

ANTI-MONEY LAUNDERING AND COUNTERING FINANCING OF TERRORISM POLICY

Deep Dive B.V.

Document Information

Subject	Anti-Money Laundering and Countering Financing of Terrorism Policy
Purpose	‘Deep Dive B.V.’ Policy document containing policies to comply with AML Legislative and Regulatory requirements.
Involvements	All departments
Responsibility	Money Laundering Reporting Officer
Approval	Directors
Review	Annually or earlier as needed

Classification	Company Confidential
----------------	----------------------

Change History

Date	Version	Author	Summary Changes	MLRO
19/08/2024	1.0	“Deep Dive B.V.”	A New document was created as part of the AML/CFT Program review.	
30/05/2025	1.1	“Deep Dive B.V.”	Updated in line with Curacao AML/CFT Policy guidelines	

Contents

Contents.....2

1. Introduction4

2. Regulatory Framework5

3. Scope of this Policy6

4. Money Laundering Reporting Officer6

5. Risk Assessment.....7

6. PEP / Sanctions Lists Checks8

7. Customer Acceptance Policy8

8. Customer Due Diligence9

9. Reliance on third parties to perform customer due diligence9

10. Payment Methods.....9

11. High-Risk Jurisdictions.....10

12. Internal Controls10

13. Suspicious Transaction Report12

14. Notifications of Fraud and Law Enforcement or Regulatory Authorities’ Requests13

15. Employee Training.....13

16. Employee Screening.....14

17. Retention of Records.....14

18. Policy Distribution14

19. Due Diligence for Third Parties15

20. Policy URL.....15

21. Compliance and Consequences of Non-Compliance15

22. Appendix 1. References15

23. Appendix 2. Glossary of Terms.....16

1. Introduction

“Money laundering” is generally defined as “engaging in acts designed to conceal or disguise the nature, control, or true origin of criminally derived proceeds so that those proceeds appear to have been derived from legitimate activities or origins or otherwise constitute legitimate assets.”

The Proceeds of Crime are funds derived from illicit sources and from which a benefit or enjoyment may be obtained. Although the aim is not to launder the funds or to fund terrorism it is still considered to be an illegal activity and subject persons should be aware of such activity and must report it as if it was ML/FT.

The policies set forth herein (the “Policies”) are intended to satisfy the statutory requirements of the relevant legislation and to provide direction to ‘Deep Dive B.V.’ (or the “Company”) in complying with its obligations at law by taking all reasonable steps and exercising all due diligence to avoid the commission of an offence of money laundering or funding of terrorism.

The Company is aware that criminals and terrorists may attempt to use the Company’s services to channel funds from illegal activities.

The National Ordinance on the Reporting of Unusual Transactions (NORUT) provides indicators to help identify unusual transactions. These indicators (consisting of objective and subjective indicators) describe when an (executed or intended) transaction is to be labeled as unusual, and thus should be reported to the pertinent national authorities.

Objective Indicator: In this case, the reporting entity is obliged to report an unusual transaction. The list of objective indicators describes under which circumstances a transaction is to be considered as unusual. Objective indicators may include the following:

- A transaction which is reported to the police or judicial authorities in connection with money laundering or the financing or terrorism.
- An intended transaction carried out by or for the benefit of a person, legal person, group or entity that is mentioned on a list compiled in pursuance of the Sanctions National Ordinance.
- A transaction giving cause to assume that it may relate to money laundering or terrorist financing.
- A transaction amounting to NAF (ANG) 4,000.00 or more, regardless of whether this transaction is carried out in cash, via a check or another payment instrument or electronically or in any other non-physical manner.
 1. A giro-based transaction amounting to NAF (ANG) 4,000.00 or more: A giro-based transaction is a transfer from a bank account of the service provider to a local or international bank account carried out at the request of the client addressed to the service provider.
 2. The taking into deposit or the releasing out of deposit of an amount of NAF(ANG) 4,000.00 or more, at the request of the client.
 3. Sale of tokens to a client in the amount of NAF (ANG) 4,000.00 or more. The term "tokens" includes at least chips and credits.
 4. Payout of prizes in the amount of NAF (ANG) 4.000.00 or more.

5. All other cases.

Subjective Indicator: In case of a subjective indicator, the transaction is considered unusual if the reporting entity (based on its knowledge of its clients, their income and their business activities, their gaming (-related) activity and any other circumstance that may be relevant) has reasonable knowledge to presume that a transaction is related to money laundering or terrorism financing. In case the answer to this assessment is yes, then the reporting entity has the obligation to report.

2. Regulatory Framework

Below is a list of all the relevant AML legislation and regulations pertaining:

- Curacao Gaming Board Regulations for AML/CFT.
- National Ordinance on Identification when rendering services (N.G 2017, no 92).
- NORUT – National Ordinance on the Reporting of Unusual Transactions (N.G 2017, no 99).
- Sanctions National Ordinance (N.G 2014, no 55).
- Kingdom Sanction Act (N.G 2016, no 54).
- National Decree entering into force of Kingdom Sanction Law (N.G 2017, no 2).
- The Code of Criminal Law (Penal Code) N.G 2011, no 48).
- National Ordinance on Games of Chance (LOK).

3. Scope of this Policy

The scope of this policy is to establish policies from which procedures on internal control, risk assessment, risk management, and compliance in relation to AML/CFT will be drawn up.

Users of this and related policies should also refer, where relevant, to the new Penal Code of Curacao, relative National Ordinances, and Ministerial Decrees, measures/guidelines which may be issued from time to time by any relevant authority or agency.

Unless the context requires otherwise, words and expressions used in the Policy shall have the same meaning as that set out in the applicable laws and regulations.

The Company is determined and committed to preventing the carrying out of financial activities through its systems that may be related to AML/CFT.

The Company shall comply with its obligations at law by establishing the necessary and relevant processes to prevent AML/CFT and to ensure any suspicious activities are escalated to the relevant authorities.

The Policies outline the general and minimum standards of internal anti-money laundering and combating funding of terrorism (AML/CFT) which should be adhered to by the Company's management and employees.

4. Money Laundering Reporting Officer

A Money Laundering Reporting Officer (MLRO) is appointed to be the business owner of AML/CFT Risk Assessment, Controls, Policies, and Procedures. The MLRO reports directly to the **Board of Directors**

The MLRO's responsibilities shall include, but are not limited to:

- Risk assessment and management,
- Ensuring customer due diligence measures and ongoing monitoring,
- Record-keeping.
- Promoting internal control,
- Perform internal auditing of AML/CFT processes (unless internal auditing function is available),
- The monitoring and management of compliance with, and the internal communication of, such policies and procedures,
- Monitoring of relevant staff and agent screening,
- Self-education and education of relevant staff in AML/CFT on an annual basis or more regularly if deemed necessary,

- Liaison with law enforcement authorities, and
- Manage Investigation Order requests received from the authorities.

5. Risk Assessment

Business ML/FT Risk

The business must conduct a Business Risk Assessment (BRA) at the outset, covering four areas:

- Customer Risk
- Geographical Risk
- Product/Service and Transaction Risk
- Distribution Channel Risk

The BRA must be reviewed at least once annually or when any major change in the above risk categories occurs, such as a new product addition or an added payment method type to the offer.

The BRA must:

- Identify AML-related risks that the business is exposed to
- Design and implement policies and procedures to manage and mitigate these assessed risks.
- Monitor and improve the effective operation of these controls; and
- Record what has been done, and why.

The company directors and MLRO must approve the BRA.

Customer ML/FT Risk

Customers are to undergo an ongoing ML/FT Risk Assessment from the start of the business relationship and thereafter based on:

- Customer type,
- Products used (e.g. sportsbook),
- Services (e.g. poker, bingo, betting exchange),
- Transactions/payment systems,
- Delivery channels, and
- Geographical origin of the customer and/or payment method.

After registration, a customer's activity will undergo ongoing monitoring through automatic and manual processes to reconsider risk level depending on changes in the customer's activity and to establish the point at reaching the relevant due diligence requirements thresholds.

6. PEP / Sanctions Lists Checks

Customers are also to be screened to confirm that they are not included on the Sanctions Lists. Customers are asked on the first deposit to confirm whether the customer is him/herself, or is a family member of, or known associate to, a person that is considered a Politically Exposed Person (“PEP”). The customer is further checked to confirm PEP status once the relevant thresholds are hit, or the customer’s profile is considered higher than low risk.

Customers matching any one of these categories are to be automatically considered as a high-risk profile, and appropriate measures are to be taken to ensure that the business activity with them is not of an ML/FT nature. Sanctioned individuals cannot be accepted as customers. Refer to **PEP / Sanctions Lists Procedure** and **Customer Acceptance Policy**. PEP and Sanctions List checks will be carried out by Shufti PRO software.

To comply with the United Nations Security Council resolutions and the Common Foreign and Security Policy of the European Union. Compliance with sanctions imposed by the UN Security Council is mandatory under the Charter of the United Nations. Upon notification of a sanctioned person playing on any of the sites across the company, any funds held on the gaming account with frozen and reported to the FIU immediately.

It is the reporting entity’s responsibility to perform ongoing checks of its client database against the international lists of designated persons/ entities/ groups to make sure the reporting entity is not permitting/ facilitating access to funds to the ones mentioned on the sanctions lists. The primary sanctions list reporting entities must check against are UN, EU, USA-OFAC lists, Curacao National Lists (currently not in place), local lists of all jurisdictions where online gaming and gambling activities are provided and/or clients are accepted.

The Sanctions Screening will be performed before the first deposit is initiated, and the rescreening may happen based on the customer’s risk.

7. Customer Acceptance Policy

The business must have a customer acceptance policy outlining:

- A description of the type of players that are likely to pose a higher-than-average risk of ML/FT/FP.
- The risk indicators present low, medium, or high risk.
- The level of Customer Due Diligence (CDD) measures, including ongoing monitoring to be applied.
- The circumstances under which service to someone is declined.
- Politically Exposed Persons (PEP) and Sanctions Screening checks and policy

8. Customer Due Diligence

Customer Due Diligence (CDD) Measures include:

- Collection of identification details.
- Verifying the Identity of the Customer.
- Determining the customer profile and levels of activity and adjusting the profile as and when necessary,
- conducting ongoing monitoring of the business relationship, to ensure transactions are consistent with what the business knows about the customer, and the results of the risk assessment; and
- Retention of records of these checks and updating them when there are changes.

The Customer Due Diligence Procedure defines the procedure used to carry out Customer Due Diligence, including timeframes when this will be triggered and in which cases Enhanced Due Diligence will need to be performed.

Depending on the customer's risk profile, customers who have been requested to complete the CDD Procedure may have their accounts restricted during this period.

Should the CDD Procedure not be completed within the established timeframes of such a request, the customer's account will be considered to have failed to complete CDD and thus will be denied from any further activity/frozen of funds. The raising of a Suspicious Transaction Report ("STR") is to be considered. Such a decision is to be taken and recorded by the MLRO.

Unless a STR has been raised and an appropriate period has passed in which the customer has still not completed CDD, the account may be closed, and deposited funds still present on the customer's account will be returned to the deposit method, where possible, less any charges incurred by the business for transmission to this destination.

9. Reliance on third parties to perform customer due diligence

The company does not rely on third parties to perform CDD measures in line with the Curacao regulatory requirements, laws, and regulations.

10. Payment Methods

The company will not accept receiving or making cash deposits or payments in relation to the customer's activities.

The company will only make use of payment methods that are offered by licensed financial institutions and regulated by a European Economic Area (“EEA”) financial regulator, and the funds do not originate from high-risk jurisdictions.

The Company will hold received payments from customers in a player’s account, distinct from the Company accounts.

The Company will always keep track of transactions carried out using these payment methods and identify funds that are received or remitted by customers, together with any transfers of funds that are made into or out of the player’s account for settling the customer’s remote gaming activity. It will also be able to identify when thresholds for due diligence have been reached.

In all instances, where possible, funds returned to customers shall be returned to the customer’s originating payment method. If this is not possible due to the nature of the payment method or in case of the account not being available anymore to receive funds, payments will be transferred only to a bank account in the customer’s name, following the completion of the customer’s due diligence process.

Transaction monitoring will be carried out using internal systems and tools.

11. High-Risk Jurisdictions

Geographical risk assessment is conducted on all countries where the company accepts customers, the assessment will be completed using the lists below:

- FATF Jurisdictions under Increased Monitoring.
- FATF/CFATF High Risk Jurisdictions subject to a Call for Action.
- EU List identifying high risk 3rd countries with strategic deficiencies.
- The US Department of State Money Laundering assessment (INCSR).
- Basel AML Index.

The company does not accept customers from any high-risk countries identified on the above lists, this is enforced by blocking players from playing from these countries. Enhanced due diligence will be requested on any customers who are resident from a high-risk country.

Deep Dive may initiate enhanced due diligence when the person's nationality, country of birth, or transactions are from countries identified by the FATF and the CFATF.

12. Internal Controls

Internal control procedures have been designed to comply with the regulations. Internal controls take the form of manual controls implemented on a daily basis by the company’s operations teams and computer/automated controls inherent within the gaming system software.

The gaming system has inbuilt internal control tools which based on the information inputted by the prospective customers can trigger red flags about suspicious activity to the operations team. Refer to some examples below:

- ***Prevention of multiple accounts held by same user:*** Inbuilt system checks confirm whether the email provided by the prospective customer is unique in the customer database preventing the possibility of a player having multiple accounts. If a player tries to open more than one account, for whatever reason, The company reserves the right to block or close any or all of the player's accounts at its discretion.
- ***Detection of any underage registrations:*** Underage registrations are automatically not allowed by the system.
- ***No cash and no credit policy:*** Credit card deposits are accepted by the system only if the customer enters a valid credit card number with sufficient funds. A player can participate in any game only if the player has sufficient funds on his/her account for such participation. It is the company's policy not to accept cash and not to give any credit whatsoever for participation in any game.
- ***Withdrawal is only allowed if the name of person requesting the withdrawal is the same name of person holding the account:*** The company's policy is that it shall only affect pay-out to an account, card, wallet, or similar instrument in the name of the player receiving pay-out. Under no circumstances shall. The company affects a payout to a player in a name other than in the name of the player. Note, the company relies on 3rd party payment providers verifying the name of the account holder for bank transfer payouts.

Internal controls are not entirely computer-dependent. The operations teams also has an important part in detecting and preventing money laundering. The below are a number of controls operated by the operations team:

- Ongoing monitoring and assessment of players' risk indicators and changes in player's patterns.
- On a daily basis, a deposits report is reviewed by the payment and risk department, and follow ups made on suspicious transaction deposits.
- Monitoring of large deposits and withdrawals, and/or deposits and immediate withdrawals or withdrawals with insufficient gameplay.
- All withdrawals are checked and approved by the team
- The operations team confirms that the name of the person requesting the withdrawal is the same name as a person holding the bank account. Suspicious credit card deposits, transactions, and accounts are followed up by a verification process, including outbound calls.
- Customer log activity is regularly analysed for indications of suspicious activity.
- Additional verification on suspicious deposits, transactions, or accounts will include, but not be limited to:
- Call Player to verify telephone number, take note of player's response/phone manner in call. This call is made by support staff in the same language as the player's account.

- Check if player exists on local country phone book, tax records, electoral register, additional public databases, with the same information.
- Request additional ID, proof of address, and copies and statements of bank or credit cards.

The management team has stats on the volumes such procedures are yielding and performs monthly quality checks on agent work done, sampling at least 25 cases per agent.

13. Suspicious Transaction Report

The company is required to adhere to the stipulations of the National Ordinance for Identification of Services and to detect and report either intended or unusual transactions. Deep Dive has implemented adequate procedures to cover:

- The recognition of unusual transactions.
- The documentation of unusual transactions.
- The reporting of unusual transactions.

The Regulations for the combating of Money Laundering, the Financing of Terrorism and Proliferation of weapons of mass destruction, state that the following transactions or intended transactions are deemed unusual

- Transactions which in connection with money laundering or terrorism financing are reported to the Police or the Department of Justice
- Transactions by or on behalf of a natural or legal person, a group or an entity, that is named on a list, adopted by virtue of the Sanctions National Ordinance (N.G. 2014 no. 55)
- Transactions in the amount of NAf. 5,000 or more, regardless of whether the transaction is made in cash, by check or other form of payment, or through electronic or other non-physical means. This includes but is not limited to:
 - A cashless transaction in the amount of NAf. 5,000 or more.
 - Accepting or releasing a deposit in the amount of NAf. 5,000 or more at the request of the client
 - A cashless transaction is a transfer from a bank account of the casino to a local or international bank account, at the request of the client.
 - Accepting or releasing a deposit in the amount of NAf. 5,000 or more at the request of the client.
 - Sale to a customer of chips in the amount of NAf. 5,000 or more. "Chips" include, but is not limited to, tokens and credits.
 - A cash out in the amount of NAf. 5,000 or more.

An internal Suspicious Transaction Report is to be sent directly to the MLRO whenever there is a suspicion that a customer is engaged in ML/FT.

No one is to divulge to co-workers, line managers, and especially the customer/s that an STR has been raised as this is potentially considered to be 'tipping-off'. An employee who raises an STR must escalate directly to the MLRO.

Refer to the Internal Suspicious Transaction Report Procedure for guidance on STR escalation.

14. Notifications of Fraud and Law Enforcement or Regulatory Authorities' Requests

The Company will record and take appropriate actions whenever notification of fraud or requests by Law Enforcement or relevant Regulatory Authorities are received. The Company will follow due process to ensure such notifications or requests are processed without delay, and the Company will, within its abilities, assist such authorities effectively.

Notifications, Law Enforcement, and Regulatory authorities' notifications may also provide just cause to ensure the company's Responsible Gambling, Fraud, Money Laundering, and Terrorist Funding risk mitigation strategies are working effectively. Where gaps are identified, the Company will take immediate action to resolve such gaps.

All reports should be sent without delay to the FIU. The term "without delay" is interpreted as follows:

- Regarding Objective Reports (Reports based on an objective indicator): With the exception of the Banking Sector, all reporting entities should send their unusual transaction reports within 48 hours after the transaction has been executed, or after there has been an intention for a transaction.
- Regarding Subjective Reports (Reports based on a subjective indicator): For all reporting entities, including the Banking Sector, the period between the execution of the transaction (or the intention to execute a transaction) and the moment the Compliance Officer receives the report, should not exceed 24 hours. As of the moment that the Compliance Officer receives the transaction report, the Compliance Officer will have 10 working days to complete the relevant research with regard to a possible Money Laundering/Terrorism Financing (ML/TF) situation. If, after the research period (maximum 10 working days), there is a suspicion of ML/TF, the Compliance Officer must report the transaction within 48 hours to the FIU.

15. Employee Training

Within an appropriate period of the commencement of employment, employees are to be provided with ML/FT training to ensure they are aware of measures, policies, controls, and procedures that are in force. This training shall include:

- General awareness of Money Laundering / Terrorism Funding for all employees,
- Specific Guidance on the related measures, controls, policies, and procedures in place within the company for employees specifically occupying roles related to AML/CFT Controls and Compliance,
- An assessment is needed to ensure that the employee has grasped the key points of the training received.

The evidence of the training provided to employees is to be recorded. Training needs to be refreshed at least annually.

The MLRO is also required to attend annual refresher training and to keep up to date with the subject.

16. Employee Screening

The Company's prospective employees who are to be involved with or connected to activities that would fall within the scope of this policy are to be screened before they are employed.

The company is to ensure that they are fit and proper to occupy positions in which they will participate in the provision of services to the customer. The use of third-party screening providers may be engaged to ensure this.

The Company will carry out monitoring of the activities of its employees during their employment to identify concerns of internal fraud or other criminal activity potentially affecting the company's operations and obligations. The Company will always do its utmost to respect the privacy of its employees.

Employees are also encouraged to report internal suspicious or fraudulent activity by employees to the MLRO and/or Directors directly, and should they wish to remain anonymous, to do this via an anonymous letter or email service providing as many facts and information as possible.

17. Retention of Records

Customer and Transactional data collected during the relationship with the customer will be maintained for a period of five (5) years from the end or termination of the customer relationship. End of the customer relationship is defined as from the last day the customer effected any movement of funds to and from his account, or a successful login.

Should statutory obligations arising from other laws, regulations, or based on a request from a regulator, a requirement be established to keep records for a longer period be in place, this will be taken into consideration and adhered to.

Documents will not be retained beyond the required obligations and will be deleted.

18. Policy Distribution

All employees receive a copy of the AML policy and other associated policies upon induction, and each year, once a review is completed and signed, the new AML documents is circulated to all staff, including subcontractors and Third-party suppliers when applicable by email, including a summary of any material changes.

19. Due Diligence for Third Parties

The company has processes in place, when applicable, to carry out due diligence upon establishing a business relationship in line with our regulatory requirements and to ensure that the company only works with reputable entities.

20. Policy URL

This policy cannot be accessed online through the company website.

21. Compliance and Consequences of Non-Compliance

The company is obligated to apply to all regulations covered under section 2 of the regulatory framework within this policy. Should Deep Dive violate these regulations, the company can be subject to disciplinary actions, legal implications, or business risks.

In situations of non-compliance, the following actions could be taken:

- The company will be subject to regulatory fines.
- Regulatory enforcement.
- Respective action on particular regulations and processes.
- License revoked.
- Assess adequately the risk of money laundering or terrorist financing.

Contact Information

Any questions regarding this policy, please contact:

Name – Mark Taylor

E-mail Address – markt@diligenzagroup.com

Contact Number - +356 99911164

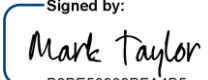
22. Appendix 1. References

United Nations - [Financial Sanctions Consolidated List](#)

European Union – [Consolidated list of sanctions](#)

23. Appendix 2. Glossary of Terms

- AML – Anti Money Laundering CDD – Customer Due Diligence
- CFT – Combatting Funding of Terrorism EDD – Enhanced Due Diligence
- DE – Designated Employee
- FATF – Financial Action Task Force (www.fatf-gafi.org) MLRO- Money Laundering Reporting Officer
- PEP – Politically Exposed Persons
- RBA – Risk Based Approach SAR – Suspicious Activity Report SDD – Simplified Due Diligence
- STR – Suspicious Transaction Report

Signed by:

Signature: B3BE58983BFA4B5...

MLRO: Mark Taylor