

AML Policy

Date: 01/05/2025

Version: 1.5

From: Compliance
Department

To: Alea Employees

Objective :

The general policy sets the frame of all Alea Overseas N.V. specific policies, procedures and controls related to the prevention of money laundering and financing terrorism under the applicable laws and regulations.

AML POLICY

Version 1.5.

Version	Effective date	Approving official	Responsible officer	Comments	Net review date
1.0.	08-05-2020	eMoore N.V.	Helene Klein – Compliance Manager	First version	
1.1.	11-01-2021	eMoore N.V.	Helene Klein – Compliance Manager	Proceeding with the below amendments: • Adding references to the relevant Curaçao legal framework instead of only having references to the 'national and European Union regulations. • Adding references to the Curaçao FIU, and not only to the 'Authority'.	
1.2.	15-03-2021	eMoore N.V.	Helene Klein – Compliance Manager	• Changing all the mentions of 'Alea Games N.V.' to 'Alea Overseas N.V.'	•
1.3.	14-09-2021	eMoore N.V.	Helene Klein – Compliance Manager	• Updating the Policy as per the Board Decision held on 10/09/2021 and Board Decision communicated on 14/09/2021.	•

AML POLICY

Version 1.5.

1.4.	02-09-2022	eMoore N.V.	Helene Klein – Compliance Manager	Yearly review and making sure the Policy is still up-to-date with the current Laws and Regulations in Curaçao.	
1.5.	01-05-2025	eMoore N.V.	Lilly Gourbin – Compliance Manager	Review adapting the protocol to the current Curaçao legal framework.	01-05-2026

Table of Contents

Table of Contents.

<i>Definitions and Abbreviations.....</i>	<i>5</i>
<i>1. AML/CFT Policy.....</i>	<i>8</i>
1.1 Policy	8
1.2 Objectives.....	9
<i>2. Policy, controls, and procedure.....</i>	<i>9</i>
<i>3. Regulatory Framework</i>	<i>10</i>
3.1 National regulations.....	10
3.2 International regulations.....	11
<i>4. Risk assessment.....</i>	<i>11</i>
4.1 Business Risk Assessment.....	12
<i>5. Policy, controls, Client relationships.....</i>	<i>15</i>
5.1 Customer Due Diligence (CDD).....	15
5.2 Termination of the business relationship.....	16
5.3 Internal controls.....	16
5.4 Training	17
<i>6. Record keeping.....</i>	<i>18</i>
<i>7. The Monitoring of Counterparty activities</i>	<i>18</i>
<i>8. Compliance Manager: internal and external reports.....</i>	<i>19</i>
a. Internal reports to the Compliance Manager.....	19
b. External reports by the Compliance Manager	20
<i>9. Operational Due Diligence Process</i>	<i>21</i>
a. Prior to signing a new Client: Simple Due Diligence.....	21
b. When a client reaches 1M GGR: Enhanced Due Diligence.....	21

Definitions and Abbreviations

Account Holder	An individual who has a Player Account on the Website.
Anti Money Laundering ("AML")	All efforts focused on the prevention of money laundering, the direct or indirect participation in any transaction that seeks to conceal or disguise the nature or origin of funds derived from illegal activities.
Caribbean Financial Action Task Force ("CFATF")	An organization of states and territories of the Caribbean territory that have agreed to implement common countermeasures against money laundering and terrorism financing. (www.cfatf-gafic.org)
Combatting terrorist financing ("CFT")	All efforts focused on the prevention of providing funds at the disposal of terrorists to be used for committing terrorist attacks.
Combatting proliferation of weapons of mass destruction ("CPWMD")	Efforts aimed at combatting the financing or provision of funds for the sale, transfer, or export of nuclear, chemical or biological weapons, their delivery systems and related materials.
Cryptocurrency	Distributed, open-source, mathematically based peer-to-peer virtual currencies that have no central administering authority, and no central monitoring or oversight. Examples include Bitcoin, Ethereum, Litecoin and Dogecoin.
Cryptocurrency transaction	The deposit and withdraw of cryptocurrencies into and out of a Player Account held by a Player.
the Company	Alea Overseas N.V., a limited liability company duly organized under Curaçao law registered with the Chamber of Commerce and Industry in Curaçao under number 131334
Employee	Any person working for the Company.

AML POLICY

Version 1.5.

Financial Action Task Force ("FATF")	An intergovernmental organization dedicated to developing standards and promoting effective implementation of legal, regulatory and operational measures for combating money laundering, terrorist financing and other related threats to the integrity of the international financial system. (www.fatf-gafi.org)
Financial Intelligence Unit ("FIU")	Pursuant to FATF Recommendation no. 26, countries must establish a Financial Intelligence Unit (FIU) that serves as a national center for the receiving (and, as permitted, requesting), analysis and dissemination of suspicious transaction reports (STR) and other information regarding potential money laundering or terrorist financing.
Know Your Client ("KYC")	Know Your Client, the mandatory process of identifying and verifying the client's identity when opening a Player Account and periodically over time.
Money Laundering ("ML")	A process through which criminals conceal, or attempt to conceal, the origin of the proceeds of their illegal activities and disguise, or attempt to disguise, such proceeds to make them appear to be legitimate.
Money Laundering Reporting Officer ("MLRO")	Designated individual in charge of the review of KYC information and the monitoring of Player Account activities. The MLRO might further be assisted by designated personnel.
Player	Individual who has registered with the Company for the purpose of making use of the Services offered on the Website and for which a Player Account has been opened providing him/her with a unique code.
Player Account	An account granted to an individual after registration on the Website. The Player Account is created and issued by the Company and is required for wagering with real money. Only one Player Account is permitted per person, per IP address, per family and per Shared Environment.

AML POLICY

Version 1.5.

Politically Exposed Person ("PEP")	A person entrusted with a prominent public function, such as a senior political figure. Individuals closely related to this person, for instance immediate family members and close associates, are also considered PEPs. PEPs are classified as a Money Laundering risk since they may be exposed to property that has been generated by corruption and bribery because of their position.
Prohibited Jurisdictions	Jurisdictions prohibited under the Curaçao license conditions by the Curaçao Gaming Authority at a certain moment, jurisdictions restricted by decision of the Company's managing director at a certain moment when and where still applicable, as well as countries mentioned on the FATF blacklist or on which any financial sanctions has been imposed by the EU/ U.N. and/or the OFAC.
Proliferation Financing ("PF")	The act of providing funds or financial services which are used, in whole or in part, for the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials (including both technologies and dual-use goods used for non-legitimate purposes), in contravention of national laws or, where applicable, international obligations.
the Regulator	The Curaçao Gaming Authority (CGA). The regulator for the entire gaming industry operating in and from Curaçao.
Shared Environment	An environment that has a common internet connection which includes but is not limited to airplanes, households, universities, libraries, cyber cafes, coffee shops and offices. Only one Player Account is permitted per Shared Environment.
Service	the gaming and betting offers provided by the internet gateway operated by the Company to the Account Holder, through the Website.

AML POLICY

Version 1.5.

Terms and Conditions	The terms and conditions for the use of the Services, as published on the Website.
Terrorism Financing ("TF")	The process of making funds or other assets available to terrorist groups or individual terrorists to support them, even indirectly, in carrying out terrorist activities.
Website	the online gaming platform offering online gaming services operated by the Company.

1. AML/CFT Policy

1.1 Policy

Money Laundering, Terrorism Financing and proliferation of weapons of mass destruction are some of the ever-growing threats for national and international economies throughout the world, forcing all vulnerable sectors to have measures in place for the prevention of their misuse for these purposes. Individuals involved in ML and/or TF continually attempt to exploit services and products to conceal their unlawful activities and proceeds' true nature. Illicit efforts by such individuals must be recognized and thwarted by all feasible means. AML policies incorporate regulations and laws for limiting financial criminals from concealing funds collected through illicit sources.

ML in the online gaming industry manifests itself in two opposing forms:

- The use of criminal funds to fund gambling activities; and
- The exchange of criminally acquired funds for legitimate money.

In both cases, authorities fear that those phenomena damage sports, the online gaming industry, and society as a whole. Therefore ML, when not eliminated, can have far-reaching implications.

TF may not involve the proceeds of criminal conduct but rather an attempt to conceal the origin or intended use of the funds, which will later be used for unlawful purposes. Terrorists regularly adapt how and where they raise and move funds and other assets in order to circumvent safeguards that jurisdictions have put in place to detect and disrupt this activity. Identifying, assessing and understanding TF risks is an essential part of dismantling and disrupting terrorist networks, as well as the effective implementation of the risk-based approach of CFT measures. PFWMD may involve the sale, transfer, export, of weapons of Mass destruction, like nuclear weapons and atomic weapons. Such proliferation must be countered as well due to it posing a signification threat to international peace and security, as identity by relevant United Nations

AML POLICY

Version 1.5.

Security Council Resolutions (UNSCRs). Therefore, the CP measures involve identifying and assessing the risks of potential breaches or evasion of the targeted financial sanctions to proliferation financing and taking appropriate mitigating measures with the level of risks identified.

The Company takes AML/CFT/CPF seriously and has policies in place to ensure compliance with the regulations in the jurisdictions where we operate. The Company's procedures and internal controls are designed to ensure compliance with all applicable national and international regulations and will be reviewed and updated on a regular basis to ensure appropriate policies, procedures and internal controls are in place to account for both changes in applicable law and changes in our business.

1.2 Objectives

This Policy outlines the AML/CFT strategy of the Company in order to:

- a) ensure that statutory and regulatory obligations to prevent ML and FT are met, taking positive action to minimize risk of the Company's products and services being used for the purpose of laundering funds and using proceeds of criminal activity, or terrorist financing;
- b) ensure that the Company does not engage with or continue established relationships with those whose conduct gives rise to suspicion of involvement with ML and/or TF;
- c) terminate any relationships where the Account Holder's conduct gives the Company reasonable cause to believe or suspect involvement with illegal activities. Any such termination shall follow the reporting of the suspicion and thereafter shall be undertaken in conjunction with the relevant authorities and in accordance with the relevant regulations; and
- d) comply with the Company's AML, CFT and CPF obligations based on national and international regulations.

2. Policy, controls, and procedure

According to the Curaçao legal framework, Alea Overseas N.V. shall maintain written policies, procedures and controls approved by its Senior Management or/and Board of Directors to mitigate and manage effectively the risks identified in its risk assessment.

Those policies, procedures and controls must include:

- Customer due diligence (CDD), including the systems for Client's identification and verification, enhanced due diligence (EDD), measures for high-risk Clients, circumstances in which additional information will be sought in the light of Clients' activity, identification and scrutiny of unusual patterns of activity.

AML POLICY

Version 1.5.

- Internal controls including the screening of relevant employees and the establishment of an independent audit function.
- Training of relevant/all employees.
- Record Keeping.
- Internal reporting of any knowledge or suspicion of money laundering to the Compliance Manager. The recording of information not acted upon by the Compliance Manager with reasoning why no further action was taken, the arrangements for Compliance Manager reports to senior management, the procedures for handling Suspicious Activity Reports (SARs) including the circumstances in which a defense (appropriate consent) must be sought.
- The monitoring and management of compliance with such policies, procedures and controls by the Compliance Manager, including the arrangements for and record keeping of communicating such documentation and any change thereto to all relevant employees¹.

Policies, procedures and controls will be communicated to relevant employees by the Compliance Manager from the email address internal.compliance@alea.com.

3. Regulatory Framework

3.1 National regulations

Pursuant to the Code of Criminal Law (Penal Code) (N.G. 2011, no. 48), money laundering is a criminal offence in Curaçao.

Further main national regulations relating to money laundering and terrorist financing are the following:

- a) The National Ordinance on Money Laundering (P.B. 1993, no. 52);
- b) The National Ordinance on the Reporting of Unusual Transactions (N.G. 1996, no. 21) as lastly amended by N.G.2024, no.41(N.G.2017, no.92)(NORUT) together with all amendments thereto and all related National Decrees containing general measures and Ministerial Decrees with general operations;
- c) The National Ordinance on Identification of Clients when Rendering Services (N.G. 1996, no. 23) as lastly amended by N.G. 2024 no.41 (N.G. 2017, no. 99)) (NOIS) together with all

¹ Relevant employees are employees whose work is relevant to the compliance with the current legislation, employees capable of contributing to the identification and mitigation of the risks as well as to prevention and detection of money laundering. This includes the holders of personal management licenses as well as employees responsible for completing Customer Due Diligence measures.

- amendments thereto and all related National Decrees containing general measures and Ministerial Decrees with general operations;
- d) The National Decree containing general measures on the execution of articles 9, paragraph 2, and 9a, paragraph 2, of the National Ordinance on Identification of Clients when rendering Services. (National Decree containing general measures on Penalties and Administrative Fines for Service Providers) (N.G. 2010, no. 70);
 - e) Sanctions national decree Al-Qaida c.s., the Taliban of Afghanistan c.s. Osama bin Laden c.s., and terrorist to be designated locally (N.G. 2010, no. 93); and
 - f) National Ordinance on the Obligation to report Cross-border Money Transportation N.G. 2002, no. 74) together with all amendments thereto and all related National Decrees containing general measures and Ministerial Decrees with general operations.
 - g) National Ordinance extension of validity sanction decrees 2018 (N.G. 2018, no. 34);
 - h) Kingdom Sanction Act (N.G. 2016, no. 54);

These laws and decrees serve as the basis for the procedures maintained by the financial sector of Curaçao to detect and deter industry related risks for money laundering, the financing of terrorism or other criminal activities.

3.2 International regulations

As a member of the Financial Action Task Force (www.fatf-gafi.org) and of the Caribbean Financial Action Task Force (www.cfatf-gafic.org), Curaçao is meeting international standards by regularly implementing these standards in its national legislation.

On an international level, the FATF plays an important role in the combating of ML, TF and PF. The FATF monitors the progress of its members in implementing necessary measures, reviews ML and TF techniques and countermeasures, and promotes the adoption and implementation of appropriate measures globally.

In performing these activities, the FATF collaborates with other international bodies involved in combating money laundering and the financing of terrorism. In total 34 countries are direct members of the FATF and through regional organizations over 180 countries are connected to the FATF.

Subsequently the present policy is a combination of the FATF and local AML/CFT rules and regulations. This ensures a solid, internationally accepted basis regarding AML/CFT. In case local laws and regulations require additional compliance duties, the Company is free to develop additional procedures to comply with local regulations.

4. Risk assessment

The possibility of online gaming being used by criminals to assist ML and/or TF poses many risks for the Company, such as criminal and regulatory sanctions and/or reputational damage for the

AML POLICY

Version 1.5.

Company and/or its Employees. For this purpose, the Company must carefully identify its risks and manage them accordingly.

The Company takes the following steps to manage its risks appropriately:

- i. identifying the ML and TF risks relevant to the Company;
- ii. assessing the level of risk;
- iii. understanding the impact of the risk;
- iv. designing and implementing appropriate policies, procedures and controls to manage and mitigate these risks;
- v. monitoring and improving the effective operation of these controls and identifying any weaknesses; and
- vi. recording what has been done and why.

In view of the above, the Company must conduct a risk assessment to analyse the risks faced by the Company and ensure that the identified risks are properly mitigated and resources adequately invested.

The possibility of online gaming being used by criminals to assist ML and/or TF poses many risks for the Company, such as criminal and regulatory sanctions and/or reputational damage for the Company and/or its Employees. For this purpose, the Company conducted a comprehensive risk assessment consisting of a Business Risk Assessment and a Customer Risk Assessment to identify its risks and manage them accordingly. In line herewith, further specific procedures are drawn up to further describe the processes that need to be in place.

4.1 Business Risk Assessment

The following table outlines the identified risks, the corresponding risk category as well as their likelihood and potential impact during the course of business and the risk score.

Risk ID	Risk	Risk Category	Likelihood	Impact	Risk score (LxI)
R001	Breach of licensing terms in any jurisdiction	Regulatory & legal	4	5	20
R002	Failure to comply with AML/CTF regulations	Regulatory & legal	5	5	25
R003	Non-compliance with responsible gambling regulations	Regulatory & legal	4	4	16
R004	Advertising violations	Regulatory & legal	3	4	12
R005	High player payout rates reducing profit margins	Financial	3	4	12
R006	Cash flow liquidity issues	Financial	4	5	20
R007	Fraudulent chargebacks	Financial	4	3	12
R008	DDoS attack disrupting platform access	Cybersecurity	3	5	15

AML POLICY

Version 1.5.

R009	Data breach or data loss	Cybersecurity	4	5	20
R010	Unauthorized access to customer data	Cybersecurity	3	5	15
R011	System outages or downtime during peak events	Operational	3	5	15
R012	Dependence on third-party software or platforms	Operational	4	3	12
R013	Poor internal controls over betting limits or bonuses	Operational	2	4	8
R014	Entry of a dominant competitor in key market	Market	4	4	16
R015	Decline in consumer trust in online gambling	Market	3	5	15
R016	Reduced customer retention	Market	3	4	12
R017	Negative media coverage or scandals	Reputation	4	5	20
R018	Social responsibility criticisms	Reputation	3	4	12
R019	Players developing gambling addiction	Responsible Gambling	3	5	15
R020	Failure to intervene with at-risk players	Responsible Gambling	2	4	8
R021	Poor performance of software vendors	Vendor	3	4	12
R022	Payment processor instability or failure	Vendor	4	4	16

Mitigation strategy and residual risk

The following tables show the mitigation strategy to be implemented and the effectivity rate, followed with the activities to reduce residual risk, the residual risk score and the residual risk level.

Risk ID	Mitigation Strategy	Mitigation control effectiveness
R001	Regular audits, engage local counsel	12
R002	Automated monitoring tools, staff training	15
R003	Self-exclusion tools, RG team	10
R004	Ad approval workflow, legal review	7
R005	Game RTP analysis, betting limits	7
R006	Liquidity reserves, cash forecasting	12
R007	Payment verification systems, fraud detection software	7
R008	Cloudflare, WAF, redundancy	9
R009	Encryption, multi-layer security	12
R010	Role-based access control, 2FA	9
R011	Load testing, cloud infrastructure	9
R012	SLA enforcement, redundancy plans	7
R013	Control dashboards, alerts	5
R014	Brand differentiation, loyalty programs	10
R015	Transparency campaigns, PR management	9
R016	Personalized offers, CRM automation	7

AML POLICY

Version 1.5.

R017	Crisis communication plan	12
R018	Fund RG programs, public reports	7
R019	Monitoring, self-exclusion tools	9
R020	Behavior tracking algorithms	5
R021	Performance KPIs, backup vendors	7
R022	Multiple PSPs, weekly performance review	10

Risk ID	Activities to reduce Residual risk	Risk score (LxI)	Residual risk score	Residual risk level
R001	Continuous license compliance training, implement internal reviews	20	8	Medium
R002	Enhance KYC processes, deploy AI for transaction monitoring	25	10	Medium
R003	Audit RG tools quarterly, include customer feedback	16	6	Medium
R004	Implement retention journeys, feedback loops with frequent users	12	5	Low
R005	Build trust with player protection features, transparency dashboards	12	5	Low
R006	Introduce real-time liquidity dashboards, diversify revenue streams	20	8	Medium
R007	Analyze competitor promotions, improve personalization engine	12	5	Low
R008	Set up DDoS scrubbing service, automate scaling responses	15	6	Medium
R009	Conduct periodic penetration testing, enforce data classification policies	20	8	Medium
R010	Apply anomaly detection for access patterns, monitor admin activities	15	6	Medium
R011	Use high-availability architecture, incident response planning	15	6	Medium
R012	Use player interaction scoring, initiate guided interventions	12	5	Low
R013	Implement regular vendor reviews, renegotiate SLAs	8	3	Low
R014	Perform market SWOT analysis, adjust promotional strategies	16	6	Medium
R015	Assess vendor dependency, contractual penalties for downtime	15	6	Medium
R016	Develop reputation resilience strategy, engage media consultants	12	5	Low
R017	Media monitoring, train spokespersons, prepare PR statements	20	8	Medium
R018	Fund responsible gambling campaigns, issue public responsibility reports	12	5	Low
R019	Install automated alert systems, limit manual overrides	15	6	Medium
R020	Perform regular PSP reliability audits, diversify payment options	8	3	Low
R021	Automate detection of addictive behaviors, player nudges	12	5	Low
R022	Onboard backup payment partners, conduct stress tests	16	6	Medium

5. Policy, controls, Client relationships

Politically Exposed Persons

According to Article 1.A.18 Amendment P.B 2024, n° 41 of National Ordinance on identification when rendering Services (PB.2017, n° 92) and National Ordinance on the Reporting of Unusual Transactions (P.B 2017, n° 99)

“a natural person who holds or has held a prominent public function, as well as his or her immediate family members and close associates, or persons who hold or held a prominent function in international organizations, as well as his or her immediate family members and close associates”

Pursuant to Article 1.q. National Ordinance on identification when rendering Services (PB.2017, n° 92), where a person who was a politically exposed person is no longer entrusted with a prominent public function, this person shall still be considered as such for a period of 12 months after the date on which that person ceased to be entrusted with that public function.

According to Article 5.a National Ordinance on identification when rendering Services (PB.2017, n° 92) and Article 1.k Amendment P.B 2024, n° 41 of National Ordinance on identification when rendering Services (PB.2017, n° 92) and National Ordinance on the Reporting of Unusual Transactions (P.B 2017, n° 99), Alea Overseas N.V. must have in place appropriate risk-management systems and procedures to determine whether a Client or the beneficial owner of a Client is a politically exposed person, or a family member or a known close associate of a politically exposed person, and to manage the enhanced risks arising from the relevant person's business relationship or transactions with such a Client.

Alea Overseas N.V. will not enter business relationships with politically exposed persons, family members or known close associates thereof.

5.1 Customer Due Diligence (CDD)

Pursuant to Article 2 National Ordinance on identification when rendering Services (P.B 2017, n° 92), Alea Overseas N.V. must apply customer due diligence measures when establishing a business relationship, suspects money laundering or terrorist financing and doubts the veracity or adequacy of documents or information obtained for the purposes of identification or verification.

Alea Overseas N.V. must also apply customer due diligence measures at other appropriate times to existing Clients on a risk-based approach when becoming aware that the circumstances of an existing Client relevant to its risk assessment for that Client have changed.

The extent of CDD measures may differ from case to case insofar that they reflect the risk assessment carried out by Alea Overseas N.V. and the assessment of the level of risk arising for each Client (*refer to Part VII for more details*).

AML POLICY

Version 1.5.

The size of the transactions undertaken by a Client, as well as the regularity and the duration of the business relationship shall be taken into account in assessing the level of risk of a Client.

Alea Overseas N.V. is not required to continue to apply CDD measures where all the following conditions are met:

- continuing to apply customer due diligence measures in relation to that Client would result in the commission of the offense of tipping off².

5.2 Termination of the business relationship

Alea Overseas N.V. has the obligation to terminate business relationships with customers where CDD requirements are not completed.

5.3 Internal controls

Relevant employees appointed by Alea Overseas N.V. are employees whose work is relevant to the compliance with National Ordinance on Identification when rendering Services (N.G. 2017, n° 92) and National Ordinance on the Reporting of Unusual Transactions (N.G. 2017, n° 99), employees capable of contributing to the identification and mitigation of the risks as well as to prevention and detection of money laundering. This includes the holders of personal management licenses, as well as employees responsible for completing Customer Due Diligence measures.

Alea Overseas N.V. shall carry out screening³ of relevant employees both before the appointment and during their appointment. To assess their integrity, all relevant employees are required to provide an extract of criminal record when recruited. Alea Overseas N.V. considers introducing an obligation for relevant employees in their employment contracts to update their employer in case of change in their situation.

Alea Overseas N.V. will implement an independent audit function with the responsibility to:

- examine and evaluate the adequacy and effectiveness of the policies, procedures and controls to comply with current legislation.
- make recommendations in relation to those policies, procedures and controls.
- monitor the operator's compliance with those recommendations.

Alea Overseas N.V. has systems in place enabling it to respond to enquiries from anti-money laundering and law enforcement authorities as to whether it maintains or has maintained in the

² Tipping off (regulated sector) is the fact for a person to disclose any matter reported to the Nominated Officer or to disclose that an investigation into allegations that an offence related to money laundering or terrorism financing is being contemplated while such disclosure is likely to compromise any investigation to be conducted and the information on which the disclosure is based came to the person in the course of a business in the regulated sector.

³ According to GCB (Curaçao Gaming Control Board) guidelines, screening means an assessment of the skills, knowledge, and expertise of the employee to carry out their functions effectively and an assessment of the conduct and integrity of the individual.

previous 5 years a business relationship with any person and the nature of that relationship. To ensure Alea Overseas N.V. answers fully and rapidly, all requests from official authorities shall be redirected to the Compliance Manager on the dedicated email address internal.compliance@alea.com.

5.4 Training

According to Art. 22mm.3 National Ordinance on the Reporting of Unusual Transactions (N.G. 2017, n° 99) O 5 SEPTIES 92, Alea Overseas N.V. shall ensure that its relevant employees are:

- made aware of the law relating to money laundering and terrorist financing and of the requirements of data protection relevant to the application of said regulation.

Relevant employees shall be made aware of their legal obligations and responsibilities (namely, failure to disclose, tipping off and harming investigation) under POCA 2002 Part 7 Money Laundering and Terrorism Act 2000 Part 3. Relevant employees have a legal defence to prosecution if they make an internal report to the Compliance Manager as soon as is reasonably practicable after information or other matter comes to their attention in the course of business, as a result of which they know or suspect, or have reasonable grounds for knowing or suspecting, that a person is engaged in money laundering or terrorist financing.

Reasonable enquiries of a Client, conducted in a tactful manner, regarding the background to a transaction or activity that is inconsistent with the normal pattern of activity is prudent practice, forms an integral part of CDD and should not give rise to tipping off.

As regards to data protection, specifies that processing personal data for the purpose of preventing money laundering or terrorist financing is to be considered necessary for the exercise of a function conferred on Alea Overseas N.V. by the law (task carried out in the public interest). The relevant employees shall be made aware that any personal data obtained for the purpose of preventing money laundering or terrorist financing may only be processed for those purposes.

- Relevant employees/all will be regularly trained in how to recognize and deal with transactions and other activities or situations which may be related to money laundering or terrorist financing.

ACAMS⁴ training programs⁵ shall be provided to all relevant employees in accordance with their role and level/nature of responsibilities. The effectiveness of the trainings must be monitored through assessments of competence following the trainings (competency tests following training). A written record of the trainings given to relevant employees shall be maintained to monitor who has been trained, when they received the training, the nature of the training and the effectiveness thereof through the collection of assessment questionnaires.

⁴ Association of Certified Anti-Money Laundering Specialists - <https://www.acams.org/>

⁵ Appendix 1

6. Record keeping

According to Article 7 National Ordinance on Identification when rendering Services (N.G. 2017, n° 92), Alea Overseas N.V. shall keep:

- copy⁶ of any documents and information obtained to fulfill the customer due diligence requirements for a period of 5 years starting from the closure of the Client's account.
- supporting records must be maintained, subject to CDD measures and ongoing monitoring, to allow for the reconstruction of the transaction for a period of 5 years starting from the closure of the Client's account.

Where the record-keeping obligations under the current legislation are not observed, an operator or person is open to prosecution and sanctions, including imprisonment for up to two years and/or a fine, or publication of statement of censure by the supervisory authority.

Once the period of 5 years has expired, any personal data obtained to prevent money laundering and terrorist financing shall be deleted unless Alea Overseas N.V. is required to retain records containing personal data (for the purposes of a court proceeding for example) or has reasonable grounds for believing that records containing the personal data need to be retained for the purpose of legal proceedings.

7. The Monitoring of Counterparty activities

The Managing director of the Company takes reasonable steps to prevent the activities of ML, TF and PF and monitors the usage of the services and related transactions conducted by the Counterparty to detect any possible attempts for misuse of the platform through either the tampering with the provided software or any further requests.

Unusual activities

Any activities which are outside of the scope of the business relation, are not in line with the usual activities of the Counterparty and/or do not fit the normal business profile of a counterparty, require further investigation into the specifics of the case and might result in the submission of an unusual activity report to the Curaçao FIU where the activity gives rise of a suspicion of money laundering. Examples are:

⁶ Copy means a copy of the original document which would be admissible as evidence of the original document in court proceedings.

AML POLICY

Version 1.5.

Identity fraud

At the detection of any use of falsified documentation (identity fraud) of the Counterparty, the Company will proceed to conduct an in-depth investigation. If the investigations confirm this fault, the Company will resolve to cancel/terminate the agreement with the Counterparty.

Refund requests

Refunding creates a legitimate paper trail between the Company and the Counterparty. Any business proposal or activity creating a credit which merits a refund is to be analyzed to prevent an unnecessary creation of the refund of an excess amount, thereby possibly aiding in the layering of ML by creating a legitimate financial transaction originated by the Company. The following activities should be thoroughly reviewed:

- Overcalculation of usage: intentional overcalculation of the required usage of a product followed by a refund request for the non-use;
- Overpayment: the intentional overpayment followed by a request for a refund
- Unnecessary upgrades/ changes in the product portfolio followed by a request for refunding for the unused products.

8. Compliance Manager: internal and external reports

a. Internal reports to the Compliance Manager

Any employee – not only relevant employees - to whom information or other matter comes in the course of business, as a result of which they know or suspect, or have reasonable grounds for knowing or suspecting, that a person or customer is engaged in money laundering or terrorist financing must make an internal disclosure to the Compliance Manager using the dedicated email address internal.compliance@alea.com

- Knowledge means knowing something to be true and can be inferred from circumstances (e.g.: failure to ask obvious questions).
- Suspicion means thinking that the possibility of the fact exists but a vague feeling of unease or a speculation does not suffice. An unusual transaction is not ultimately suspicious, it is only the basis for further enquiry which may require judgement as to whether there is or not suspicion.

AML POLICY

Version 1.5.

- Having reasonable grounds for knowing or suspecting means that from facts or circumstances known in the course of business it is reasonable to infer knowledge or to form suspicion (= objective test of suspicion). When a court decides that an objective test of suspicion is satisfied and no internal report was made, to defend themselves, the employees must demonstrate that they took reasonable steps in the particular circumstances to conduct appropriate level of Customer Due Diligence.

Once an employee has properly reported to the Compliance Manager as soon as practicable, they have satisfied their statutory obligation (legal defence).

All suspicions reported internally to the Compliance Manager should be documented or electronically recorded. The report should include full details of the Client who is the subject of concern and a full statement of the information giving rise to the grounds for knowledge or suspicion of money laundering or terrorist financing, as well as the corresponding documentation. Internal reports do not require to know the exact nature of the criminal offence.

b. External reports by the Compliance Manager

The Compliance Manager shall consider any internal report and determine whether it gives rise to knowledge or suspicion, or reasonable grounds for knowledge or suspicion, that a person is engaged in money laundering or terrorist financing. In the course of this review, the Compliance Manager shall consider any available information held about the Clients such as the length of the business relationships and the identification records. The Compliance Manager may require further information to be obtained from the Clients depending on what is already known and how easy it is to make further enquiries. Any approach to the Client should be made sensitively and preferably by someone already known to the Client, to minimize the risk of alerting the Client.

If the Compliance Manager decides not to submit a report to the Curaçao FIU, the reasons for not doing so should be clearly documented or electronically recorded and retained. These records should be kept separately by the Compliance Manager so that the information therein is not disclosed accidentally.

The Compliance Manager must make a disclosure as soon as practicable to the Curaçao FIU where he/she decides that a report gives rise to grounds for knowledge or suspicion. External reports do not require to know the exact nature of the criminal offence.

Alea Overseas N.V. will request defense from the Curaçao FIU whenever reporting SARs. The statutory mechanism which allows the Curaçao FIU either to grant or to refuse the 'prohibited act' going ahead is called appropriate consent.

Anytime a SAR is reported, Alea Overseas N.V. will aim at ending the business relationship with the concerned Client. The defense will in any case be requested for closing the Client account. No action shall be taken on the Client account until appropriate consent is granted and the Compliance Manager advises to take action.

In the event where a law enforcement agency would request Alea Overseas N.V. to continue trading with a Client as further investigations are conducted, the Compliance Manager should:

- record the risk of participating in such activity, assurances provided by law enforcement, possible money laundering offenses, timetables provided, gravity of the offenses being investigated and the purpose of the request.
- ask in writing for confirmation of such request from the law enforcement agency.

9. Operational Due Diligence Process

Art. 3 NOIS (Nº92)

a. Prior to signing a new Client: Simple Due Diligence

- Copy of gambling license of the jurisdiction(s) in which the Client's Company is operating;
- Dated, Signed and Certified Corporate Structure;
- Copy of the Memorandum and Articles of Association;
- Copy of the Certificate of Incorporation;
- Copy of the valid colored passport or identity card of each Director and shareholder/Ultimate Beneficiary Owner (UBO);
- Register of Directors / Commercial Register.

b. When a client reaches 1M GGR: Enhanced Due Diligence

- Recent* Police Conduct in the case the Company is owned by a single UBO;
- Recent* Utility Bill for each Director and shareholder/UBO;
- Certificate of Incumbency / Good Standing;
- Bank Reference Letter.

**Recent means that the documents cannot be older than 3 months.*

Contact Information

For any questions regarding this policy, please contact:

eMoore N.V.

Legalcompliance Department

Groot Kwartierweg 10, Livestrong Building Willemstad, Curaçao

Telephone: +599 9 7471401

Email: legalcompliance@the-emgroup.com