff escalate it to the Compliance/AML Officer or designated team.
 - The compliance team investigates further and determines whether the activity warrants a report to the FIU.
- **Reporting to the FIU**
 - If the activity is deemed suspicious, the company submits a Suspicious Activity Report (SAR) or Suspicious Transaction Report (STR) to the appropriate FIU.
 - The report typically includes:
 - Customer details (identity, account history).
 - Transaction specifics (amount, frequency, method).
 - Reason for suspicion (behavioural or transactional anomalies).
- **Confidentiality**
 - The company or its employees are legally prohibited from tipping off the customer about the report.
 - Only authorized personnel are involved in the reporting process to ensure confidentiality and regulatory compliance.

7.6 Record Keeping

The company retains all relevant AML records, including:

- Customer identification documents.
- Transaction records.
- Suspicious activity reports (SARs).
- Internal and external communications related to AML compliance. Records will be maintained for a minimum of 7 years, or longer if required by law.

7.7 Sanctions Compliance

The company will not conduct business with individuals, entities, or countries subject to international sanctions. All customer data and transactions will be screened against applicable sanctions lists.

7.8 Employee Training

All employees are required to undergo AML training upon hiring and at regular intervals thereafter. Training topics include:

- Identifying and reporting suspicious activities.
- Understanding AML regulations and red flags.
- Responsibilities under this policy.

7.9 Independent Audit

Regular independent audits will be conducted to evaluate the effectiveness of the AML program. The audit findings will be reviewed by senior management, and corrective actions will be taken as necessary.

7.10 Risk Profile

A key element of the AML profile of a player is the risk profile of a player, this is to be reviewed after a player initiates account activity, as this activity provides the data needed to evaluate risk factors.

- Upon Account Registration: due to limited information, a preliminary or default risk level will be assigned.
- Activity Commencement: Once players engage in activities (e.g., deposits, withdrawals, bets), the system gathers behavioural and transactional data to perform a more robust risk assessment.

- Behavioural Analysis: Players' activities, such as unusual transaction patterns, excessive deposits, or sudden changes in behaviour, are analysed to determine their risk level.
- Dynamic Risk Scoring: our risk management systems uses dynamic models that update risk levels continuously based on ongoing activity.

7.11 Adverse Media Searches

Adverse Media searches will be conducted on players to review publicly available information (news articles, blogs, legal records, etc.) for negative coverage or associations involving a customer. These searches help uncover potential risks such as:

- Criminal activity (fraud, money laundering, corruption, or organized crime).
- Regulatory violations or financial misconduct.
- Reputational risks (media controversies, legal disputes, etc.).
- Connections to sanctioned entities or Politically Exposed Persons (PEPs).

The Adverse Media Searches will be conducted during EDD for customers triggering Enhanced Due Diligence, such as high-value gamblers or individuals exhibiting suspicious activity, and as part of ongoing monitoring of players, Adverse Media checks will be part of continuous monitoring to capture new or emerging risks.

The company will perform the following Adverse Media Searches

- Manual Searches: Conducting keyword-based searches through search engines and public databases.
- Automated Solutions: Utilizing third-party tools or AML compliance software that scan media databases for adverse information efficiently.
- Structured and Unstructured Data: Reviewing both formal (news outlets, legal filings) and informal sources (blogs, forums, social media).

7.12 PEP/Sanctions Screening

The company will perform Sanctions screening by verifying customer data (e.g., name, date of birth, address) against official sanctions lists to ensure the company does not engage with:

- Individuals or entities subject to financial, economic, or trade restrictions.
- Persons or organizations involved in illegal activities, such as money laundering, terrorism financing, or proliferation of weapons.
-

The company will utilise the following Sanctions Lists:

1. United Nations Security Council (UNSC) Sanctions List
2. Office of Foreign Assets Control (OFAC) – U.S. Treasury Department's list (including SDN: Specially Designated Nationals).
3. European Union (EU) Sanctions List
4. HM Treasury's Financial Sanctions List – United Kingdom
5. Local/Regional Sanctions Lists – Depending on the player's jurisdiction.

The PEP screening for the company involves identifying individuals who hold or have held prominent public positions and their close associates or family members. PEPs are considered higher risk due to their potential exposure to corruption, bribery, and money laundering.

Categories of PEPs Include:

- Government officials (heads of state, ministers, parliament members).
- Senior executives of state-owned enterprises.
- Judges or high-ranking judicial officials.
- Military officials or heads of law enforcement agencies.
- Immediate family members and close associates of PEPs.

The Sanctions/PEP Screening is performed at the following periods:

1. At Onboarding: All new customers are screened to identify PEPs or sanctions risks before account activation.
2. Ongoing Monitoring: Existing customers are screened periodically to identify updates in sanctions or PEP status.
3. During Enhanced Due Diligence (EDD): High-risk customers or transactions trigger additional screening.

7.13 Transaction Reviews

This process involves analysing historical transaction data to identify any suspicious activities or patterns that may have been missed during initial monitoring.

A **retrospective transaction review** refers to a backward-looking analysis of a customer's past transactions and behaviours to detect:

- Unusual patterns: Transactions inconsistent with the customer's profile.
- Red flags: Missed indicators of money laundering, fraud, or suspicious behaviour.
- Compliance gaps: Areas where automated systems or manual monitoring failed to flag transactions.

The Company performs a retrospective transaction review when the following occurs:

- Regulatory Trigger:
 - After a regulatory audit or a request from an authority to examine historical data.
- Post-Incident Review:
 - Following the detection of suspicious activity, fraud, or AML breaches involving a customer or group of customers.
- System Enhancement:
 - When new monitoring tools, rules, or parameters are implemented, a retrospective review ensures previously overlooked risks are identified.
- Periodic Risk-Based Review:
 - Companies may proactively conduct reviews based on the risk level of customers or transactional volumes.

The Company will follow the steps below in the review:

- Data Collection:
 - Gathering historical customer transactions, account activity, and behavioural data.
- Analysis:
 - Reviewing for anomalies such as rapid deposits/withdrawals, third-party funding, or unusual transaction sizes.
- Risk Scoring:
 - Reassessing customers' risk profiles based on findings from the review.
- Flagging Suspicious Activity:
 - Identifying previously unreported transactions and submitting Suspicious Activity Reports (SARs) or Suspicious Transaction Reports (STRs) where necessary.
- Documentation and Reporting:
 - Maintaining detailed records of the review process and findings for regulatory compliance.

8. Crypto Payment Monitoring

Customer paying by Crypto currency generates unique challenges for the Company due to the following:

- Anonymity: Transactions are anonymous but traceable through blockchain analysis.

- Cross-Border Nature: Payments can easily move across jurisdictions.
- Volatility: Value fluctuations can complicate monitoring.
- AML Risks: Crypto can be misused for illicit purposes like money laundering or terrorism financing.

The Company has the following Crypto Payment Monitoring Procedure

1. Customer Due Diligence (CDD) and Enhanced Due Diligence (EDD)
 - Collect and verify customer identity before accepting crypto payments.
 - Conduct EDD for high-risk customers, ensuring the legitimacy of crypto sources.
2. Blockchain Analytics Tools
 - The company uses Chainalysis analytics platforms.
 - This tool analyses and monitors crypto transactions to detect:
 - Links to dark web markets or illicit activities.
 - Funds originating from high-risk wallets, mixers, or tumblers.
 - Anomalous transaction patterns (e.g., rapid transfers or layering).
3. Transaction Screening and Monitoring
 - Track crypto payments for:
 - High-value transactions inconsistent with a customer's risk profile.
 - Rapid movement across multiple wallets (indicative of layering).
 - Transactions from or to sanctioned wallets or entities.
 - Implement real-time or periodic screening of wallets against global sanctions lists.
4. Source of Funds Verification
 - Require customers to provide proof of the source of crypto funds where applicable.
 - This can include wallet ownership verification or evidence of legitimate acquisition (e.g., purchase records).
5. Risk-Based Approach
 - Apply more stringent monitoring to high-risk transactions or customers, such as:
 - Large crypto payments.
 - Customers from high-risk jurisdictions.
 - Payments involving privacy coins
6. Suspicious Activity Reporting (SAR/STR)
 - Flag and investigate unusual or suspicious crypto transactions.
 - Report to relevant Financial Intelligence Units (FIUs) when needed.
7. Ongoing Monitoring
 - Implement systems to continuously monitor and assess crypto transactions.
 - Update processes and tools as new crypto risks or regulatory requirements emerge.

8. Prohibited Activities

BG8 Entertainment NV strictly prohibits:

- Accepting funds or engaging in transactions that are known or suspected to involve criminal activity.
- Establishing or maintaining anonymous accounts or accounts under fictitious names.
- Engaging in transactions with individuals, entities, or countries on sanctions lists.

9. Reporting Obligations

Reporting Procedures for Suspicions of Money Laundering

Where a director, an employee and/or consultant knows of or suspects money laundering activity, they must disclose this as soon as practicable to the board of directors or the director of the holding company, Sheermore Holding Limited. The disclosure should be within "hours" of the information coming to your attention, not weeks or months later.

The report must include as much detail as possible, for example:

- Full details of the people, provider or customer involved (including employee, if relevant);
Full details of the nature of their involvement;
The types of possible money laundering activity involved (please see types of offences listed on the first page of this policy);
The dates of such activities, including whether the transactions have happened, are ongoing or are imminent;
- Reasons for suspicion or concern;
- Any other relevant information.

Do not attempt to investigate the activity yourself, discuss it with others, including colleagues, suspected person or provider, or with anyone else, make any comments or notes in any shared files or documents, and do not remove any relevant files or information unless specifically instructed by the board of directors or the director of the holding company, Sheermore Holding Limited. You may be requested to provide additional information about your report to Sheermore or directly to the law enforcement authorities.

10. Breaches of this Policy

The consequences for not making a report under this policy may be detrimental to the Company and to you personally. Other than your personal direct liability under the Mauritius money laundering laws, you may face disciplinary action, which could result in termination of your employment or services contract.

This policy does not form part of the contract of employment and the Company may amend it at any time. This policy and any amendments are made available to you at all times on the Company's shared online resources.

In relation to the consultants or directors, this policy is an integral part of your consultancy agreement; any amendments to this policy or its revocation will be communicated to you according to the provisions of the terms of the agreement.

11. Investigations

You need to take caution not to do anything that may prejudice the investigation by the authorities.

Criminal conduct may also be relevant to the money laundering offences if conducted overseas. If, in the course of performance of your work or services for or on behalf of the Company you know or suspect someone is undertaking or is involved in the activities described above in another country, you need to follow this policy.

Risk factors which may, either alone or cumulatively with other factors, suggest the possibility of money laundering activity are:

- A new service provider or a customer with no previous 'history' with Sheermore or any company within Sheermore group of companies (the "service provider" and the "customer").
A secretive service provider or customer (one that refuses to provide requested information without a reasonable explanation);
- Concerns about the honesty, integrity, identity of a service provider or a customer;
- Illogical third party transactions: for example, unnecessary routing or receipt of funds from third parties or through third party accounts;
- Involvement of an unconnected third party without logical reason or explanation;
- Payment or offer of a payment of an invoice in cash;
 - Overpayments by a customer;
 - Changes of the recipient of payments or a payer, particularly to and from a higher risk country;
 - Where, without reasonable explanation, the size, nature and frequency of transactions or instructions is out of line with normal expectations;
- A transaction without obvious legitimate purpose or which appears uneconomic, inefficient or irrational;
- Poor business records or internal accounting controls;

- A previous transaction for the same provider or the customer which has been, or should have been, reported as suspicious.

It is impossible to give a definitive list of ways in which to spot money laundering or how to decide whether to make a report. Facts which tend to suggest that something 'odd' is happening may be sufficient for a reasonable suspicion of money laundering to arise.

12. Compliance

This Anti-Money Laundering Policy applies to all BG8 Entertainment NV employees, including temporary employees, and its directors and consultants. Sheermore requires that all of its directors, staff and consultants to demonstrate the highest standards of honesty and integrity in the performance of their work and services, and this includes compliance with the appropriate legislation.

In its business activities Sheermore is striving to comply with the spirit of the anti- money laundering laws. Potentially any director, an employee or a consultant could be caught by the money laundering provisions if they know of or suspect money laundering and either become involved with it in some way and/or do nothing about it; then they may be liable to prosecution. Heavy penalties and criminal prosecution can follow for those who are convicted of the money laundering.

13. Internal AML Audit

As part of the companies regulations, the company will conduct internal AML audits to ensure compliance with AML/CTF (Counter-Terrorism Financing) laws and identifying weaknesses or gaps in the AML framework.

Purpose of Internal AML Audits

1. Assess Compliance: Verify that the company complies with AML regulations, policies, and procedures.
2. Evaluate Effectiveness: Measure the performance of AML systems, controls, and reporting mechanisms.
3. Identify Gaps: Highlight weaknesses, inefficiencies, or non-compliance in the AML program.
4. Mitigate Risks: Ensure risks of money laundering or terrorist financing are effectively managed.

The company will perform an internal AML audit every quarter, and the process is as follows:

- A review of the company's AML policies, procedures, and risk assessments.
- Assessing customer due diligence (CDD) and enhanced due diligence (EDD) processes.
- Evaluating the effectiveness of transaction monitoring systems.
- Examining the process for filing Suspicious Activity Reports (SARs) or Suspicious Transaction Reports (STRs).
- Ensuring staff AML training is current and effective.
- Confirming record-keeping and reporting requirements are met.

14. Policy Review and Updates

This AML Policy will be reviewed annually or as necessary to ensure compliance with changes in laws, regulations, and business practices.

15. Contact Information

For questions or to report suspicious activities, contact:

- **Compliance Officer:** Joseph Noonan, AML Manager, j.noonan@magloo.com

16. Approval and Acknowledgment

This AML Policy has been approved by the Board of Directors and is effective as of 17/12/2024. All employees are required to read, understand, and acknowledge their adherence to this policy.

Authorized Signatory:

A handwritten signature in blue ink, appearing to read 'Patrick Roberts', with a stylized flourish at the end.

Patrick Roberts, Director
Updated 17/12/2024

This comprehensive policy ensures compliance with AML regulations while mitigating risks associated with money laundering and terrorist financing. It should be adapted based on the specific services, customer base, and regulatory environment of your company. Consult legal or compliance experts for further customization.