

Green Platform N.V.

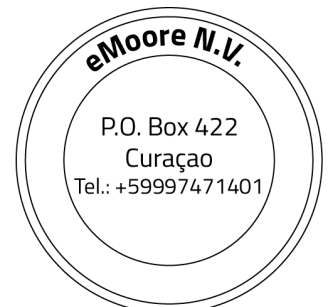
**POLICY FOR THE ANTI-MONEY LAUNDERING, COMBATING
THE FINANCING OF TERRORISM AND COUNTER-
PROLIFERATION FINANCING**

Version 1.2

2024



21/02/2024



eMoore N.V. as Director of Green Platform N.V., Executed by Lilianne Kroon as Proxy Holder

INTRODUCTION

Policy for the Anti-Money Laundering, Combating the Financing of Terrorism and Counter-Proliferation Financing (hereinafter - the Policy) of Green Platform N.V. (also hereinafter referred to as the “Company”) is developed based on requirements of the applicable normative acts of the Curacao, European Union, Financial Action Task Force (FATF) recommendations and on generally accepted standards of international practice.

This Policy describes in more detail the measures, actions and procedures that Green Platform N.V. must perform in accordance with the laws and the regulatory requirements of Curacao and the countries in which Green Platform N.V. operates (hereinafter referred to as the “Rules”) in order to detect and prevent attempts to launder money and finance terrorism. The Company implements the Policy through the creation of an effective system to prevent money laundering and terrorist financing.

The Company is obliged to implement, constantly update the Policy in accordance with the Rules and Recommendations and other provisions that regulate the system of prevention of money laundering and financing of terrorism. All employees and subdivisions of Green Platform N.V. are required to implement this Policy.

DEFINITIONS

Money laundering is the process by which proceeds from a criminal activity are disguised to conceal their illicit origin. Criminal activities, such as drug trafficking, smuggling, human trafficking, corruption and others, tend to generate large amounts of profits for the individuals or groups carrying out the criminal act. However, by using funds from such illicit sources, criminals risk drawing the authorities' attention to the underlying criminal activity and exposing themselves to criminal prosecution. In order to benefit freely from the proceeds of their crime, they must therefore conceal the illicit origin of these funds. Although it is not possible to measure money laundering in the same way as legitimate economic activity, the scale of the problem is considered to be enormous. Examples of such actions can be: conversion or transfer of property acquired from criminal activity, with aim to conceal or disguise its origin, or to assist a person committing criminal activity to evade the legal consequences of this person's actions, conceal or disguise real origin of a source, place, movement of a property or handling or modification of rights with respect to a property, knowing that such a property was acquired from criminal activity. acquisition, possession, use or disposal of property, being aware of its origin from criminal activity etc.

Terrorist financing involves the solicitation, collection or provision of funds with the intention that they may be used to support terrorist acts or organizations. Terrorist financing may not involve the proceeds of criminal conduct, but rather an attempt to conceal either the origin of the funds or their intended use, which could be for criminal purposes.

Legitimate sources of funds are a key difference between terrorist financiers and traditional criminal organizations. Although the motivation differs between traditional money launderers and terrorist financiers, the actual methods used to fund terrorist operations can be the same as or similar to methods used by other criminals to launder funds. Funding for terrorist attacks does not always require large sums of money and the associated transactions may not be complex.

Politically exposed person (PEP) - means natural persons who are or have been entrusted with prominent public functions and immediate family members, or persons known to be close associates, of such persons. Many PEPs hold positions that can be abused for the purpose of laundering illicit funds or other predicate offences such as corruption or bribery. Politically exposed person includes the following:

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

Family members includes the following:

- the spouse, or a person considered to be equivalent to a spouse, of a politically exposed person;
- the children and their spouses, or persons considered to be equivalent to a spouse, of a politically exposed person;
- the parents of a politically exposed person;

Persons known to be close associates' means:

- natural persons who are known to have joint beneficial ownership of legal entities or legal arrangements, or any other close business relations, with a politically exposed person;
- natural persons who have sole beneficial ownership of a legal entity or legal arrangement which is known to have been set up for the de facto benefit of a politically exposed person.

Ultimate Beneficial Owner - the natural person who is the owner of the Client - legal entity or who controls the Client or in whose behalf the business relationship is established or the any occasional transaction is carried out, and is at least:

- in the case of legal entity - a natural person who directly or indirectly holds more than 25 per cent of the capital shares of a legal entity or voting shares, or which is controlled directly or indirectly by him,
- in the case of legal establishments - a natural person who owns or has an interest in the formation or operation of a legal establishment, or who directly or indirectly carries out control over it, including the founder, authorized representative or manager.

1. Company Policy

1.1. This Policy of the Company is meant to prohibit and actively prevent money laundering and any activity that facilitates money laundering or the funding of terrorist or criminal activities (also hereinafter to as the “Policy”). The Company strives to comply with all applicable requirements under the legislations in force in the jurisdictions of the European Union members and other countries in which the Company operates, pursuant to the *Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing*¹ and the forthcoming Fourth Directive on Money laundering.

1.2. The Company is licensed and regulated by Curacao. The main business of the Company is to provide gaming services to its Clients (Operators), under the National Decree August 18, 1998 No. 14. Under the license conditions issued by Curaçao, the Company is required to have in place adequate measures to prevent its systems from being used for the purposes of money laundering, terrorist financing or any other criminal activity.

¹ Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing (Text with EEA relevance). Available: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32005L0060>

1.3. The Company is therefore obliged to follow the provisions contained in the Curaçao legal framework in particular the National Decree August 18, 1998 No. 14 and the legislations in force in any other jurisdiction in which the Company undertakes its activities.

2. Objective of the Policy

2.1. The Company is fully committed to be constantly vigilant to prevent money laundering and combat the financing of terrorism in order to minimize and manage risks such as reputational risk, legal risk and regulatory risk. It is also committed to its social duty to prevent serious crime and not to allow its systems to be abused in furtherance of these crimes.

2.2. The Company endeavor to keep itself updated with developments both at national and international level on any initiatives to prevent money laundering and the financing of terrorism. It commits itself to protect, at all times, the organization and its operations and safeguards its reputation and all from the threat of money laundering, the funding of terrorist and other criminal activities.

2.3. The Company's policies, procedures and internal controls are designed to ensure compliance with all applicable laws, rules, directives and regulations relevant to the Company's operations and will be reviewed and updated on a regular basis to ensure appropriate policies, procedures and internal controls are in place.

3. Regulatory Framework

3.1 Pursuant to the National Ordinance of Money Laundering (1993), money laundering is a criminal offence in Curaçao. Further main national regulations relating to money laundering and terrorist financing are amongst others:

a) The Code of Criminal Law (Penal Code) (N.G. 2011, no. 48);

b) The National Ordinance on the Reporting of Unusual Transactions (N.G. 1996, no. 21) as lastly amended by N.G. 2009, no. 65 (N.G. 2010, no. 41) (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. 2009, no. 66 (N.G. 2010, no. 40) (NOIS) together with all 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);

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;

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 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.

4. Client`s Due Diligence

4.1. Client`s due diligence is the processes used by the Company to collect and evaluate relevant information about a Client or potential client. It aims to uncover any potential risk to the Company of doing business with a Client or potential client by analyzing information from a variety of sources. These include:

- Clients themselves, who needs to provide certain information in order to do business with the Company;
- Sanctions lists published by governments or territories;
- Public data sources.

4.2. The overarching goal of the Client's Due Diligence is to obtain assurance that the funds involved in Client`s activity have not been obtained by criminal means, the purpose of Client`s activity is not related to money laundering attempts or Client`s activity will not be used to finance terrorism or proliferation.

4.3. In order to implement the overarching goal referred to in Clause 4.2., the main goal of the Client's Due Diligence is to determine the Client's risk in connection with the possibility of money laundering or terrorist or proliferation financing.

4.4. The Company will take reasonable steps:

1. to check Client`s corporate data, its business reputation using reliable, independent source documents, data or information;
2. to identify the ultimate beneficial owner of the Client, and take reasonable measures to verify the identity of the beneficial owner. This should include understanding the ownership and control structure of the Client;
3. to understand and, as appropriate, to obtain information on the purpose and intended nature of the business relationship;
4. to conduct ongoing due diligence on the business relationship and scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the Company`s Policy and KYC, business and risk profile, including, where necessary, the source of funds.

4.5. The Company will keep at all times a secure list of all its Clients and information and documents will be retained. Company is committed to ensuring that its business operates with the highest degree of integrity and in compliance with those that prohibit money laundering, terrorist financing, corruption, bribery and other criminal conduct.

4.6. For the purposes of the Due Diligence before entering business relation with Client, the following documents should be provided:

Information and copies of the documents certifying company's good standing:

- Certificate of incorporation;
- Memorandum and articles of incorporation;
- Good standing certificate (not older than 6 months);
- Valid license certificate (or evidence of applications pending, if a license is not issued yet);
- Copy of Operator`s AML/CFT policy;
- Copy of Operator`s anti-bribery, anti- fraud and anti-corruption policy.

Information and copies of the documents certifying legal ownership structure of the company, its

directors, officers and shareholders:

- Certified director registry;
- Certified shareholders register (certification not older than 6 months), if the respective information is not included in the good standing certificate;
- Structure chart certified by director (not older than 6 months).

Information and personal ID document copies of the UBO of the company:

- Identification document – copy of a certified (not older than 6 months) international identification document (e.g. passport);
- Proof of address – copy of a certified document not older than 6 months (e.g. utility bill).

Information and personal ID document copies of the Director of the company:

- Identification document – copy of a certified (not older than 6 months) international identification document (e.g. passport);
- Proof of address – copy of a certified document not older than 6 months (e.g. utility bill).

4.7. The identification documents are only accepted in high quality as a scan, photocopy or a photograph; all four corners of the document should be visible, and in case of ID cards – both sides should be provided.

The document should not be accepted in the following cases:

- When it is difficult to read the information in the identification documents due to poor quality;
- When it is difficult to see the photo of the identification document holder due to poor quality;
- When some information and/or part of the document is covered or for any other reason cannot be seen;
- When only a certain part of the identification document is received;
- When the identification document is received in other language than English and cannot be read.

The following documents are accepted as the proof of address:

- correspondence from a central or local government authority, department or agency;
- an official conduct certificate;
- any other government-issued document not mentioned above;
- a lease contract or agreement;
- Utility bill (gas/electricity/home internet) – not older than 3 months;

- a bank statement or a reference letter issued by a recognized credit institution or entity – not older than 3 months.

The document should not be accepted in the following cases:

- When the received document is older than 3 months;
- When it is difficult to read the information in the identification documents due to poor quality;
- When some information and/or part of the document is covered or for any other reason cannot be seen;
- When the document is received in other language than English and cannot be read;
- When the name on the proof of address does not match the name in the identification document.

In cases when the inappropriate or insufficient document is received – another copy and/or document should be received in order to complete the verification procedure.

4.8. If any significant information of a Client changes, verification documents will be requested.

4.9. If the beneficial owner is a politically exposed person, a relative or a person closely associated with the politically exposed person:

- must obtain permission from senior management to enter into or continue a business relationship;
- all risk-based procedures that identify the source of funds and material well-being of the Client must be documented.

4.10. Verification and Validation of Source of Funds

Source of Funds validation and verification should be conducted for ongoing monitoring purposes, as well as with respect to politically exposed persons (PEPs).

Enhanced due diligence and enhanced ongoing monitoring should be carried on when:

- a high risk of money laundering has been identified under the risk assessment or from information provided;
- Client is from a high-risk country, or operates on high-risk market;
- any other situation which can be assessed as presenting a higher risk of money laundering.

As part of the DD process, the source of wealth should be verified with evidence obtained from the Client and/or independent source until it is understandable where the Clients's and/or its UBO overall wealth has been derived from and (to the best of knowledge) that it's legitimate.

4.11. PEP (Politically Exposed Persons) and Sanctions Screening

All UBOs of Client, upon entering business relations, are screened against all sanctions list and existing PEP lists. Re-screening is also conducted on regular basis.

For PEPs, family members, close associate and entities in which their presence is founded, an enhanced due diligence must be conducted:

- have approval from senior management for establishing or continuing the business relationship with that person;
- where the business relationship is entered into, conduct enhanced ongoing monitoring of the business relationship with that Client.

4.12. Sanctions

Any potential matches are immediately reviewed and verified prior to onboarding if confirmed as false matches. If a true match is detected, the onboarding is rejected, and the relationship is exited. Further actions (such as reporting to the authorities) may be taken on case by case basis and if required. The Company complies with the following sanctions measures:

- The United Nations (UN) Security Council consolidated sanctions list;
- The EU's consolidated list of persons, groups and entities;
- The UK HM Treasury (HMT), Office of Financial Sanctions Implementation, "consolidated list of targets"
- The US Department of the Treasury, Office of Foreign Assets Control (OFAC) sanctions lists including the SDN list (Specially Designated Nationals and Blocked Persons List);
- Any local government issued list.

4.13. The Company shouldn't operate with the Clients to the following countries and territories, and Clients shouldn't accept End Users from the following countries and territories:

- Democratic People's Republic of Korea;
- Islamic Republic of Iran;
- Republic of the Union of Myanmar;

- Dutch Caribbean (Curacao, Bonaire, Aruba, Statia, St Maarten, Saba);
- Netherlands;
- France;
- USA.

5. RISK-BASED CUSTOMER DUE DILIGENCE AND RISK PROFILING

Risk of all the Clients shall be categorized into 3 different categories: High Risk, Medium Risk and Low Risk based on their risk profile considering certain indicative criteria to avoid money laundering and other compliance risk.

- I. Low Risk: Clients, their UBO`s and Director whose identities and sources of wealth can be easily identified and transaction maintained by such customer is done via bank account shall be categorized as "Low Risk".
- II. Medium Risk: Clients, their UBO`s and Director who are conducting normal nature of wealth but lack sufficient information and documents for categorizing under 'Low Risk' shall normally be categorized as medium risk. Besides, all Clients who do not fall under the category of either High Risk or Low Risk profile shall also be categorized as Medium risk.
- III. High Risk: Clients, their UBO`s and Director that are likely to pose a higher risk depending on their background, sources of funds etc. can be categorized as high risk. Also as High Risk Clients should be categorized Clients, who make payments using cryptocurrencies. Some of the indicative list of High Risk Clients are:
 - Clients having unusual amount of transactions, including transactions in Games.
 - Any related person who is suspected for directly or indirectly assisting terrorism, terrorist activities, terrorist organizations, organized crimes, illicit drugs and any other criminal activities. Normally the Company should not establish business relationship with such Clients.
 - Firms, companies, organizations, agencies or entities, established and being operated without Regulatory or supervisory Authority.
 - Clients, their UBO`s and Director who have been generally known through public media to be involved in Money Laundering and other financial crimes.

- Clients, their UBO`s and Director, who have been understood / heard to be involved in evading or misappropriating tax, customs, fees or any other revenue.
- Clients, their UBO`s and Director are residents of the country, which is classified as non-cooperative country by Financial Action Task Force (FATF).
- Clients, their UBO`s and Director are nationals of a country, which has not adopted necessary standards of AML/CFT.
- Clients, their UBO`s and Director are citizens of the country which is not serious on the matters of customer identification.
- Clients, their UBO`s and Director are citizens or institutions of a country on which the United Nations or any Inter Governmental International Organizations has imposed sanctions or warns.
- Clients or its Players whose transactions are suspicious on the basis of normal course of business.
- Clients, their UBO`s and Director are connected to the PEP.

6. TIPPING OFF

Company, its Directors, officers and employees should be protected from criminal and civil liability for breach of any restriction on disclosure of information imposed by contract or by any legislative, regulatory or administrative provision, if they report their suspicions in good faith to the Financial Intelligence Unit Cuacao (FIU), even if they did not know precisely what the underlying criminal activity was, and regardless of whether illegal activity actually occurred; and prohibited by law from disclosing (“tipping-off”) the fact that a suspicious transaction report or related information is being filed with the FIU. Tipping off a money launderer can include: changing the way the company handles the account informing other people not related to the investigation of the suspicions directly alerting them of a suspicion.

Suspicious matter reports are crucial in combatting money laundering, terrorism financing, and other serious crimes. It’s important that Company, its Directors, officers and employees don’t disclose any information about an SMR, or infer that Company, its Directors, officers and employees have submitted or will submit an SMR.

7. SUSPICIOUS TRANSACTIONS AND REPORTING

The responsible employee will report any suspicious Client or its transactions conducted or attempted by the Client where the responsible employee knows, suspects or has reason to suspect:

- a. The Client, its UBO`s and/or Director are included on any list of individuals assumed associated with terrorism or on a sanctions list;
- b. The Client, its UBO`s and/or Director is politically exposed person;
- c. The source of wealth of the Client, its UBO`s and/or Director transaction involves funds derived from illegal activity or is intended or conducted in order to hide or disguise funds or assets derived from illegal activity as part of a plan to violate or evade laws or regulations or to avoid any transaction reporting requirement under law or regulation;
- d. The transaction has no ordinary lawful purpose or is not the sort in which the Client or its Players would normally be expected to engage, and after examining the background, possible purpose of the transaction and other facts, we know of no reasonable explanation for the transaction; or
- e. The transaction involves the use of the Company to facilitate criminal activity.

Responsible employee should report unusual transactions that Company encounter delivering its designated services to the Financial Intelligence Unit of Curacao or FIU-Curacao. Financial Intelligence Unit of Curacao or FIU-Curacao, has been designated in the National Ordinance on Reporting of Unusual Transactions NORUT as the authority to which reporting entities must report on Suspicious matter reports.

The basis for that obligation and designation lies in the FATF recommendations to combat money laundering and terrorist financing. The FIU Curacao analyzes these reports and maps out transactions and money flows that can be associated with money laundering, their underlying predicate offenses as well as terrorist financing.

Responsible employee may report about suspicious or unusual transactions to the FIU of other countries, where its Client operates, or where it has its legal address or registered office.

8. DOCUMENTATION STORAGE

8.1. For at least five years after the termination of the business relationship, the Company keeps:

- all information obtained within the Due Diligence process;

- information on all payments made by the Clients;
- correspondence with the Clients on corporate and financial issues, including electronic correspondence.

8.2. At the end of the storage period, the Company destroys the Clients documents and other information about Client in its possession. The period of storage of Client's information begins after the termination of the business relationship.

9. Training Programs

9.1. The Company ensures that its employees are adequately trained and informed about the requirements set out in Company's AML/CTF and Sanctions policies and procedures. The Company also ensures that the daily duties of its employees are executed in accordance with Company's regulations and technical instructions specified in Company's AML/CTF and Sanctions procedures. An employee of the Company, who violates AML/CTF regulatory documents or acts illegally in the course of performance of his/her duties, shall be subject to disciplinary sanctions, as stipulated in Company's rules of internal order, and to the liability, as provided for in the regulatory enactments of the Curacao.

9.2. Employee AML/CTF and Sanctions training is comprised of two key elements:

9.2.1. Induction Training – the senior management is responsible for identifying relevant new staff that are required to undertake induction training within 45 days after commencement of employment relationship. The training is provided by the responsible employee or an external service provider and is a face to face training. The contents of the training include awareness training, covering ML/TF and Sanctions. Until a new member of staff has been signed off as competent, no direct client contact is allowed;

9.2.2. Refresh Training - all relevant staff must undertake a face to face refresher or online training at least an annual basis. The training is provided by the responsible employee or an external service provider, and assessment of staff understanding is carried out throughout the training.

The training includes also:

9.2.3. how to identify red flags and signs of money laundering that arise during the course of the employees' duties;

9.2.4. what to do once the risk is identified;

9.2.5. what employees' roles are in the Company's compliance efforts and how to perform them;

9.2.6. the Company's record retention policy; and

9.2.7. the disciplinary consequences for non-compliance with legislation.

9.3. The Company develop ongoing employee training under the leadership of the responsible employee or an external service provider and senior management. The training occurs on at least an annual basis. It based on the Company's size, its Client base, and its resources and be updated as necessary to reflect any new developments in the law.

10. STAFF DUE DILIGENCE

It is imperative that the Company's employees are of undisputed integrity. To ensure this objective, the Company follows a procedure whereby all applicants must produce a curriculum vitae, at least two references and relevant educational qualification certificates, and/or professional certificates, which are checked and verified by the Company's Human Resources Department.

Date: February 01, 2024