

AML and KYC Policy

Peak Interactive N.V.

April 2025

POLICY

Definitions

AML / Compliance Department – The unit which has primary responsibility for the initiation and delivery aspects of the AML program within Organization.

Business relationship – Business or commercial relationship between a Customer and the Organization and which is expected, at the time when the contact is established, to have an element of duration for a certain period (e.g. conclusion of an agreement between the Customer and the Organization, continuous performance of gambling/betting and monetary operations and transactions).

Close Associate – A natural person who, together with the Politically Exposed Person, is a member of the same legal entity or of a body without legal personality or maintains other business relationship.

Close family member – The spouse, the person with whom partnership has been registered (i.e. the cohabitant), parents, brothers, sisters, children and children's spouses, children's cohabitants.

Customer due diligence (CDD/KYC) – Identification of the Customer and verification the Customer's identity on the basis of documents, data or information obtained from a reliable and independent source; assessment and, as appropriate, obtainment of information on the purpose and intended nature of the Business Relationship; the conducting of ongoing monitoring of the Business Relationship including scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the Organizations' knowledge of the Customer.

Customer/Client/Player – a person that uses online gambling and betting services provided by the Organization.

FATF – The Financial Action Task Force.

FIU – Financial Investigation Unit Curacao.

High-risk third countries – countries identified as having strategic deficiencies in their AML/CFT regime, which pose a significant threat to the Union’s financial system (Article 9 of Directive (EU) 2015/849).

Identification – A part of Customer Due Diligence, allowing to ascertain the identity of a person on the basis of the personalized unique information directly related to that person.

Law – Law on the Prevention of Money Laundering and Terrorist Financing.

Money laundering (ML) – the doing of any act which constitutes an offence of money laundering and is defined in the Law on the Prevention of Money Laundering and Terrorist Financing of Curacao. The criminal acts cover all procedures that seek to change the identity of illegally obtained funds, arising from drug dealing, terrorist activities or any other crime in order to give impression that such money originated from legitimate or legal sources. Money laundering is the participation in any transaction that seeks to conceal or disguise the nature or origin of funds derived from illegal activities such as, for example, fraud, corruption, organized crime, or terrorism etc.

Organization/Company/Our – Peak Interactive N.V., an online gambling institution established and authorized under the laws of Curacao (Pending license number OGL/2024/860/0410) and, therefore, falling within the definition of an institution that falls under the Curacao legislation on the Prevention of Money Laundering and Terrorist Financing. The term “Company / Organization /Our” when used in these Policies also refers to the management bodies of the Organization and the members of such bodies as well as the employees of the Organization.

Policy – AML/CFT and Sanctions Compliance Policy.

Politically Exposed Person (PEP) – Natural persons who are or have been entrusted with Prominent Public Functions and Close Family Members or Close Associates of such persons.

Prominent Public Functions:

The head of the state, the head of the government, a minister, a vice minister or a deputy minister, a secretary of the state, a chancellor of the parliament, government or a ministry;

- A member of the parliament
- A member of the Supreme Court, the Constitutional Court or any other supreme judicial authorities whose decisions are not subject to appeal
- A mayor of the municipality, a head of the municipal administration
- A member of the management body of the supreme institution of state audit or control, or a chair, deputy chair or a member of the board of the central bank
- Ambassadors of foreign states, a charge d'affaires ad interim, commander of the armed forces and units, chief of defense staff or senior officer of foreign armed forces
- A member of the management or supervisory body of a public undertaking, a public limited company or a private limited company, whose shares or part of shares, carrying more than 1/2 of the total votes at the general meeting of shareholders of such companies, are owned by the state
- A member of the management or supervisory body of a municipal undertaking, a public limited company or a private limited company whose shares or part of shares, carrying more than 1/2 of the total votes at the general meeting of shareholders of such companies, that are owned by the state, and which are considered as large enterprises
- A director, a deputy director or a member of the management or supervisory body of an international intergovernmental Organization
- A leader, a deputy leader or a member of the management body of a political party

Source of funds – means the origin of the funds involved in a business relationship or occasional transaction. It includes both the activity that generated the funds used in the business relationship, for example the customer's salary, as well as the means through which the customer's funds were transferred.

Source of wealth – refers to funds that the customer has acquired during a prolonged period of time and that make up the customer's entire body of wealth (total funds). When determining the source of wealth, the focus is the acquisition of information on customer's activities that indicate how the customer acquired wealth.

Terrorist financing (TF) – the solicitation, collection or provision of funds with the intention that they may be used to support terrorist acts or organizations. Funds may stem from both legal and illicit sources. More precisely, according to the International Convention for the Suppression of the Financing of Terrorism, a person commits the crime of financing of terrorism "if that person by any means, directly or indirectly, unlawfully and willfully,

provides or collects funds with the intention that they should be used or in the knowledge that they are to be used, in full or in part, in order to carry out" an offense

General Statements

As per February 15, 2019, the Curaçao Gaming Control Board (GCB) was officially appointed the supervisory authority for AML/CFT compliance for the whole gaming sector. This appointment is retroactive until January 1, 2016.

The NOIS, the NORUT, the Sanction National Ordinance and the Kingdom Sanction Act contain provisions for service providers to prevent those entities for being used for money laundering, the financing of terrorism and the proliferation of weapons.

Different countries act together to combat money laundering and terrorist financing in the Financial Action Taskforce on money laundering (FATF). It was established by the G-7 Summit that was held in Paris in 1989. The Dutch Kingdom is member of the FATF, Curaçao is member of Caribbean Financial

The most important obligations for the gaming casino resulting from the AML/CFT laws refer to the conducting of Customer Due Diligence (CDD/KYC) and the reporting of unusual transactions. All this prevents the casino from being used by individuals for the laundering of their criminally acquired funds.

The Regulations for combating Money Laundering, the Financing of Terrorism and Proliferation of weapons of Mass Destruction (ML/FT/FP) are an integral part of the online gambling license requirements for the Curaçao jurisdiction. These Regulations are issued in implementation of article 2 paragraph 8 and article 11, paragraph 3, of the National Ordinance on Identification when rendering Services (NOIS) (N.G. 2017 no. 92) and; article 22mm, paragraph 3, of the National Ordinance on the Reporting Unusual Transactions

- (NORUT) (N.G. 2017 no.99);
- Kingdom Sanction Act (N.G. 2016, no. 54).
- Sanctions National Ordinance (N.G. 2014, no. 55);

With these Regulations, the GCB offers the casinos (Peak Interactive N.V.) a guideline to promote compliance with the laws and decrees with regard to money laundering, financing of terrorism and financing of proliferation and to implement sound internal policies and procedures to combat Money Laundering and the Financing of Terrorism. These include among others:

- The National Ordinance on Identification of Clients when Rendering Services (N.G. 2017, no. 92);
- The National Ordinance on the Reporting of Unusual Transactions (N.G. 2017, no. 99);
- Ministerial Decree with general operation of November 11, 2015, laying down the indicators as mentioned in article 10 of the National Ordinance on the Reporting of Unusual Transactions
- (Regulation Indicators Unusual Transactions) (N.G. 2015, no. 73); 5
- 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);
- National decree for general measures, of the 10th of July 2015, for the implementation of article Council Resolutions concerning Al-Qaeda c.s., the Taliban of Afghanistan c.s., ISIL c.s. ANF c.s. and persons and organizations to be designated locally (N.G. 2015, no. 29);
- National Decree for general measures, of the 10th of July 2015, for the implementation of article 2 of the Sanctions National Decree containing implementation of the
- Council resolutions concerning Libya (Sanctions Ordinance Libya) (N.G. 2015 no. 28);
- National Decree for general measures, of the 10th of July 2015, for the implementation of article 2 of the Sanctions National Ordinance, containing implementation of Resolutions 1695 (2006),
- 1718 (2006), 2087 (2013) and 2094 (2013) of the United Nations Security Council (Sanctions National Ordinance extension of validity sanction decrees 2018 (N.G. 2018, no. 34); The Code of Criminal Law (Penal Code) (N.G. 2011, no. 48).

These laws and regulations and any additional regulations issued pursuant to the NOIS, NORUT, the Sanction National Ordinance and the Kingdom Sanction Law form the main legal basis for the Curaçao Gaming Sector to combat money laundering, the financing of terrorism and the proliferation of weapons. As indicated, these Regulations for the combating of Money Laundering, the Financing of Terrorism and Proliferation of weapons of mass destruction (Regulations) are applicable to Curaçao casinos (land-based and online) offering games of chance and other online games.

These regulations are effective as of January 9, 2025. All online casinos are bound to comply with these Regulations as of April 2025.

1. SCOPE OF THE POLICY

As part of the commitment to maintaining the highest standards and following all relevant regulations, it is Peak Interactive N.V. policy to prohibit and prevent any cases of money laundering and terrorist financing.

Whereas Peak Interactive N.V. is an online betting and gambling provider registered under the laws of Curacao with registration number 10847 and its license number OGL/2024/860/0410

Money Laundering is the participation in any transaction that seeks to conceal or disguise the nature, or the origin of funds derived from illegal activities. Money laundering involves not only the proceeds of drugs trafficking, but funds related to other illegal activities, including fraud, corruption, organized crime, terrorism, and many other crimes. Generally, money laundering consists of three stages:

Placement: introduction of cash originating from illegal / criminal activities into financial or non-financial institutions.

Layering: separating the proceeds of criminal activities from their source through the use of layers of complex financial transactions. These layers are designed to hamper the audit trail, disguise the origin of funds and provide anonymity.

Integration: placing the laundered proceeds back into the economy in such a way that they re-enter the financial system as legitimate funds.

Terrorist Financing (TF) encompasses the means and methods used by terrorist organizations to finance their activities. This money can come from legitimate sources, for example from profits from businesses and charitable organizations. But terrorist groups can also get their financing from illegal activities such as trafficking in weapons, drugs or people, or kidnapping for ransom.

This Policy is updated yearly (or as warranted before) by the Anti-Money Laundering (AML) Officer of the Organization based on the general principles set up by the Board of Directors of the Organization and in cooperation with the GCB of Curacao in relation to the prevention of money laundering and terrorist financing.

The Policy applies to all employees of the Organization and the responsibilities of the staff members as well as to ensure compliance with the following legislation:

European Directive 2005/60/EC and European Directive 2018/843 on the prevention of the use of the Financial System for the purpose of money laundering and terrorist financing as transposed into National Law (L188(I)/2007-2018 the National Ordinance on identification when rendering services (Landsverordening identificatie bij dienstverlening (LID), PB 2017, no. 92) the National Ordinance on the reporting of unusual transactions (Landsverordening melding ongebruikelijke transacties (LMOT), PB 2017, no. 99).

All amendments and/or changes to the current version of the Policy must be approved by the Company's Board of Directors.

1.1 RECIPIENTS OF THE DOCUMENT:

Recipients of the Document:

- Gaming department
- Customer support department
- Fraud Prevention department
- Payments department
- AML department
- Board of Directors

2. BOARD OF DIRECTORS

The Board of Directors is responsible for ensuring that the Organization complies with its obligations under the Law. The Board shall assess and periodically review the effectiveness of the policies, arrangements and procedures put in place to comply with the obligations under the Law, and to take appropriate measures to address any deficiencies.

The main duties and responsibilities of the Board of Directors in relation to the prevention of money laundering and terrorist financing mainly include:

- Determining, recording and approving the general policy principles of the Organization in relation to the prevention of money laundering and terrorist financing and inform the Anti-Money Laundering Officer accordingly
- Appointment of an Anti-Money Laundering Officer
- Approval of the AML policy and procedures
- Communication of the AML policy to all employees of the Organization

- Ensuring that the Anti-Money Laundering Officer has full access to all documents and information necessary for the execution of his/her duties and responsibilities
- Ensuring that the requirements of the Law and the AML Directive are applied, and that the Organization maintains appropriate, effective and sufficient systems and controls for the prevention of money laundering and terrorist financing
- Ensuring that all employees of the Organization know the Anti-Money Laundering Officer and report to him/her all suspicious transactions in accordance with the requirements of the AML Laws and the Directive
- Establishing reporting chain of suspicious transaction to the Anti-Money Laundering Officer
- Ensuring that the Anti-Money Laundering Officer has sufficient resources for the effective execution of his/her duties and responsibilities
- Assessing and approving the Annual Report
- Reviewing the report submitted to the Board by the Anti-Money Laundering Officer

3. INTERNAL COMPLIANCE CONTROLS

The Organization has assigned an AML Officer to test current practices and provide suggestions for improvements. The Audit is performed at least on an annual basis.

Any findings are submitted to the Board of Directors which decides the necessary measures that need to be taken to ensure compliance.

4. ROLE AND RESPONSIBILITIES OF AML OFFICER

The AML Officer has the necessary authority, resources and expertise to carry out his/her relevant duties and responsibilities and also has access to all relevant information. The employees of the Organization are informed of the person carrying out AML role and on ways of contacting him/her. Per regulations, one (1) employee shall be assigned the role of AML Officer.

In case of any changes in the structure of AML Department – this will be communicated to the Gaming Control Board accordingly.

4.1 Responsibilities of AML Officer:

- To monitor and evaluate the sound and effective implementation of the Organizations general policy principals and to manage the associated risks in relation to the Prevention of Money Laundering and Terrorist Financing

- Ensure that KYC and EDD procedures are followed
- Ensure Sanctions Compliance procedures are followed
- Advise employees on implementation of anti-money laundering program within the Organization
- Provide necessary materials and training on AML/CFT and Sanctions Compliance to the employees of the Organization
- Report to Management, and if necessary, the Board of Directors any cases of non-compliance with laws, regulations and directives issued by Curacao Gaming Control Board
- Recommend to the Board of Directors any amendments necessary to the AML Policy
- Receive and evaluate information from all personnel regarding suspicious client transactions and activities - If considered necessary; to report such transactions and activities to FIU Curaçao
- Ensure the preparation, maintenance and updating of lists of client categorization following a risk-based approach
- Screen existing clients and transactions to ensure that the AML policies are followed and verify whether any are subject to reporting
- On an annual basis, review the risks arising from existing and new clients, new financial instruments and services
- Review all internally reported unusual transactions for their completeness and accuracy
- Keep records of internally and externally reported unusual transactions
- Execute closer investigation of unusual transactions if necessary
- Report to Senior Management, at least annually, on compliance issues or improvements
- Prepare the Annual AML Report and submit it to the Board of Directors
- Verify adherence to local laws and regulations regarding the detection and deterrence of money laundering and terrorist financing
- Offer training sessions for the staff on various compliance-related issues
- Prepare the external report of unusual transactions
- Be informed of developments on money laundering and terrorist financing and to make suggestions to management for improvements; and
- Provide updates on the casino's efforts against money laundering and financing of terrorism and financing of proliferation.

5. AML ANNUAL REPORT

The AML Annual Report will be prepared and submitted for approval to the Board of Directors within two (2) months from the end of each calendar year and made available to the Curacao Gaming Control Board (if requested) along with all meeting notes during the approval process.

5.1 The Annual Report should deal with money laundering and terrorist financing preventive issues pertaining to the year under review and should cover the following if applicable:

- Measures taken and/or procedures introduced for compliance with any amendments and/or new provisions of the Law and the AML Directive which took place during the year under review
- Information on the inspections and reviews performed by the AML Compliance Officer
- The number suspicion reports submitted by employees to the AML Compliance Officer.
- The number of reports submitted by the AML Compliance Officer to FIU Curacao, with information/details on the main reasons for suspicion and highlights of any particular trends
- Information on the policy, measures, practices, procedures and controls applied by the Organization in relation to high-risk clients as well as the number and country of origin of high-risk clients with whom a business relationship is established.
- Information on the procedures applied by the Organization for the ongoing monitoring of client accounts and transactions
- Information on the training courses/seminars attended by the AML Compliance Officer and any other educational material received
- Information on training/education and any educational material provided to staff during the year
- Assessment of the effectiveness of staff training and recommendations for next year's training program.
- Information on the structure and staffing of the department of the Compliance Officer as well as recommendations and timeframe for their implementation, for any additional staff and technical resources which may be needed for reinforcing the measures and procedures against money laundering and terrorist financing.

The Organization will make the following items readily available at GCB request:

- Its written and approved AML Compliance Program on money laundering, terrorist financing and financing of proliferation
- Records of its Business Risk assessment
- The name of each Compliance Officer responsible for the casino's overall money laundering and terrorist financing policies and procedures and his/her designated job description
- Records of reported unusual transactions
- Records of unusual transactions which required closer investigations
- Records of frozen accounts; (AML related/ applicable)
- Schedule of the training provided to the casino's personnel regarding money laundering, terrorist financing and proliferation of weapons
- The assessment report on the casino's policies and procedures on money laundering, terrorist financing and financing of proliferation by the internal audit department or an external auditor
- The customer's files including customer risk assessment, CDD, customer acceptance and transaction information.

6. MANDATORY RISK PROCEDURES AND THE RISK-BASED APPROACH

General Overview

As regulation needs and risks continually change, the Company and AML Officer shall monitor and evaluate the procedures of the *adopted* Risk-Based Approach on an ongoing basis.

The principal Risk-Based Approach of the Company is that AML resources should be directed proportionately in accordance with the extent of the ML/FT risks posed, so that the Players posing the highest risks receive the highest attention meeting regulatory needs while effectively combating ML/FT. The application of a Risk-Based Approach should ensure that measures to prevent or mitigate ML/FT are proportionate with the risks identified and that resources are allocated in the most efficient ways.

The Policy sets the framework for the Company's Risk-Based Approach. Risk factors that must be taken into account, relating to:

- Client Category (Risk Level)
- Jurisdiction
- Product (Casino/Sports)
- Transaction Types
- Playing Channels

6.1 ADOPTED RISK-BASED APPROACH

The *adopted* Risk-Based Approach that is pursued by the Company, and described in the Policy, was developed by the following methodology:

- Allowing the Company to apply its own approach in the formulation of policies, procedures and controls in response to the Company's individual circumstances
- Provide the Company with reasonable control policies that match the risk of our particular customer profiles and financial transactions
- Recognizing that AML issues vary across game types, players, countries and types of financial transactions
- Recognizing the opportunity of ML/TF occurring through online gaming and betting transactions and understanding its role in following the Law and GCB's regulations and guidance

The Risk-Based Approach adopted by the Company involves specific measures, indicators, and procedures in assessing the most appropriate way to identify and manage the AML risks faced by the Organization. Such measures include:

- Identifying and assessing the ML/TF risks deriving from player profiles that are not standard along with transactions that appear to be out of place of a player of the same profile type.
- Mitigating the assessed risks by the application of appropriate and effective measures, procedures and controls
- Continuous monitoring and improvements in the effective operation of the policies, procedures and controls

Execution of appropriate actions, controls and measures because of different “check off” indicators. Such MACRO indicators include the following:

- Location of player and transaction(s)
- Player profile overall
- Volume and size of deposit and withdrawal transactions and frequency thereof
- Location origin and destination of player funds (must be the same)
- Notable deviations from typical/expected deposit/transaction volumes of player profile type or individual player
- Recording the action(s) taken so the Company shall be, at all times, in a position to demonstrate to the Gaming Control Board that the extent of AML measures and control procedures it applies are proportionate to the risk it faces while providing online gaming and betting services.

6.2 IDENTIFIED RISKS

The Risk-Based Approach adopted by the Company involves the identification, recording and evaluation of the risks that should be managed. Generally established and known in the gaming industry, players display similar characteristics and (NON-AML risks) patterns overall which are routinely recognizable. Therefore, the Company is positioned on a MICRO-LEVEL to act upon transactions and activities that fall outside what is commonly “normal and standard” expectations.

The following are sources of risks which the Organization faces with respect to ML/TF and respective risk categories the Organization shall take into consideration when adopting a Risk-Based Approach and building Client AML risk categorization:

- Players engaged in transactions which involve significant amounts of money
- Players originating from high-risk countries or countries known for high level of corruption, terrorist activities, human trafficking, organized crime or drug trafficking
- Players reluctant/refusing to provide accurate information or KYC documents
- Players using VPN or Proxy servers to hide their IP addresses
- Players removing/hiding their computer or Mobile operating system details
- Players using different devices to access the website of the Organization

- Amount, origin and destination of funds for deposits and withdrawals (must be the same)
- Deposit and withdrawal methods used, number of cards, number of methods
- Games played, betting volumes, time of play, style of play
- Suspected or direct associated account profiles and transactions
- Account opening dates and location
- Source of advertising
- Inactive Player profiles with random logins with high volume transactions in short login times
- Odd deposit and withdrawal amounts
- PEPs

6.3 TYPES OF PLAYERS REGARDING THEIR RISK PROFILE

The adopted approach is based on the above sources of risk should be performed at the inception of a Business Relationship with a Player. However, a comprehensive risk profile may only become evident once the Player has begun transacting through an account, played and completed KYC procedures when applicable.

Taking into consideration the above and the fact that the Company offers services on a non-face-to-face basis, following the performance of the risk review, the Company shall label the type of Client and the risk profile (High risk, Medium risk, Low risk) according to the following different risk variables and indicators:

High ML/TF Risk

- PEPs (Account to sanctioned)
- Players from countries that are selectively sanctioned
- Resident or origin in/from non-reputable jurisdiction according to the FATF list as amended from time to time
High deposits, low play volumes/time
- High deposits whereas betting ratios do not match deposit amount
- Unverified Player
- Any of the above-mentioned indicators, or, any other indicator not listed, will automatically classify the account as High Risk

Medium ML/TF Risk

- Not yet verified Player, but no illicit indicators
- Medium to high deposits
- Client that does not fall under any of the categories of High Risk or Low Risk
- Any other Client determined by the Company itself to be classified as such

Low ML/TF Risk

- Verified Player
- Resident and origin of an EEA jurisdiction
- Very low deposits
- The country of origin and/or destination of Players' funds are both EEA jurisdiction
- Player using only debit/credit card or wire transfer
- Players identified Face-To-Face or via video conferencing
- Any Client who does not fall under the 'Medium Risk' or 'High Risk' categories

The monitoring of all Players' accounts and reviewing transactions shall be based on the level of risk and, as a minimum, shall achieve the ability to identify all high risk Players.

6.4 DYNAMIC RISK MANAGEMENT AND MONITORING

Risk assessment and management is not an isolated event for a limited duration but rather a continuous process, carried out on a dynamic basis. Players' activities change, the same happens to the transactions used for money laundering or terrorist financing.

In this respect, the Company shall endeavor to undertake regular reviews of the characteristics of existing Players, new Players, and the measures, procedures and controls designed to mitigate such risks. These reviews shall be documented, as applicable, and form part of the Annual Money Laundering Report.

For the development and implementation of appropriate measures and procedures on a Risk-Based Approach, and for the implementation of the CDD, the overall operational departments of the Company shall consult data, information and reports e.g. Players with origin or residence in countries which inadequately apply FATF, and country assessment reports that are published in following relevant international listings:

- FATF
- The Council of Europe Select Committee of Experts on the Evaluation of Anti-Money Laundering Measures
- The EU Common Foreign & Security Policy (CFSP)
- The UN Security Council Sanctions Committees
- The International Money Laundering Information Network (IMOLIN)
- The International Monetary Fund (IMF)
- Office of Foreign Assets Control
- Due to the nature of business of the Organization, additional countries must be banned from the use of the services due to local and foreign gambling and betting regulations.

Additionally, the Company has implemented controls that monitor player activity and actions, that are unique to online gambling and are also a part of the fraud-prevention system, such as:

- VPN and Proxy Servers
- Different devices to access services
- Frequency of deposits
- Payment methods used and number
- Use cards that did not pass 3D secure verification
- Attempts to use cards with insufficient funds
- Number of bank cards
- Attempt to withdraw funds through a payment method that has not been previously used
- Bet to deposit ratio
- Bet to current balance ratio

Such triggers may influence the overall risk assessment of the Player, as well as may lead to a submission of suspicious activity report or account termination

7. SANCTIONS COMPLIANCE POLICY

The purpose of the Sanctions Compliance Policy is to set the standards of Peak Interactive N.V. for the management and prevention of sanctions breaches and to establish an internal control framework that mitigates the risks associated with sanctions violations. This is being done to avoid regulatory action and possible sanctions upon the Company.

7.1 Sanctions and Embargoes

Sanctions and embargoes are political trade restrictions put in place against target countries with the aim of maintaining or restoring international peace and security. Such actions are executed by OFAC (US), EU and the UN. Sanctions and Embargoes span from countries, companies, individual persons, companies, products, raw materials, arms and/or groups/factions.

It is the policy of the Company to make its *best knowledgeable effort* not to provide service to a sanctioned country or person. The Organization shall carry out and document a sanctions risk assessment appropriate to the type of its activities to identify, measure, understand and manage sanctions risk the Organization is exposed to.

The Organization shall carry out a sanctions risk assessment in relation to all sanctions and the sanctions risk assessment upon knowledge of a sanction and consider the following:

- Player transactions are related to a territory or border area of a territory or state that is a subject of sanctions.
- Player employed by (or suspected) or involved in arms sales, services or manufacturing
- Player's economic or personal activities do not meet their declared economic or personal activities
- Player documents supporting transactions submitted by the customer contain indications of fraud, providing evidence of possible evasion of sanctions

7.2 KYC measures to support compliance of sanctions

The Organization has implemented relevant KYC and due diligence procedures that make its best effort upon onboarding and throughout the business relationship, the relevant parties are being screened against sanction lists offered through the media, publicly issued lists or third-party services. In the event of a match, actions will be taken to determine the risk.

7.3 CDD for Sanctions compliance

The Organization has implemented relevant procedures and processes that ensure that transaction parties (meaning, that the screening is performed not only against the Customer, but also against the payments institution) are being automatically screened against sanction lists. In the event of a match, an alert will be generated for further investigation by the Company.

7.4 Third Party Automation Sanction Screening

Peak Interactive N.V. has employed third-party IT-based solutions to assist in the screening obligations. All the Company customers' key data (such as name, surname, and address) is automatically exported and matched with the sanction's lists. These checks are performed on a daily basis. The third-party external service provider is responsible for the actuality of sanctions lists. If during the matching procedure a customer is marked as a potentially Restricted Party, this is defined as a match.

Where required by applicable law, the Organization will freeze assets in accounts of parties subject to specific sanctions or where the freezing is otherwise indicated.

8. Player Acceptance Policy

The criterion for accepting new Players also defines the criteria which shall be as follows:

The Organization shall classify Players into three (3) various risk categories and based on the Risk-Based Approach described above. The Organization shall accept Players who are categorized as Low and Medium Risk Players as long as the Client passed a standard CDD profile and as long the general principles under the current Policies are followed. Players deemed High Risk will be evaluated as to the severity of such risk and appropriate actions will be taken to secure, close and/or report the account to the GCB.

8.1 – Non-Accepted Player Accounts

The following list of Player profiles shall not be acceptable for establishing a Business Relationship with the Organization:

- It is prohibited for Players to open or maintain anonymous or numbered accounts or accounts in names other than those stated in the Players official identity documents.
- Players who fail or refuse to submit the required data and information for the verification of their identity, without adequate justification
- Players that purposefully alter their KYC or identity documents
- Players that submit fraudulent documents
- Players who ask to open or maintain anonymous or numbered accounts or accounts in names other than the client's name stated in official identity documents
- Players who ask to transfer their initial deposit in cash
- Sanctioned country

- “Bad Data” profiles as reported by the gaming system database or third-party information
- On the list of people involved in terrorist financing or known to be involved in activity connected to money-laundering
- Sanctioned individuals
- Players opening multiple accounts, using multiple payment methods and bank cards

9. Player CDD/KYC processes and documentation

The Company shall duly apply Client identification procedures and CDD measures in the following cases:

- Upon first withdrawal request
- When establishing a Business Relationship with high initial volumes or number of transactions regardless of amounts
- When there is a suspicion of ML/TF, regardless of the amount of the transaction
- When there are doubts about the veracity or adequacy of customer profile data
- When there are significant amounts deposited in the Players account
- When players engage in financial transactions equal to or above Naf. 4,000; (approx. \$2500 USD)
- In case the casino carries out an occasional transaction above the monetary equivalent of NAF. 4,000, it is still obliged to apply CDD measures. Casinos are also subject to this obligation when they execute a series of linked transactions which, though individually below the applicable threshold, would cumulatively meet or exceed the NAF. 4,000 thresholds.
- Any other event when the Company finds appropriate

The Customer Support Department shall collect and file the relevant Client identification documents, according to the record keeping procedures described in the Policy. Further, the Company shall be responsible for always maintaining the documents received per the requirements of the Law and the Directive.

In cases whereby the Organization (or Player) cannot reasonably comply with customer due diligence requirements, it will not establish a business relationship and if appropriate, report the case to the FIU Curacao.

9.1 Player Account Identification

The initial identification of the Player is performed through the review of the initial registration of the players' account. The registration system collects the following information:

- Account number (generated automatically or player selected)
- IP address
- Computer or Mobile Operating Information
- Password
- Registration Date (generated automatically)
- Phone number (must be valid)
- Email Address (must be valid)
- First Name
- Surname
- Date of Birth
- Country
- Permanent Registered Address
- Nationality
- Occupation

9.2 Verification Documents

The following are standard documents that are required and/or additionally requested

- Valid color photo or scan of government issued Passport, Drivers License or Identification Card
- Front and back photocopies of bank card(s) used to transact
- Copy of bank (or e-wallet) statement showing Player name, address, and transaction(s) conducted at the casino with dates
- Copy of utility bill not older than three (3) months displaying customers registered address. Phone, water, rent lease, power, bank statement, tax bill etc.
- Photo of Player holding documents submitted (if applicable)
- Specimen signature to compare (if applicable)

When verifying the identity of the Player, the responsible employee must review the documents provided for verification of the customer to ensure that no fraud signs have been noticed and further ensure that document provided for identity verification is valid and contains the persons photograph.

The Responsible employee must make every reasonable attempt to conclude the data, documents, and information received from the Customer during the CDD is reliable and sound.

In addition, further to the information to be provided by the person him/herself, a search should be made through the dedicated software, social media and on the internet in order to obtain information on private and public positions which the prospective customer holds or held for at least the last twelve months or previously as well as whether he/she is an immediate family member or a close associate of such individual, in order to verify if the customer is a PEP.

For high volume Players, a general search of their listed residence and estimated value of such residence is prudent.

10. High Risk KYC procedures

The Company is required to take additional and enhanced measures in cases which by their nature, present a high-risk of money laundering and terrorist financing.

Apart from the Players accounts that have been classified by the Organization as High-Risk, through its' risk assessment, the Laws and Directives additionally specify the below categories of customers which should be classified as high-risk and where enhanced due diligence measures should be applied:

The minimum enhanced due diligence measures that should be applied for all High-Risk customers of the Organization are:

- Perform review and update of the customer at least once a year or at a shorter interval if necessary
- Taking more enhanced measures and supporting documentation to establish and verify the source of wealth
- Perform systematic and thorough monitoring of the transactions

In addition, as stated above, more aggressive actions further to the information to be provided by the person him/herself, a search should be made through the dedicated software, social media and on the internet in order to obtain information on private and public employment positions which the prospective customer holds or held for at least the last twelve months or previously as well as whether he/she is an immediate family member or a close associate of such individual, in order to verify if the customer is a PEP.

For high volume Players, a general search of their listed residence and estimated value of such residence is prudent.

10.1 Customers having complex or unusually large transactions or unusual type of transactions

While generally rare, the Company is required to examine, as far as reasonably possible, the background and purpose of all complex and unusually large transactions and all unusual types of transactions carried out without the apparent or legitimate purpose.

In order to further assess and determine whether such transactions or activities appear suspicious or not, the Organization should classify the customer(s), engaging in such complex or unusually large or unusual transactions, as high-risk, in order to intensify the extent and nature of the monitoring of the business relationship.

Examples of complex or unusually large or unusual types of transactions include transactions that:

- Are not in line with those expected on the basis of the Organization's knowledge of the customer and the business relationship or the category to which the customer belongs
- Constitute an unusual or unexpected type of transaction compared to the normal activity of the customer or the type of transactions associated with similar customers products or services, or
- Are particularly complex compared to other similar transactions related to similar items, products or customer services.

When the Organization detects complex or unusually large or unusual types of transactions, measures to understand the background and purpose of these transactions, by locating the source of the funds (by obtaining Bank statements, or other documents that may provide relevant information) or by obtaining more information about the customer in order to determine the plausibility of such transactions.

The set of enhanced due diligence measures to be applied for each customer will depend on the circumstances of each individual case and the characteristics that rendered the transaction complex or unusual.

10.2 Politically exposed persons (PEPS)

In the case of individual customers, where the Player falls under the definition of a PEP, then the account should be classified a High-Risk – PEP.

The establishment of a business relationship with Politically Exposed Persons may expose the Organization to increased risks, and it is considered one of the most important money laundering issues worldwide. As such, if a PEP (or an associate or a family member thereof) is determined, the Company shall not continue to offer services unless extensive CDD/KYC are conducted and the circumstances of position, reputation, source of funds and “power of position” are well established and documented. Thereafter, a clear recommendation to the Board of Directors for the continuation of the relationship or closure shall be made.

Adequate enhanced due diligence measures should be followed in order to establish the source of wealth and source of funds of the PEP that is involved in the business relationship in order to ensure that there are no funds originating from corruption or other criminal activity involved.

Business relationships with PEPs should be subject to enhanced and on-going monitoring. The Organization should perform on-going monitoring on both the transactions and the risk profile of the customer.

It is provided that when a PEP (or an associate or a family member) has ceased to have a prominent public function, the Company will consider the business relationship as High-Risk, for a period of at least 12 additional months.

All above information/documentation should be placed in the customer’s file as evidence and a report be readily available for GCB to include any and all data requested.

10.3 High Risk Countries

The Law defines as a High-Risk third country, a country indicated by the European Commission, US, UN, or FATF countries that bear deficiencies in their system of money laundering and terrorist financing which presents strategic deficiencies in its national system for combating money laundering and terrorist financing which are considered as major threats to the financial system of the EU.

Generally, the Company does not offer services in high-risk countries. The Company, however, may accept customers that are nationals of High-Risk countries, but reside elsewhere. For such customers and transactions, it is important to apply the enhanced due diligence measures, especially regarding the establishment of the source of wealth, as per the provisions of the present Policy and the Organization's Risk Assessment Policy.

It is the AML Compliance Department's responsibility to maintain and update the list of High-Risk countries, resulting from the Methodology and to communicate it to the Board of Directors and any other responsible employees when updated and amended.

10.4 Searching Information

Internet / media searches should always be performed on new players and upon the review (either regular or ad hoc) of identification records or annual account review, for all Players and their relevant persons.

The internet search serves the purpose of identifying adverse media, obtaining as much information as possible in constructing the customer's profile, identifying whether the customer is a PEP or immediate family member or close associate of a PEP as well as of cross-checking the information provided by the customer.

In evidencing the search, the employee preparing the customer's file should note the "Internet search has been made" along with any pertinent information of reasonable value to determine High Risk cases.

11. On-going Monitoring

The constant monitoring of the Players' accounts and transactions is an imperative element in the effective controlling of the risk of AML.

In this respect, the Company shall be responsible for maintaining as well as developing the on-going monitoring process of the Organization and use the appropriate IT systems in order to achieve highest monitoring abilities while keeping a cost-effective process and refresh at least annually.

The procedures and intensity of monitoring Players' accounts and examining transactions on the Client's level of risk shall include the identification transactions which, as of their nature, may be associated with ML/TF, unusual or suspicious transactions that are inconsistent with the profile of the Client for the purposes of further investigation.

Minimum trigger that would require an ongoing monitoring include, but is not limited to:

- Cumulative deposits equal or over 4000 NAf. in month
- Sudden increase in deposits
- High loss amount
- Deposits coming from different payment systems
- Request for withdrawals through an alternative payment system, different from the deposit method

It should be noted that these triggers are only samples of possible scenarios.

The Organization maintains relevant controls to track Players deposits and withdrawals, as well as have all the required technical requirements to review Players' transaction activity starting from the account opening. The data can be segregated in periods or types of transactions.

12. Updating CDD/KYC

It is a requirement that the customer's identification records should be examined on a regular basis so that it is ensured that they remain completely updated. In this respect, the procedures described below should be followed.

The frequency of review and updating depends on the risk categorization of each customer and should be as follows:

- Low risk customers: Not less frequently than once every 3 years,
- Normal risk customers: Not less frequently than once every 1 year,
- High risk customers: Not less frequently than every 6 months.

During the review procedure, the customer should be requested to confirm that the identification information held by the Organization is still accurate and valid or advise changes that have taken place. In cases that any change has taken place, the customer should be asked to present the relative supporting documentation / evidence.

The employee responsible is required to send the letter with the requirements for the update of information and records, reminders and the warning letter where needed and follow-up completion of the review procedure.

Completion of the review procedure should be approved by an approved employee in the same way as for the establishment of a business relationship.

The continuation of the business relationship with High-Risk customers should be approved by the AML Department and in some cases, by the Board of Directors (e.g. PEPs).

13. Termination of Business Relationship

The Organization should proceed with the termination of the relationship with an existing customer who:

- Had such changes in its status after the establishment of the relationship which turned it to be one of the prohibited types of customers as per the Customer Acceptance Policy
- Has a behavior in its transactions and activities which makes it a customer of excessive high-risk
- Refuses or fails to provide updated information requested by the Organization,
- Has attempted to deceive the Organization
- Breached any of the provisions of the Organization's Terms and Conditions that the Organization deems of significance
- Has been convicted for any serious predicate offence, for which a Court Order or enquiry from an authority (e.g. FIU Curacao, Curacao Gaming Control Board) has been received and by maintaining the relationship may expose the Organization to high AML or reputational risk

Before proceeding with the termination of a business relationship, the Organization should make sure that the files of the customer are KYC compliant and that the records are up to date. In this respect:

When a customer requests to proceed with the termination, or where the Organization wishes to proceed with the termination of the business relationship with a customer, the Organization should be satisfied that the data and profile information of the customer are up to date. If not, the Organization should carry out any necessary actions – depending on the case – to ensure that the customer’s status and records become updated, and that there are no concerns obstructing the Organization from proceeding with the termination.

The Organization shall not immediately proceed with the termination in cases where a customer’s review and updating of records has not been completed. When review (either annual or ad-hoc) and updating of records is requested by the Organization, and the customer does not provide all the necessary information for its completion this should constitute a ground of suspicion and it should be considered, whether it requires reporting to the FIU Curacao. Such cases should be treated, depending on the individual circumstances of each case. For example, if the Organization can establish and be satisfied that, based on the circumstances and the customer’s behaviour/attitude, not providing the required documentation does not raise any suspicions, then the Organization may proceed with the termination. Evidence of such justification should be placed in the customers’ file.

14. REPORTING SUSPICIOUS TRANSACTIONS

Whenever there is an attempt of executing transactions that raise reasonable suspicion of being related to ML/TF, the AML Officer, reports the case to the FIU Curacao through the dedicated GoAML Portal in accordance with the current Policy.

14.1 SUSPICIOUS TRANSACTIONS

The definition of a suspicious transaction as well as the types of transactions indicating ML/TF is very broad. A suspicious transaction will often be inconsistent with the normal Business Relationship patterns of the specific account. The Company shall ensure that it maintains adequate information and knows enough about its Players’ activities in order to recognize on time that a transaction or a series of transactions is unusual or suspicious.

Examples of what might constitute suspicious transactions/activities related to ML/TF are listed in Appendix 1 of the Policy. The relevant list is not exhaustive, nor it includes all types of transactions that may be used. Nevertheless, it can assist and serve as guidance to the Company and its employees (especially the AML Officer and the Client Support Department) in recognizing the main methods used for ML/TF. The detection by the Company of any such transactions contained in the said list prompts further investigation and constitutes a valid cause for seeking additional information and/or explanations as to the source and origin of the funds and the circumstances surrounding the particular activity.

In order to identify suspicious transactions, the Company shall monitor on a continuous basis any changes in the Players' transaction patterns and if a Player is engaged in any of the practices that provide any reasonable indication of an AML concern or should be subject to reporting.

Furthermore, the Company should investigate information from employees on suspicious transactions which raises reasonable suspicion of ML/TF. This information is reported on the Internal Suspicion Report. The said reports are archived by the AML Officer and in the player account profile.

If as a result of the evaluation described above, the AML Officer decides not to disclose the relevant information to the FIU, then he/she fully explains the reasons for his decision on the Internal Evaluation Report.

14.2 AML OFFICERS' REPORT TO THE FIU CURACAO

All the reports of the AML Officer will be sent or submitted directly to the FIU Curacao.

After the submission of a suspicious report according to the Policy, the Organization may subsequently wish to terminate its relationship with the Client concerned for risk avoidance reasons. In such an event, the Organization exercises particular caution in order not to alert the Client concerned that a suspicious report has been submitted to the FIU. Close liaison with the FIU is, therefore, maintained in an effort to avoid any impediment to the investigations conducted.

After submitting the suspicious report, the Organization adheres to any instructions given by the FIU and, in particular, as to whether or not to continue or suspend a particular transaction or to maintain the particular account active.

The FIU may instruct the Organization to refrain from executing or delay the execution of a Client's transaction without such action constituting a violation of any contractual or other obligation of the Organization and its employees.

Furthermore, after the submission of a suspicious report according with the current Policy, the Players' accounts concerned as well as any other connected accounts are placed under the close monitoring of the AML Officer.

The Organization and its senior management and employees shall not disclose any details or information in connection with a report filed to the FIU or a request for information made by the FIU. It is not permitted to disclose information to the customer nor to third parties. Drastic action should only be taken when there is no other way out, since any unjustified action may alert the player. In such circumstances, it would be more advisable to increase on-going monitoring and submit additional reports to the FIU on any other suspected instances of ML/TF.

14.4 SUBMISSION OF INFORMATION TO THE FIU

The Company shall ensure that in the case of a suspicious transaction investigation by the FIU, the AML Officer will be able to provide without delay the following information:

- the identity of the account holders
- data of the volume of funds or level of transactions flowing through the account
- accounts detected in similar behavior

in relation to specific transactions:

- the origin of the funds
- the type and amount of the currency involved in the transaction
- the form in which the funds were placed or withdrawn
- the identity of the person that gave the order for the transaction
- the destination of the funds
- the form of instructions and authorization that have been given
- the type and identifying number of any account involved in the transaction

15. RECORD-KEEPING PROCEDURES

The Organization shall retain records, including documentation and information, for use in an investigation into, or an analysis of, the possibility of ML/FT. These records can be requested by the Curacao Gaming Control Board or the FIU Curacao or by other relevant competent authorities as required. The records maintained by the Organization are extremely important to competent authorities responsible for analysis, investigation, law enforcement and prosecution since they may constitute evidence of the audit trail and of money flows. It is therefore crucial that subject persons adhere to the legal obligations applicable in this area.

In case the Organization will establish a documents/data retention policy, the AML Officer shall ensure that the said policy shall take into consideration the requirements of the Law and the Directive.

The AML Officer shall review the adherence of the Company to the above, at least annually.

15.1 RECORDS TO BE RETAINED

The Client Support Department of the Organization shall maintain records of all documents related to the verification process performed on a client in relation to all Business Relationships formed:

- The Client identification documents obtained during the CDD, as applicable
- Monitoring reports obtained during and after the establishment of Business Relationship
- The Organization should also retain the following records required as evidence of compliance with the Law and Directive and for statistical purposes
- Internal suspicious reports made to the AML Office
- Reports made by the subject person to the FIU
- A record of the reasons for not forwarding an internal report to the FIU

A record of AML Officer training provided, including: the date on which the training was delivered; the nature of the training; the names of employees receiving the training; the results of any assessment undertaken by employees; a copy of any hand-outs or slides;

other important records, including: any reports by the AML Officer to senior management/ Board of Directors made for the purposes of complying with the obligations under the Law.

15.2 PERIOD OF RETENTION OF RECORDS

The Organization shall maintain the records for a period of at least five (5) years. The date of commencement of this time period depends on the type of records to be retained.

With respect to CDD and/or EDD documentation, the time period of five (5) years commences from the date on which the Business Relationship is terminated.

It is provided that the documents/data mentioned above which may be relevant to ongoing investigations shall be kept by the Organization until the FIU confirms that the investigation has been completed and the case has been closed.

15.3 FORM OF RECORDS

The Organization maintains records in any one of the following forms: physical file, scanned form, computerized or electronic form.

Subject persons should use a standardized approach to record keeping and must ensure that the approach used enables the quick retrieval of records for the purposes laid out in Section 15.4 below.

15.4 RETRIEVAL OF RECORDS

Subject persons are required to maintain efficient record-keeping procedures that enable them to retrieve information in a timely manner when so requested by the relevant authorities acting in accordance with the Law and Directive.

To this effect, the Organization shall establish effective systems which are commensurate with the size and nature of its business and that enable it to respond efficiently, adequately, promptly and comprehensively to such enquires made to them by Curacao Gaming Control Board, the FIU Curacao or other relevant competent authorities in accordance with Law. The provision of this information is of particular importance in the context of procedures leading to measures such as freezing or seizing of assets, including terrorist assets.

When requests for information are made by the Curacao Gaming Control Board or the FIU Curacao, the Organization should ensure that it is able to reply to these enquiries in a timely manner but not later than five (5) working days from when the demand is made, unless the subject person makes representations justifying why the requested information cannot be submitted within the said time.

15.5 CERTIFICATION & LANGUAGE OF DOCUMENTS

The documents/data obtained, shall be in their original form or in a copy form. A translation shall be attached in the case that the documents above are in a language other than Dutch or English.

Each time the Company shall proceed with the acceptance of a new Client, the Client Support Department shall be responsible for ensuring compliance with the provisions of points above.

16. EMPLOYEES' OBLIGATIONS, EDUCATION AND TRAINING ON ANTI-MONEY LAUNDERING AND TF

The Organizations' employees can be personally liable for failure to report information or suspicion, regarding money laundering or terrorist financing.

The employees cooperate and report, without delay, anything that comes to their attention in relation to transactions for which there is a slight suspicion that are related to money laundering or terrorist financing.

The employees are aware of their obligations of not tipping off customers, where there are any suspicions in regard to money laundering or when there is an ongoing investigation.

The Organization shall establish and adhere to proper policies and procedures in screening their employees for criminal records. The Organization shall develop training programs and provide training to all personnel who handle transactions that may be qualified as unusual based on the indicators outlined in the Ministerial Decree regarding the Indicators for Unusual Transactions (N.G. 2015 no. 73). Training includes setting out rules of conduct governing employee's behavior and their ongoing education to create awareness of the casino's policies against money laundering and terrorist financing. Most areas of the institution should receive training, and the target audience should include most employees. But each segment should be trained on topics and issues that are relevant to them.

Training must at least address the following topics:

New employees. A general training of the nature and process of money laundering and terrorist financing, and the need to report any unusual transactions to the appropriate designated officer must be provided to all new employees who will handle customers or their transactions, irrespective of their level of seniority. They shall be made aware of the existing internal policies, procedures and regulations concerning money laundering, terrorist financing, proliferation of weapons and the reporting requirements. They must also be trained on the money laundering methods and trends in the gambling sector. They must receive an explanation on customer due diligence and objective and subjective indicators for reporting unusual transactions.

Audit staff. Those charged with overseeing, monitoring and testing money laundering controls should also be trained about changes in regulation, money laundering methods and enforcement, and their impact on the organization.

AML Compliance staff. People authorized to perform functions related to the provision and implementation of the AML policy will need specialized training to be able to stay on top of new trends or changes that impact the organization and the way it manages risk. This will require attending conferences or AML-specific presentations to go into greater detail.

Supervisors and Managers. A higher level of instruction covering all aspects of money laundering, terrorist financing policies, procedures and regulations must be provided to those with the responsibility to supervise or manage the staff.

Senior management and board of directors. Money laundering issues and dangers should be regularly and thoroughly communicated to the board. This to keep board members aware of the reputational risk that money laundering poses to the institution. Refreshment training must be arranged at regular intervals to ensure that staff members are kept informed of current and new developments regarding money laundering and terrorist financing techniques, methods and trends. To demonstrate compliance with aforementioned staff training guidelines, the casino shall maintain records that include: Details on the content of the training programs; The names of the staff members who have received the training; The date on which the training was provided; The results of any testing carried out to measure staff understanding of money laundering and terrorist financing requirements; and An ongoing training plan.

The Organization will organize internal and external training for its employees and AML/CFT compliance officer. The AML Officer will additionally provide training to the employees of the Organization, when needed. The main purpose of the training is to ensure that relevant employees become aware of:

- AML Law of Curacao
- European Union laws and directives
- Organizations' Anti-Money Laundering Policy and relevant Procedures
- Statutory obligations of the Organization to report suspicious transactions
- Employees own personal obligation to refrain from activity that would result in ML/TF
- Importance of the Players' due diligence and identification measures requirements for ML/TF prevention purposes.

The training program will have a different structure for new employees and existing employees. On-going training shall be given at regular intervals so as to ensure that the employees are reminded of their duties and responsibilities and kept informed of any new developments.

The Organization will keep documented records, in regard to the trainings attended, dates and the names of the employees that have received the training.

17. REVIEW AND UPDATE OF THE POLICY

The adequacy of internal control measures intended for the prevention of money-laundering and terrorist financing shall be regularly revised in order to ensure that the measures implemented remain up-to-date and are proportionate to risks arising for the Organization. The AML Policy must be reviewed at least annually as well as in the event of any changes in the applicable regulations and/or in cases when provision of new services are being considered.

This AML Policy was updated and executed in April 2025 and filed with the Gaming Control Board and posted publicly on the Company's website for the public.

Peak Interactive N.V. registration number 10847 and its license number OGL/2024/860/0410

Company Directors:

