

GALAKTIKA N.V.

V 1.0

Document

KYC Policy

Document Information

Subject	KYC Policy
Purpose	Defines identity verification and risk management standards to ensure compliance with Curaçao NOIS and NORUT legislation
Involvements	All departments
Ownership	MLRO
Approval	Directors
Review	Annually or earlier as needed
Classification	Company Confidential

Change history

Date	Ver.	Author	Summary Changes	Director
23 June 2026	1.0	Anti-Financial Crime	New document created as part of AML/CFT Program review	

Table of contents

Document Information	1
Purpose and Scope	4
Purpose of the Policy	4
Scope of Application	4
Service Provider Oversight.....	5
Governance and Responsibilities	5
Senior Management Responsibilities	5
Money Laundering Reporting Officer (MLRO)	5
AML/CFT/CFP Compliance Officer	5
Staff and Employee Duties.....	6
Timing of Customer Due Diligence (CDD)	6
Onboarding and Registration	6
Threshold-Based Triggers	6
Event-Based and Subjective Triggers.....	7
Ongoing Monitoring and Periodic Reviews.....	7
Documentation and Information Requirements.....	8
Initial Registration Information	8
Verification of Identity (Proof of Identity)	8
Verification of Address (Proof of Address)	8
Enhanced Due Diligence (EDD) Data	8
Management of Documentation Gaps and Relationship Termination	9
Handling of Missing Documentation and Information	9
Verification Escalation Process	9
Termination of the Business Relationship	10
CDD and Risk Assessment Criteria.....	10
Customer Risk Assessment (CRA) Objective	10
Core Risk Factors	10
Risk Scoring and Categorization	11
Mandatory Escalation and Review Factors	11

Non-Acceptable Criteria	12
Ongoing Monitoring Framework.....	12
Objective of Ongoing Monitoring.....	12
Transactional and Behavioural Monitoring	12
Identification of Red Flags and Suspicious Indicators.....	13
Periodic Reviews and Data Refresh	13
Internal Escalation and Reporting	13
Politically Exposed Persons (PEP) Protocols	14
Politically Exposed Persons (PEPs).....	14
Screening Frequency and Methodology	14
Screening Alert Review and Verification	15
Risk Treatment and Response to Confirmed Matches	15
Sanctions Screening and Alert Management.....	15
Definition and Objective	15
Sanctions Regimes Covered by the Company	16
Screening Controls and Monitoring Frequency	16
Alert Review and Resolution	16
Procedures for True Sanctions Matches	17
Confidentiality and Reporting	17
Data Retention and Recordkeeping	17
General Principles.....	17
Retention Periods.....	18
Scope of Retained Information	18

Purpose and Scope

Purpose of the Policy

This Know Your Customer ("KYC") Policy sets out the standards and procedures implemented by Galaktika N.V. to identify, verify, and monitor its customers throughout the lifecycle of the business relationship. The Policy forms part of the Company's broader AML/CFT/CPF framework and supports the effective management of financial crime risks associated with its gaming operations.

The objectives of this Policy are to:

- Ensure compliance with the National Ordinance on Identification when Rendering Services (NOIS), the National Ordinance on the Reporting of Unusual Transactions (NORUT), and all other applicable AML/CFT/CPF laws, regulations, and regulatory requirements.
- Prevent the Company's products, services, and systems from being used for money laundering, terrorist financing, proliferation financing, sanctions evasion, fraud, or any other unlawful activity.
- Maintain the integrity and security of the Company's gaming operations by applying appropriate customer due diligence measures at onboarding and throughout the duration of the customer relationship.

Scope of Application

This Policy applies to all operations, business processes, technological solutions, and personnel operating under the authority and control of Galaktika N.V. It governs the implementation of customer due diligence measures across all areas of the Company's activities and includes, without limitation, the following:

- **Products and Services:** All online gaming products, casino offerings, and related services made available through websites and domains operated under the Company's gaming licence.
- **Customers:** All individuals (players) who register for, access, or maintain an account with the Company, irrespective of their assigned customer risk classification (Low, Medium, or High).
- **Compliance Systems and Technologies:** All automated and manual tools used to support KYC controls, including sanctions and PEP screening solutions, transaction monitoring platforms, and third-party identity verification providers.
- **Teams and Departments:** All employees

Service Provider Oversight

The Company engages external technology partners and third-party compliance service providers to support key operational and regulatory functions, including software integrity controls, customer identity verification, and sanctions and PEP screening activities.

All such service providers fall within the scope of this Policy. The Company exercises appropriate oversight to ensure that the controls, procedures, and services provided by these third parties remain consistent with the Company's risk appetite, compliance framework, and applicable regulatory requirements.

Governance and Responsibilities

Senior Management Responsibilities

Senior Management is accountable for ensuring ongoing compliance with AML/CFT/CPF requirements within their respective areas of responsibility. In carrying out this obligation, Senior Management shall:

- **Resource Allocation:** Ensure that the MLRO and Compliance Officer are provided with sufficient resources, authority, and support to effectively perform their duties and responsibilities.
- **Policy Approval:** Review and formally approve the Company's AML/CFT/CPF framework, including the Business Risk Assessment (BRA), Customer Acceptance Policy (CAP), Know Your Customer (KYC) Policy, and other related compliance policies and procedures.

Money Laundering Reporting Officer (MLRO)

The MLRO operates independently when assessing suspicious activities and has unrestricted access to all information necessary to perform their responsibilities. The MLRO's duties include:

- **Policy Management:** Developing, maintaining, and updating policies to ensure continued compliance with applicable legal and regulatory requirements.
- **Internal Assessment:** Reviewing all internal reports, alerts, and suspicions to determine whether a disclosure to the Financial Intelligence Unit (FIU) is required.
- **Decision Authority:** Making the final determination regarding the refusal of a prospective customer or the termination of an existing business relationship.

AML/CFT/CPF Compliance Officer

The Compliance Officer is responsible for the operational implementation and day-to-day administration of the AML/CFT/CPF programme. Responsibilities include:

- **Procedural Oversight:** Implementing and maintaining procedures and controls designed to monitor and test compliance with applicable AML/CFT/CPF laws and regulations.
- **Risk Management:** Implementing and overseeing policies and controls intended to manage and mitigate the risks identified through the Business Risk Assessment (BRA).
- **Reporting:** Providing Senior Management with at least one annual report outlining relevant regulatory and industry developments, together with a summary of the Company's internal compliance activities.

Staff and Employee Duties

All employees, irrespective of their position or function within the Company, are required to remain alert to the potential risks of money laundering, terrorist financing, and other financial crime activities. Responsibilities include:

- **Reporting:** Promptly reporting any knowledge, concerns, or suspicions relating to money laundering to the MLRO.
- **Compliance:** Adhering to all procedures and controls relating to customer identification, ongoing monitoring, and record retention requirements.

Timing of Customer Due Diligence (CDD)

Onboarding and Registration

Customer Due Diligence (CDD) commences at the initial point of contact with the customer. The Company does not permit participation in online gaming activities or the deposit of funds until the customer has personally completed the registration process, created an account, and accepted the applicable Terms and Conditions.

- **Mandatory Information Collection:** Registration cannot be completed unless all required information, including the customer's name, date of birth, nationality, and residential address, has been provided.
- **Account Activation:** Customers are not permitted to deposit funds or receive bonuses until their account has been activated through the verification link sent to the registered email address.
- **Initial Screening:** Automated screening tools are used to identify Politically Exposed Persons (PEPs) and sanctioned individuals at the time of registration or upon the first deposit.

Threshold-Based Triggers

The requirement to obtain documentation for identity verification is triggered when a customer reaches specified financial thresholds.

- **Qualifying Payments:** Identity verification must be completed where payments to a customer exceed XCG 4,000 (or the equivalent amount in another currency) in a single transaction or exceed XCG 4,000 in aggregate during any 30-day period.

Event-Based and Subjective Triggers

The Company shall re-perform or strengthen customer due diligence measures whenever specific risk factors are identified, irrespective of whether the applicable financial threshold has been reached.

- **Suspicion of Underage Gaming:** Where there is reason to believe that a customer may be underage and using the details of an adult, additional due diligence documentation and information shall be requested.
- **Changes to Identity Information:** Where a customer's identity or personal details are amended, including but not limited to a change of name, the Company shall repeat the applicable verification procedures.
- **Risk Re-Assessment:** The Customer Risk Assessment (CRA) shall be reviewed and updated whenever material changes occur, including a change of country of residence, the introduction of new payment methods, or renewed activity following a period of account inactivity.

Ongoing Monitoring and Periodic Reviews

Ongoing monitoring is a mandatory and continuous requirement for all customer accounts and is conducted to ensure that customer activity remains consistent with the Company's knowledge of the customer and the customer's declared Source of Funds.

Formal reviews of the Customer Risk Assessment (CRA) are carried out in accordance with the following schedule:

- **High Risk:** Every 12 months.
- **Medium Risk:** Every 24 months.
- **Low Risk:** Every 30 months.

Documentation and Information Requirements

Initial Registration Information

Before a customer account can be established, the following information must be provided during the registration process:

- Date of Birth (minimum age requirement: 18 years);
- First and Last Name;
- Current Residential Address;
- Nationality;
- Email Address;
- Selected Username and Password.

Verification of Identity (Proof of Identity)

Where identity verification requirements apply, the Company accepts any one of the following valid government-issued identification documents, provided the document is signed, unexpired, and submitted as a clear colour copy:

- A Passport.
- A full Driving Licence;
- A national Identity Card;
- An armed Forces Identity Card.

Verification of Address (Proof of Address)

For address verification purposes, customers may be required to provide a document issued within the previous six months which does not reference a P.O. Box. Acceptable documents include:

- Utility bill, rates bill, or council tax statement (excluding mobile telephone bills);
- Bank, building society, or credit card statement;
- Official correspondence issued by a government authority or other independent source;
- Mortgage statement issued by a recognised lender;
- Lawyer's confirmation of property ownership

Enhanced Due Diligence (EDD) Data

Where Enhanced Due Diligence measures are required, the Company may request additional information to better understand the customer's profile and the nature of the relationship. Such information may include:

- Source of Funds evidence, including bank statements or e-wallet statements;
- Source of Wealth evidence, including payslips or employment contracts;
- Supplementary identification information, including former names, aliases, and previous residential addresses.

Management of Documentation Gaps and Relationship Termination

Handling of Missing Documentation and Information

The Company requires customers to provide all information and supporting documentation necessary to satisfy applicable verification and due diligence obligations. This includes Customer Due Diligence (CDD), Enhanced Due Diligence (EDD), Source of Funds, and Source of Wealth requirements.

A customer who does not provide the requested information, or declines to do so without reasonable justification, will not meet the Company's customer acceptance standards and may not establish or continue a business relationship with the Company.

Verification Escalation Process

The Company monitors all accounts that remain outstanding from a verification perspective and applies additional controls where required documentation has not been received within the prescribed timeframe.

Where verification requirements remain incomplete for a period of 30 days following the initial request:

- account restrictions must remain in force, including any restrictions relating to betting activity and payment transactions; and
- a review of the customer's account activity must be undertaken.

The purpose of this review is to identify behavioral patterns that may indicate elevated risk or suspicious activity. Particular consideration shall be given to situations where a customer seeks to withdraw funds after engaging in limited or no gaming activity. Any such indicators must be referred to Compliance for further examination.

Termination of the Business Relationship

The Company is required to discontinue a business relationship where it is unable to satisfy the applicable Customer Due Diligence (CDD) obligations, in accordance with Article III.8 of the Curaçao AML Regulation.

A business relationship may be terminated in circumstances including, but not limited to:

- inability to verify the identity of the customer or beneficial owner;
- failure to obtain adequate information regarding the purpose and intended nature of the relationship;
- inability to complete the required Enhanced Due Diligence (EDD) measures; or
- reasonable grounds to believe that the relationship may be associated with money laundering, terrorist financing, or proliferation financing, where the identified risks cannot be effectively mitigated.

The authority to approve the termination of a customer relationship rests with the MLRO.

All termination decisions, together with the reasons supporting the decision and any actions taken, shall be appropriately documented and retained.

CDD and Risk Assessment Criteria

Customer Risk Assessment (CRA) Objective

As part of its risk-based approach, the Company evaluates the risk profile of each customer when a business relationship is established. The assessment is not static and is reviewed on an ongoing basis to reflect any changes in the customer's profile or activities.

The Customer Risk Assessment (CRA) is designed to determine the level of exposure to money laundering (ML), terrorist financing (TF), and proliferation financing (PF) risks that may arise from providing services to a particular customer.

Core Risk Factors

The Company adopts a risk-based methodology when assessing customers. The overall customer risk profile is established using information obtained throughout the customer relationship, including data collected during account registration, onboarding procedures, verification activities, screening checks, and ongoing monitoring processes.

For the purpose of calculating the Customer Risk Assessment (CRA) score, the Company considers a range of weighted risk indicators, including:

- **Payment Method Risk:** The nature of the payment methods and payment service providers used by the customer.
- **Country Risk:** The customer's country of residence, nationality, and any other relevant connections to particular jurisdictions.
- **Lifetime Risk:** The duration of the customer relationship and the customer's historical activity with the Company.
- **Age Risk:** Risk considerations associated with the customer's age bracket.
- **Monthly Spending Risk:** The customer's actual deposit and withdrawal behaviour, including transaction volumes.

Risk Scoring and Categorization

Based on the calculated numerical score, customers are assigned to one of three risk categories :

Risk Category	Score Range	Requirement Level
Low	$0 \leq \text{score} < 20$	Standard CDD and ongoing monitoring
Medium	$20 \leq \text{score} < 50$	Standard CDD plus additional measures (e.g., enhanced monitoring)
High	$50 \leq \text{score} \leq 100$	Enhanced Due Diligence (EDD)

Mandatory Escalation and Review Factors

Certain risk indicators require immediate review and cannot be assessed solely through the numerical Customer Risk Assessment (CRA) score. Where any of the following circumstances are identified, the matter must be subject to manual review, escalation, or rejection, as appropriate:

- **Transaction Behavior:** Activity patterns indicative of structuring, pass-through transactions, or the use of third-party funding sources.
- **Source of Funds / Source of Wealth Concerns:** Outstanding or unresolved concerns relating to the origin of the customer's funds or wealth.
- **Sanctions and PEP Exposure:** Any potential or confirmed match against sanctions databases or Politically Exposed Person (PEP) lists.

- **Identity or Account Inconsistencies:** Discrepancies in customer information, indicators of linked accounts, or attempts to conceal location through VPNs or proxy services.
- **Adverse Media:** Negative media coverage or publicly available information that may indicate elevated risk.

Non-Acceptable Criteria

The Company shall not establish or maintain a business relationship with any customer whose risk profile falls outside the Company's approved risk appetite. Without limitation, the following customers are considered unacceptable:

- Individuals subject to confirmed sanctions measures.
- Politically Exposed Persons (PEPs), including their family members and close associates, where such status has been confirmed.
- Customers associated with prohibited or restricted jurisdictions.
- Individuals reasonably suspected of acting on behalf of another person, including through the use of mule accounts.
- ☐ Customers who fail or refuse to provide requested Customer Due Diligence (CDD) or Enhanced Due Diligence (EDD) information.

Ongoing Monitoring Framework

Objective of Ongoing Monitoring

The Company conducts ongoing monitoring on a continuous basis to ensure that customer information remains accurate, complete, and up to date. Ongoing monitoring also enables the Company to verify that customer activity remains consistent with the customer's established risk profile. This process plays a key role in identifying unusual, unexpected, or potentially suspicious activity that may arise during the course of the customer relationship following onboarding.

Transactional and Behavioural Monitoring

The Company continuously reviews customer activity through a combination of automated monitoring tools and manual oversight procedures. Monitoring activities include, but are not limited to, the following:

- **Activity Consistency Reviews:** Assessing whether the volume, frequency, and characteristics of deposits and withdrawals are consistent with the Company's understanding of the customer, their risk profile, and their declared Source of Funds.
- **Automated Monitoring Alerts:** Using system-generated alerts to identify activity that differs from expected behaviour, including significant increases in transaction volumes or rapid movement of funds.

- **Payment Method Monitoring:** Reviewing the use of multiple payment instruments or third-party payment methods and seeking to ensure that withdrawals are returned, where possible, to the original funding source.

Identification of Red Flags and Suspicious Indicators

Employees receive training to identify behavioural patterns and risk indicators that may suggest money laundering or other suspicious activity. The Company considers, among others, the following warning signs during its monitoring activities:

- **Structuring (Smurfing):** Repeated transactions designed to remain below applicable verification thresholds (e.g., NAF 4,000).
- **Pass-Through Activity:** The deposit of substantial funds followed by a withdrawal request after little or no gaming activity.
- **Profile Inconsistencies:** Customer activity that is inconsistent with the customer's declared occupation, financial circumstances, or economic profile.
- **Concealment of Identity or Location:** Frequent amendments to personal information or repeated use of VPNs, proxies, or similar technologies to obscure the customer's actual location.
- **Collusive Behavior:** Indicators suggesting that multiple accounts may be connected or operated in a coordinated manner.

Periodic Reviews and Data Refresh

To maintain accurate and current Customer Due Diligence (CDD) records, the Company performs periodic reviews of each Customer Risk Assessment (CRA) according to the following schedule:

- High Risk: Reviewed every 12 months.
- Medium Risk: Reviewed every 24 months.
- Low Risk: Reviewed every 30 months.

As part of these reviews, the Compliance Team confirms that identification documents remain valid and assesses whether any new risk factors have emerged, including adverse media findings or Politically Exposed Person (PEP) status.

Internal Escalation and Reporting

Where ongoing monitoring identifies activity that may be considered unusual or suspicious, the Company follows the escalation process set out below:

1. **Identification:** A potential red flag is identified either by an employee during the course of their duties or through the generation of a high-priority alert by an automated monitoring system.
2. **Internal Reporting:** The employee or investigator prepares an internal Suspicious Activity Report (SAR) documenting the circumstances and reasons giving rise to the suspicion.

3. **MLRO Review:** The SAR is submitted to the MLRO for assessment. The MLRO has sole authority to determine whether the matter should be reported to the Financial Intelligence Unit (FIU) Curaçao.
4. ☐ **Prohibition on Tipping-Off:** Under no circumstances shall the customer be informed that they are the subject of a suspicion, review, investigation, or potential report to the FIU during the monitoring or escalation process.

Politically Exposed Persons (PEP) Protocols

Politically Exposed Persons (PEPs)

For the purposes of this Policy, a Politically Exposed Person (PEP) is an individual who currently holds, or has previously held, a prominent public position or function. PEPs include, but are not limited to:

- Members of the executive branch, including Heads of State, Heads of Government, Ministers, Deputy Ministers, and Assistant Ministers;
- Individuals serving in national parliaments or other comparable legislative bodies;
- Members of governing or executive bodies of political parties;
- Senior judicial officials, including judges of supreme courts, constitutional courts, or equivalent judicial institutions;
- High-ranking military officers, as well as ambassadors and chargés d'affaires;
- Senior management, supervisory, or administrative officials of state-owned enterprises;
- Members of the boards of directors, including directors and deputy directors, of international organisations..

The PEP classification also applies, where relevant, to:

- **Family Members**, including spouses, partners, children, and parents; and
- **Close Associates**, including persons who maintain close business relationships or share beneficial ownership interests in legal entities with a PEP.

Screening Frequency and Methodology

To mitigate regulatory and financial crime risks, the Company applies a structured screening process designed to identify and manage PEP-related exposure.

- **Onboarding Identification:** Screening against recognised global PEP databases is performed at the point of registration or upon the first deposit transaction.
- **Continuous Monitoring:** Customers are subject to automated daily rescreening in order to detect any change in PEP status occurring after onboarding.

- **Adverse Information Review:** Screening processes also incorporate checks of adverse media sources to identify potential political exposure or indications of corruption or misconduct involving public officials.

Screening Alert Review and Verification

All alerts generated through the Company's automated screening tools are subject to a structured review and verification process to determine their relevance and accuracy:

- **Preliminary Assessment:** The Compliance Team performs an initial assessment of each alert to determine whether it constitutes a false positive (for example, due to name similarity) or a potential match requiring further review.
- **Additional Verification Measures:** Where an alert is assessed as a potential match, the Company may request supplementary identification data, such as full name details, middle names, or identification numbers, in order to confirm or rule out the match.
- **MLRO Review and Determination:** Any alerts confirmed as true matches are escalated to the MLRO, who is responsible for making the final determination regarding the appropriate action.

Risk Treatment and Response to Confirmed Matches

In line with the Company's Customer Acceptance Policy (CAP), individuals identified as Politically Exposed Persons (PEPs), including their family members and close associates, are not eligible for onboarding or continued business relationships.

- **Onboarding Outcome:** Where a PEP match is identified during the onboarding process, the application is rejected and no customer relationship is established.
- **Ongoing Monitoring Outcome:** Where an existing customer is identified as a PEP during ongoing monitoring, the business relationship must be terminated.
- **Internal Recordkeeping and Confidentiality:** All decisions relating to rejection or termination are documented for internal audit and compliance purposes. The customer is not informed of the specific reason related to PEP classification in order to prevent any risk of tipping-off.

Sanctions Screening and Alert Management

Definition and Objective

Sanctions refer to restrictive measures imposed at international level to combat financial crime, terrorism, and related illicit activities. These measures are intended to apply pressure on designated countries, entities, or individuals where other diplomatic or preventive efforts have not achieved the desired outcome.

Galaktika N.V. implements sanctions screening procedures to ensure that its services and financial operations are not made available to sanctioned individuals or entities. Such persons are deemed outside the Company's acceptable risk framework and are therefore not eligible for any form of engagement.

Sanctions Regimes Covered by the Company

As part of its compliance obligations, the Company monitors and screens against key international sanctions lists, including:

- **United Nations (UN) Sanctions:** Consolidated lists issued by the UN Security Council targeting individuals and organisations involved in terrorism-related activities, including ISIL and Al-Qaeda.
- **European Union (EU) Sanctions:** Restrictive measures adopted under the EU Common Foreign and Security Policy framework.
- **United States (OFAC) Sanctions:** Economic and trade sanctions issued by the US Office of Foreign Assets Control, including those applicable to USD transactions.
- **United Kingdom and Australian Sanctions:** National sanctions regimes maintained by HM Treasury (OFSI) and the Australian Sanctions Office (ASO).

Screening Controls and Monitoring Frequency

- **Onboarding Screening:** Automated screening tools are applied at the time of customer registration and/or upon the first deposit to identify any sanctioned individuals or entities.
- **Continuous Monitoring:** The Company conducts daily automated rescreening using third-party compliance systems to ensure ongoing detection of any changes in sanctions status.

Alert Review and Resolution

All screening alerts generated by the Company's monitoring systems are subject to mandatory review by Compliance personnel in order to determine whether the alert constitutes a false positive or a true match.

- **False Positive Determination:** Where an alert is assessed as a false positive based on identifier comparison (including name, date of birth, nationality, or other available data), the decision and supporting rationale must be recorded. In such cases, the customer relationship may continue without interruption.
- **True Positive Confirmation:** Where a match is confirmed as a true positive, the Compliance analyst must immediately escalate the matter by submitting an internal report to the MLRO for further action.

Procedures for True Sanctions Matches

Where an individual or entity is confirmed as a sanctioned party, the following measures must be implemented without delay:

- **Asset Restriction:** All funds and economic resources belonging to or controlled by the client within the Company must be immediately frozen.
- **Service Cessation:** The Company must cease all financial transactions and discontinue provision of services to the client.
- **Account Suspension:** The customer account must be suspended pending instructions from the MLRO.
- **Enhanced Due Diligence:** Enhanced Due Diligence (EDD) procedures must be applied to ensure full documentation and confirmation of the match.
- **Post-Onboarding Offboarding:** Where a sanctioned status is identified after onboarding, the relationship must be terminated, subject to applicable freezing and regulatory reporting obligations.

Confidentiality and Reporting

- The Company enforces a strict prohibition on any disclosure to the customer or any external party regarding the application of freezing measures or the existence of any ongoing investigation or review. Disclosure is strictly limited to authorized internal personnel, including the MLRO and senior management, where required for compliance purposes.
- Where the MLRO determines that reasonable grounds exist in relation to a confirmed match or suspicious activity, the MLRO is responsible for ensuring that the relevant report, together with all required supporting information, is submitted to the Financial Intelligence Unit (FIU) in accordance with applicable regulatory obligations.

Data Retention and Recordkeeping

General Principles

The Company implements a comprehensive recordkeeping framework to ensure that all customer-related information and transactional data are properly stored and retrievable for regulatory, supervisory, and law enforcement purposes. This framework is designed to support a complete and reliable audit trail of all customer activity.

All compliance-related materials, including internal policies, risk assessments, procedures, and training records, are retained within a secured back-office environment. Access to this environment is strictly controlled and granted on a need-to-know basis, with full system access reserved exclusively for the Money Laundering Reporting Officer (MLRO).

Retention Periods

The Company retains customer-related and compliance-related records in accordance with applicable statutory and regulatory requirements to ensure full traceability of customer activity and compliance decisions:

- **Customer Records:** All identification data, Customer Due Diligence (CDD) and Enhanced Due Diligence (EDD) documentation, and full transactional history are retained for a minimum period of five (5) years following account closure or the date of the last recorded transaction.
- **AML and Compliance Registers:** Records contained in internal and external reporting registers, including those relating to suspicious activity and money laundering or terrorist financing inquiries, are retained for five (5) years after termination of the business relationship, or longer where required by the Financial Intelligence Unit (FIU).

Scope of Retained Information

The Company maintains secure and systematically backed-up records of key operational and compliance data, including:

- **Customer Onboarding and Verification Data:** Registration details, identity verification documents, and all CDD and EDD materials.
- **Financial Transaction Records:** Complete records of deposits, wagering activity, withdrawals, winnings, and payment reconciliations.
- **Account Lifecycle Information:** Records relating to account suspensions, closures, and self-excluded or restricted users, including the reasons for such actions.
- **Responsible Gaming Records:** Data relating to self-exclusion requests (temporary or permanent) and customer-defined gaming limits.
- **Customer Communications:** All correspondence between customers and customer support or operational teams.
- **Investigation and Audit Materials:** Internal case files, investigation notes, and audit trails relating to customer activity reviews and compliance checks.