

Riotech N.V.

Know Your Customer Policy

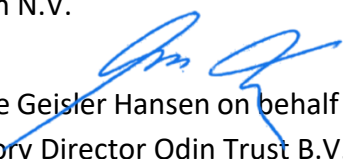
Policy Owner	Riotech N.V.
Approver	 Christie Geisler Hansen on behalf of Statutory Director Odin Trust B.V.
Date approved	31 Mar 2025
Date last reviewed	31 Mar 2025
Review frequency	Annual
Next review date	31 Mar 2026
Responsible for document management and update	Maksym Fedorenko, MLRO
Security classification	Private and Confidential
Status	New Policy

TABLE OF CONTENTS

1. DEFINITIONS	4
2. STATEMENT	6
3. SCOPE AND PURPOSE	6
4. ROLES AND RESPONSIBILITIES	7
5. DUE DILIGENCE FRAMEWORK AND CUSTOMER RISK ASSESSMENTS	8
5.1 Overview	8
5.2 Customer Due Diligence (CDD)	9
5.3 Enhanced Due Diligence (EDD)	10
5.4 Indicators of High-risk Customers	11
6. ONBOARDING A NEW CUSTOMER	13
6.1 Registration and Pre-onboarding Stage	13
6.2 CDD Minimum Requirements	13
6.3 EDD Minimum Requirements	14
6.3.1 Results from screening and background checks	15
6.3.1.1 The customer is a possible PEP	15
6.3.1.2 The customer may be a sanctioned individual, or linked to a sanctioned entity	16
6.3.1.3 The customer has a criminal conviction	16
6.3.1.4 The customer's name is on the Self-exclusion list	17
6.3.1.5 Other screening hits	17
6.3.2 Adverse Media Screening	17
6.3.3 Four-eye Review	17
7. ACCEPTABLE VERIFICATION DOCUMENTS	18
8. DEPOSIT AND WITHDRAWAL METHODS	19
9. TRANSACTION-DRIVEN DUE DILIGENCE	19
9.1 Initial 2000 EUR trigger	20
9.2 Subsequent 2000 EUR triggers	21
10. REVIEWING A CUSTOMER FILE	21
10.1 Periodic review frequency and due dates	22
10.2 Low-risk customer review	22
10.3 Medium and high-risk customer review	25
10.4 Escalations from the First Line of Defence	27
11. DORMANT ACCOUNTS	28
12. ESCALATION PROCEDURES	28
12.1 SAR Log	30
12.2 Account closure	29
13. SUSPICIOUS ACTIVITY REPORTING POLICY	31

13.1 Reporting Obligations	31
13.2 Indicators of Unusual Transactions	31
13.3 Reporting Procedures	32
13.4 Compliance and Review	32
14. BUSINESS RISK ASSESSMENT	32
14.1. Identification of Risks	32
14.2. Risk Assessment	33
14.3. Mitigation Measures	33
14.4. Risk Appetite	34
345	
15.1. Suppliers Minimum Requirements	35
15.1.1 Business criticality	36
15.1.2 Due Diligence	36
15.1.3 Review and approval	36
15.1.4 Standard clauses	37
15.1.5 Monitoring	37
15.2. Governance, Review	38
37	38
16.1 Purpose	38
16.2 Retention Period and Requirement	38
16.3. Expiry of Retention Period	39
17. MLRO CONTACT DETAILS	39
 Appendix 1 – Safer Gambling Questionnaire	 40
Appendix 2 – Source of Funds / Source of Wealth Questionnaire	42
Appendix 3 – EDD Checklist	43
Appendix 4 – Low-Risk Customer Review Checklist	44
Appendix 5 – Medium / High-Risk Customer Review Checklist	45
Appendix 6 – SAR Report	46
Appendix 7 – High-risk products, services and payment methods	47

1. DEFINITIONS

AML	Anti-money laundering
Customer relationship	The commercial relationship between a remote gaming operator and a customer, which is expected to have an element of duration.
Criminal spend	In the context of gambling, the use of the proceeds of crime to fund gambling as a leisure activity (also known as lifestyle spend)
CTF	Counterterrorist financing
CGA	Curaçao Gaming Authority
High-risk countries	The Financial Action Task Force maintains an internationally recognized list of countries that are of high-risk for financial crime
High-risk products or services and payment methods	A list of products or services and payment methods which are considered high-risk by Riotech N.V. listed in Appendix 7
Low-risk countries	Countries that are not considered by the Financial Action Task Force as high-risk for financial crime
MLRO	Money Laundering Reporting Officer
Money laundering	The process by which criminal or 'dirty' money is legitimized or made 'clean', including any action taken to conceal, arrange, use, or possess the proceeds of any criminal conduct
FIU	Financial Intelligence Unit Curaçao. This is the unit in Curaçao that is responsible for the collection, collation, processing, analysis and dissemination of information to combat money laundering and the funding of terrorism
Operator	A company that holds an operating license issued by the the Curaçao Gaming Authority
PEP	Politically Exposed Person
Proceeds of crime	Property from which a person benefits directly or indirectly, by being party to criminal activity, for example, stolen money, money from drug dealing or property stolen in a burglary or robbery

SAR	A suspicious activity report – the means by which suspicious activity relating to possible money laundering or the financing of terrorism is reported to the FIU
Source of funds	Where the funds, money, or cash to finance the transaction come from
Source of wealth	The origins of a person’s overall body of wealth (that is, their total assets), which should give an indication of the volume of wealth the person actually has, and how they acquired it.
Terrorist Financing	The raising and processing of funds to supply terrorists with resources, through exploitation of the vulnerabilities in financial systems that allow for an inappropriate level of anonymity and opacity in the execution of financial transactions

2. STATEMENT

Riotech N.V. is committed to complying with all applicable Anti-Money Laundering (AML) and Counter-Terrorist Financing (CTF) laws and regulations, including those issued by the Curaçao Gaming Authority and the Financial Intelligence Unit of Curaçao. This Know Your Customer (KYC) Policy establishes the company’s intent to uphold a robust customer due diligence framework that effectively identifies, verifies, and monitors customer identity and activity throughout the entire business relationship.

The policy applies to:

- All Riotech N.V. business units involved in customer onboarding and transaction monitoring,
- All staff involved in risk management and compliance, and
- Third-party service providers acting on behalf of Riotech N.V. where relevant to customer due diligence.

This policy forms part of the company’s broader AML/CTF compliance framework and must be implemented alongside the company’s Business Risk Assessment (BRA), Customer Risk Assessment (CRA), Suspicious Activity Reporting procedures, and Responsible Gaming practices.

3. SCOPE AND PURPOSE

Riotech N.V. is regulated by the Curaçao Gaming Authority under application number OGL/2024/599/0274 and is subject to the AML CFT/CFP-Regulations for online gaming providers as of January 9, 2025.

The purpose of this Know Your Customer (KYC) Policy is to establish a structured framework of requirements for the onboarding and verification of all new and reactivated customers, in accordance with the applicable legal and regulatory obligations. The policy forms part of Riotech N.V.'s broader AML/CFT compliance programme and aims to ensure effective mitigation of money laundering, terrorist financing, and other financial crime risks.

This policy further supports responsible gambling practices and the protection of vulnerable individuals, as required under the regulatory framework in Curaçao.

The MLRO will periodically review this policy for consistency with relevant guidance issued by regulatory authorities. All relevant business units and staff must adhere to the policy.

Failure to comply may:

- Result in Riotech N.V. inadvertently facilitating financial crime;
- Expose vulnerable individuals to gambling-related harm;
- Lead to enforcement action by the regulator; and/or
- Cause significant reputational and financial damage to the Company.
- result in internal disciplinary action, suspension of access to systems, or reporting to the Regulator as deemed necessary.

4. ROLES AND RESPONSIBILITIES

To ensure the company operates effective systems and controls for the management and oversight of financial crime and gambling harm risks, the control environment is based upon the three lines of defence model.

1. The first line of defence (1LOD) consists of automated systems that handle risks associated with ML/FT/FP. The 1LOD includes various automated processes such as transaction monitoring software, machine learning algorithms, and fraud detection software.
2. The second line of defence (2LOD) comprises those within the Compliance Department, this includes MLRO and their respective teams. They have responsibility for setting and maintaining a financial crime and responsible gambling framework, monitoring and investigating alerts generated by automated systems, compliance within the first line of defence and reporting internally to senior management, and externally, when applicable.

The MLRO has ultimate oversight of the financial crime framework.

3. The third line of defence (3LOD) is an independent function represented by Internal Audit which provides independent assurance to senior management regarding the effectiveness with which the organization assesses and manages its risk, including the effectiveness of the 1LOD and 2LOD. The Internal Audit function is outsourced.

5. DUE DILIGENCE FRAMEWORK AND CUSTOMER RISK ASSESSMENTS

5.1 Overview

Due diligence is the process of identifying, gathering information about customer, and understanding the customers sufficiently in order to ensure that the Company is comfortable with establishing and maintaining a customer relationship with them and ensuring that there is no legal barrier to providing them with the product or service requested. This includes not permitting the customer to make any deposits upon reaching the threshold of 2000 EUR or equivalent in another currency.

Due diligence and ongoing monitoring must be conducted throughout the lifecycle of the customer relationship to ensure the company continues to demonstrate that it has identified and understands the risks posed by the customer and that the information obtained remains accurate and up to date.

According to the AML CFT/CFP-Regulations for Curaçao providers of online gaming as of January 9, 2025, the operator has the obligation to undertake Due Diligence measures when:

- When players engage in financial transactions equal to or above 2000 EUR;
- carrying out occasional transactions above the monetary equivalent of 2000 EUR;
- there is a suspicion of money laundering or terrorist financing; or
- the operator has doubts about the veracity or adequacy of previously obtained customer identification data.

Due Diligence also includes measures aimed at establishing beneficial owner. If Riotech N.V. has reasonable grounds to believe that the funds being wagered are collected from multiple persons who will eventually share in any winnings, the particular transaction will not only be considered as having been undertaken by the customer but undertaken also for the benefit of those persons providing the necessary funding. These persons would be considered as

beneficial owners and we would therefore have to identify them and verify their identity in accordance with EDD procedure.

The extent of due diligence measures applied will be determined by the customer's risk profile. In doing so, Riotech N.V. has adopted a risk-based approach in accordance with the AML CFT/CFP-Regulations for Curaçao providers of online gaming as of January 9, 2025 (as may be amended from time to time). When determining the risk profile of a customer, consideration is also given to responsible gambling risks.

The following levels of due diligence are applied depending on the final risk rating:

Risk Rating	Level of Due Diligence
Low Risk	Customer Due Diligence
Medium Risk	Enhanced Due Diligence
High Risk	Enhanced Due Diligence

The frequency of periodic reviews and additional heightened monitoring will vary for each risk level.

The risk profile of a customer may change during the period of the customer relationship, for instance, where there are possible gambling harm risks.

5.2 Customer Due Diligence (CDD)

CDD is the lowest level of due diligence that can be applied and can only be applied where the customer's risk rating is low, both for financial crime and responsible gambling purposes. CDD must be applied before a customer's account can be opened, and before they are able to make a deposit.

In order to be considered of low risk, the customer must meet the following criteria:

- Be an individual aged 18+ (or 21+ where applicable). Customers under the legal gambling age are strictly prohibited;

- Be a resident of the countries that are considered low risk;
- Automated screening checks are passed. Such checks are performed by SEON Identity Verification Service;
- A valid residence permit (both sides if applicable); and
- A utility bill (less than 3 months old) for gas, electricity, or phone, or a rental invoice. Alternatively, a document from a government department, mortgage statement, or equivalent are provided.
- Employment status and income levels are within the low risk category (see figure 1 below).

5.3 Enhanced Due Diligence (EDD)

EDD is the level of due diligence to be performed for customers who are considered to be of medium or high risk.

A customer is considered to be of medium risk when they meet the following criteria:

- Be an individual aged 18+ (or 21+ where applicable). Customers under the legal gambling age are strictly prohibited;
- Be a resident of the High-risk countries;
- Automated screening checks are passed;
- A valid residence permit (both sides if applicable); and
- A utility bill (less than 3 months old) for gas, electricity, or phone, or a rental invoice. Alternatively, a document from a government department, mortgage statement, or equivalent are provided.
- Employment status and income levels are within the medium risk category (see figure 1 below).

A customer is considered to be of high risk when they meet any of the following criteria;

- Their identity documents are not electronically verified;
- Their place of residence or date of birth is not electronically verified;
- Automated background checks result in a hit which requires review (for example, the customer has PEP status); or

- Employment status and/or income levels are within the high-risk category (see figure 1).

High risk customers will also be subject to more frequent periodic reviews.

5.4 Indicators of high-risk customers

Examples of the types of responses during EDD, or other correspondence, which should give rise to concerns in relation to financial crime and/or gambling harm risks include but are not limited to:

- Details about self-exclusions;
- Lack of veracity in relation to source of wealth / funds, i.e. bank statements show funding levels that far exceed the customer's declared income, or are there often large and irregular payments being made into an account;
- Information indicating that the customer is experiencing financial difficulties;
- Information indicating that the customer is seeking to use gaming as a source of income;
- Comments made by the customer that indicate possible addiction, such as comments about being anxious or stressed;
- Jovial comments about their physical or mental health;
- Information indicating cognitive impairment; and/or
- Possible connections to jurisdictions that are considered high-risk for the purpose of money laundering and terrorist financing.

This list is not exhaustive, so it's important to exercise appropriate judgment and caution when reviewing EDD information.

Figure 1.

This is the initial risk profile to be applied to a customer based on registration information and in the absence of any screening hits.

Unemployed Student Retired	Full-time employment Part-time employment Self-employed	Full-time employment Self-employed Part-time employment	Full-time employment Self-employed Part-time employment
Income - N/A	Annual income of 14,999 EUR or lower	Annual income of 50,000 EUR or higher	Annual income of 15,000 to 49,999 EUR
High Risk	High Risk	Medium Risk	Low Risk
Enhanced due diligence	Enhanced due diligence	Enhanced due diligence	Customer Due diligence

6. ONBOARDING A NEW CUSTOMER

6.1 Registration and pre-onboarding stage

All individuals seeking to become a customer of Riotech N.V. must first complete an online registration form via the company's website.

Customers are required to provide the following information:

- Full name
- Last name
- Email address
- Username
- Date of Birth
- Place of Birth
- Country of Residence
- Permanent Residential Address
- Identity number
- Nationality
- Confirmation that the User is not a PEP (politically exposed person), agrees to KYC procedure and is registering to play on his/her own behalf.
- Acceptance of the Terms and Conditions and Privacy Policy
- Consent to receive promotional emails and offers (optionally)

6.2 CDD Minimum Requirements

CDD is the level of due diligence applied for low-risk customers and also resembles minimum requirements for all customers. For those customers categorized as low risk, their account can be opened following satisfactory completion of CDD.

The minimum requirements are:

- Provision of information stipulated in section 6.1.

The Riotech N.V. representatives may conduct verification of identification documentation when customers deposit at least 200 EUR or equivalent. Riotech N.V. may collect CDD-required documents from customers if deposits are below 200 EUR or equivalent when they request a withdrawal, regardless of the withdrawal amount.

6.3 EDD Minimum Requirements

EDD is additional due diligence that must be applied for medium and high-risk customers.

Enhanced Due Diligence **has to** be conducted where the risks of money laundering or terrorist financing are higher. This concerns for example:

- Residents of higher-risk geographic areas;
- Political Exposed Persons (PEP's);
- Products or transactions that might favor anonymity;
- New products and new business practices, including new delivery mechanisms and the use of new or developing technologies for both new and pre-existing products.

The minimum requirements when performing EDD are:

- Identification and proof of address and date of birth, plus verification as per section 6.2;
- Obtaining information in relation to the customer's occupation;
- Safer Gambling Questionnaire (Appendix 1);
- Obtaining information in relation to the customer's source of wealth/source of funds by filling out the Source of Wealth / Source of Funds Questionnaire (Appendix 2);
- Updating the identification data of the customer more regularly;
- Requiring the first payment to be carried out through an account in the customer's name with a bank subject to similar CDD standards.
- Completing background checks and screening that is performed via Sumsub. The checks performed are:
 - PEP status
 - Sanctions (at minimum, check in accordance with the UN Sanctions List and EU Sanctions List)
 - Whether the name matches the address listed against register

Questionnaire responses must be satisfactory, requiring staff to use sound judgment regarding financial crime and responsible gambling risks. If responses are unsatisfactory or

are not provided within the timeframe of 30 days, Riotech N.V. has to terminate the relationship with the player and report the transaction to the FIU if a presumption of money laundering or terrorist financing exists. If no presumption of money laundering exists, the funds should be transferred to the same bank account or wallet it was deposited from. If presumption of money laundering or terrorist financing exists, Riotech N.V. may at its sole discretion block player's funds and inform the player.

Riotech N.V. records of all the attempts made to get the necessary information and documentation during CDD and/or EDD.

If uncertain, it requires consultation with the MLRO for guidance. Complete the EDD Checklist (Appendix 3) to document and evidence EDD performed, including rationale and MLRO guidance. A four-eye review is required before opening accounts, as outlined in section 6.3.3

6.3.1 Results from screening and background checks

Where one or any of the factors for EDD is any of the below, EDD should also include as follows:

6.3.1.1 The customer is a possible PEP

It is Riotech N.V. policy not to allow playing and blocking of the account of any individuals who are considered to be PEP. PEP screening is one of the checks performed by Sumsb.

A PEP is an individual who is entrusted with prominent public functions, other than middle-ranking or more junior officials, including the following individuals:

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

The following individuals are also regarded as PEPs by virtue of their relationship or association with the individuals listed above:

- family members of the individuals listed above, including spouse, partner, children and their spouses or partners, and parents; and
- known close associates of the individuals listed above, including individuals with whom joint beneficial ownership of a legal entity or legal arrangement is held, with whom there are close business relations, or who is a sole beneficial owner of a legal entity or arrangement set up for the benefit of the PEP.

A PEP can either be a current PEP, or have been a PEP within the previous 12 months. In some cases, PEP status can still be applied after these 12 months, where there is a higher risk of money laundering or terrorist financing. Where an individual was a PEP more than 12 months ago, approval is to be sought from the MLRO as to whether the account can be opened and EDD must be performed. This should include, in addition to the above EDD minimum requirements:

- Adverse media screening
- Obtain approval from the MLRO to open the account.

A record of the checks and approvals should be kept in the EDD Checklist.

6.3.1.2 The customer may be a sanctioned individual, or linked to a sanctioned entity

If the checks raise that the individual is, or may be, a sanctioned person, or linked to a sanctioned entity, you should perform appropriate checks to verify whether or not the individual is sanctioned.

If the individual is sanctioned, the customer account must be immediately closed. Evidence obtained confirming sanction status should be stored on the customer's file.

Where you have reason to believe the result is a false positive, or that the nature of the sanction does not preclude Riotech N.V. from closing the account, this should be referred to the MLRO for confirmation on how to proceed.

6.3.1.3 The customer has a criminal conviction

Where there is evidence of criminal convictions, you should consider whether the nature of the conviction gives rise to a higher risk of money laundering or terrorist financing. For example, convictions in relation to drug offenses or other serious offenses should give rise to the account opening being rejected.

When reviewing a customer with a criminal conviction, in addition to the above EDD minimum requirements, you should perform:

- Adverse media screening;
- Obtain approval from the MLRO to open the account.

6.3.1.4 The customer's name is on a Self-exclusion list

When the customer's name appears on a list for being under a self-exclusion period, the customer's account cannot be opened under any circumstances.

6.3.1.5 Other screening hits

This section 6.3.1 is not an exhaustive list of items that could be raised through background and ad-hoc checks and due diligence, where something is raised that is not referenced above, please refer to the MLRO for guidance. In such cases, staff must escalate the issue to the MLRO or Compliance Officer for further assessment before any account decision is made.

6.3.2 Adverse Media Screening

Adverse media screening involves searching for negative news about a person through public sources, typically using an internet search engine. When conducting adverse media searches as part of EDD, record findings in the EDD Checklist.

Assess how negative information affects the customer's risk profile and whether the account should proceed to closing. If uncertain, seeking guidance from the MLRO is required.

6.3.3 Four-eye review

All customers who have undergone EDD must undergo a four-eye review before their accounts are opened. This entails another team member reviewing the information and rationale for account opening. If a customer has been referred to the MLRO for approval prior to account opening, the MLRO's review and approval satisfy the four-eye review requirement.

7. ACCEPTABLE VERIFICATION DOCUMENTS

Data and information about a customer's identity must come from a reliable and independent source.

Documents to be used (unexpired government-issued document containing photographic evidence):

- Driver's license
- Identification card

- Travel document or passport

For verification of residential address can also be used any of the following documents not older than 3 months old:

- Bank statement
- Utility bill
- Correspondence from a central or local government authority, department or agency
- A rental or lease agreement

Documents should be authentic, clear, legible and of good quality.

Riotech N.V. can also contact a player by telephone, letter or e-mail in order to obtain an additional confirmation.

Some documents, like passports, birth certificates, and identity cards, may naturally be older than 3 months. However, utility bills or bank statements older than 3 months cannot be accepted. While these documents are acceptable, exercise judgment when manually reviewing them. This includes querying affordability and assessing financial crime risks when customers present benefits books, and considering gambling harm if bank statements show debt or frequent gaming elsewhere, or if utility bills are in arrears.

8. DEPOSIT AND WITHDRAWAL METHODS

Riotech N.V. operates a closed loop policy with respect to the withdrawal of funds. This means electronic payments out of a customer's account are only permissible to the same card or bank account as the original deposit. A customer cannot make a deposit using one account, and then withdraw funds into a different account. Riotech N.V. can also establish the list of payment methods which are considered as high-risk (can be found in Appendix 7).

9. TRANSACTION-DRIVEN DUE DILIGENCE

The AML CFT/CFP-Regulations for Curaçao providers of online gaming as of January 9, 2025 requires certain transaction driven due diligence.

According to AML CFT/CFP-Regulations for Curaçao as of January 9, 2025 financial transactions are deposits and withdrawals (bonuses are not included). Amounts wagered and winnings are considered as gambling transactions. Gambling transactions are not considered as financial transactions.

A transaction consists of:

- The deposit of funds required to take part in remote gambling; or
- The collection of winnings, including the withdrawal of funds deposited to take part in gambling or winnings arising from such funds. Winnings from a previous transaction that have already been collected should not be considered for the purpose of the 2000 EUR threshold.

Exception: amounts wagered and winnings are considered as gambling transactions. Gambling transactions are not considered as financial transactions and do not fall under the provisions of section.

Riotech N.V. has transaction monitoring alerts to identify such transactions:

- When a customer's lifetime deposit or withdrawal reaches 2000 EUR or more; and
- When a customer deposits or withdrawals 2000 EUR in one single transaction or in a series of linked transactions. For the purpose of being linked, Riotech N.V. considers transactions to be linked when cumulatively, they amount to 2000 EUR within a 24-hour period, or they are carried out by the same player through the same game or in one gaming session.

9.1 Initial 2000 EUR trigger

Low risk customers

When a low-risk customer reaches the 2000 EUR threshold, EDD is to be performed, in accordance with section 6.3. The EDD Checklist is to be completed and saved on the customer file.

The customer's risk profile should be changed to medium, unless there are specific concerns or cause for it to be high, or, for the account to be closed.

Medium and high-risk customers

Where EDD has already been performed, due to the customer being classified as medium or high risk at onboarding, the customer file and information should be reviewed again, with respect to affordability and financial crime risks.

The on-going appropriateness of the customer's risk profile should also be considered, including whether to move the customer to high-risk, introduce additional limits, or closure of the account.

Customers should be moved from medium risk to high risk, when following review, they are considered to pose a risk of gambling harm - this is determined by whether or not any safer gambling tools are employed.

Alternatively, the account is closed due to the level of gambling harm posed, or due to financial crime risk resulting in the submission of a SAR.

When a customer reaches a cumulative transaction threshold of 2000 EUR and the casino has not yet collected the required documents under the CDD Minimum Requirements, the customer shall be subject to the following restrictions:

- The customer shall not be permitted to deposit additional funds into their account.
- The customer shall not be permitted to withdraw any funds until the required documentation is provided and verified.
- The customer may continue to play using the funds already available in their account.

If the required information and/or documents are not provided by the customer within 30 days from the moment they reach the 2000 EUR threshold, Riotech N.V. shall:

- Terminate the customer relationship and close the account.
- Assess whether there is a presumption of money laundering or terrorist financing:
 - If a presumption exists, the transaction shall be reported to the FIU, and funds should be blocked unless the customer can provide a clear source of funds documents supporting such funds.
 - If no presumption of money laundering exists, the remaining balance shall be returned to the original payment method (i.e., the same bank account or wallet from which the funds were deposited).

9.2 Subsequent 2000 EUR triggers

After a customer first reaches the 2000 EUR threshold, due diligence is to be refreshed whenever the customer deposits or withdraws 2000 EUR in one transaction or in a series of linked transactions. As above, for the purpose of being linked, Riotech N.V. considers transactions to be linked when cumulatively, they amount to 2000 EUR within a 24-hour period.

At this stage, EDD would previously have been performed, it is therefore necessary to review the customer file with consideration to financial crime risks and safer gambling.

Again, the on-going appropriateness of the customer's risk profile should also be considered, including whether to move the customer to high-risk, introduce additional limits, or closure of the account.

Customers should be moved from medium risk to high risk, when following review, they are considered to pose a risk of gambling harm – this is determined by whether or not any safer gambling tools are employed.

Alternatively, the account is closed due to the level of gambling harm posed, or due to financial crime risk resulting in the submission of a SAR.

10.

VIEWING A CUSTOMER FILE

Riotech N.V. is required to conduct event-driven reviews of customer relationships (such as those in section 9 above), and periodic reviews of all customer relationships. This involves conducting a review of the customer's activity and refreshing due diligence.

Periodic reviews are limited to customers whose accounts remain active.

10.1 Periodic review frequency and due dates

The risk profile of a customer determines the frequency of periodic reviews:

Risk Rating	Frequency
Low Risk	Every 3 years
Medium Risk	Every 2 years
High Risk	Annually

On a monthly basis, a report must be run to identify which customers are due a periodic review. It is important not to confuse customer registration date with the onboarding date, the latter is the date that should be used. The customer relationships must then be reviewed as below.

10.2 Low risk customer review

- Re-verify the customer using SEON. This is to check that the customer's name still matches the address they registered with. Where there is a discrepancy, the customer should be contacted to verify current address, together with proof of address. This should be checked through SEON also.
- If there is a flag in SEON, perform EDD and review accordingly, in accordance with section 6.3.
- Check the history on the account. This includes any previous correspondence and their play, deposit and withdrawal history.

When doing so, consider:

- Scrutiny of transactions undertaken throughout the course of the relationship, including review of any transaction monitoring alerts for the customer.
- Assessing whether there is a risk of money laundering or terrorist financing, factors to consider include:
 - Whether the customer transacts with significant amounts of cash (if over 2000 EUR, the customer's risk profile is incorrect, see section 9 above);
 - Does documentation appear false, forged or stolen (verification should have been performed at the start of the relationship, but the validity of documents should again be considered during the review);
 - Indicators that the customer operates with multiple gambling operators, particularly where this is across multiple geographical areas;
 - Inconsistencies in the declared salary / income with the amount be gambled;
 - Are sums being deposited with little or none used for gambling, before it is withdrawn;
 - Are they betting in arbitrage, so as to never lose (e.g. equal amounts on both red and black in roulette);
 - Attempts to withdraw sums to a different bank account from which the deposit was made;

- Theft of employer / company money to fund gambling – as such, illegitimate funds are being used;
- Any linked accounts indicating possible mule accounts, i.e. are there accounts for other people all linked to one address; and
- Possible connections to jurisdictions that are considered high-risk for the purpose of money laundering and terrorist financing.

Assessing whether there is a risk of gambling harm, factors to consider include:

- Affordability issues, such as inconsistencies in the declared salary / income with the amount be gambled;
- Information / statements indicating that the customer is experiencing financial difficulties;
- Betting behaviour, such as:
 - The frequency of activity;
 - Length of gaming sessions;
 - Times at which the customer games (i.e. unsociable hours at night); and
 - Chasing losses, like increasing size of individual bets, and erratic betting patterns or increased size of 'in-play' bets following losses.
- Withdrawal behaviour, frequency and number of cancelled withdrawals;
- Limits placed by the customer and related activity, does the customer keep slowly upping the limits, this may indicate the customer is not in control;
- Has the customer self-excluded since being on-boarded or since the last review;
- Theft of employer / company money to fund gambling – as such, illegitimate funds are being used so consider money laundering also;
- Customer-led interaction, such as wellbeing comments, indicators gambling is being used as a source of income or complaints about losing money; and
- Vulnerability, such as cognitive impairment or bereavement.

- Any inconsistencies or concerns should give rise to EDD checks:
 - Safer Gambling Questionnaire;
 - Source of Funds / Source of Wealth Questionnaire; and
 - Any other checks, such as adverse media that are deemed appropriate given the results of the review.

For concerns with gambling harm, appropriate customer interaction should occur, and support offered. Customers should also be referred to safer gambling tools. The customer's risk profile should also change to high. Where the harm is considered to be severe, such as the customer seems to have no control over their activity, the account should be closed.

For concerns regarding potential money laundering, this should be escalated to the MLRO for review. Customers for whom a SAR is submitted should have their account closed, in accordance with the Escalation Procedures.

Once you have concluded the review, complete the Review Checklist at Appendix 4. Where the customer's risk profile is deemed to have changed, ensure this is actioned and documented in the Checklist.

10.3 Medium and high-risk customer review

A review of a customer that is of medium or high risk requires:

- Re-verify the customer using SEON. This is to check that the customer's name still matches the address they registered with. Where there is a discrepancy, the customer should be contacted to verify current address, together with proof of address. This should be checked through SEON also.
- If there is a flag in SEON, perform EDD and review accordingly, in accordance with section 6.3.
- If there has previously been a flag in SEON, consider whether the flag still has an impact on the account. For example, does the customer still have PEP status.
- Review the EDD information and questionnaires.
- Check the history on the account. This includes any previous correspondence and their play, deposit and withdrawal history.

When doing so, consider:

- Scrutiny of transactions undertaken throughout the course of the relationship, including review of any transaction monitoring alerts for the customer.
- Assessing whether there is a risk of money laundering or terrorist financing, factors to consider include:
 - Whether the customer transacts with significant amounts of cash (if over 2000 EUR, the customer's risk profile is incorrect, see section 9 above);
 - Does documentation appear false, forged or stolen (verification should have been performed at the start of the relationship, but the validity of documents should again be considered during the review);
 - Indicators that the customer operates with multiple gambling operators, particularly where this is across multiple geographical areas;
 - Inconsistencies in the declared salary / income with the amount be gambled;
 - Are sums being deposited with little or none used for gambling, before it is withdrawn;
 - Are they betting in arbitrage, so as to never lose (e.g. equal amounts on both red and black in roulette);
 - Attempts to withdraw sums to a different bank account from which the deposit was made;
 - Theft of employer / company money to fund gambling – as such, illegitimate funds are being used;
 - Any linked accounts indicating possible mule accounts, i.e. are there accounts for other people all linked to one address; and
 - Possible connections to jurisdictions that are considered high-risk for the purpose of money laundering and terrorist financing.

Assessing whether there is a risk of gambling harm, factors to consider include:

- Affordability issues, such as inconsistencies in the declared salary / income with the amount be gambled;
- Information / statements indicating that the customer is experiencing financial difficulties;
- Betting behaviour, such as:

- The frequency of activity;
 - Length of gaming sessions;
 - Times at which the customer games (i.e. unsociable hours at night); and
 - Chasing losses, like increasing size of individual bets, and erratic betting patterns or increased size of 'in-play' bets following losses.
 - Withdrawal behaviour, frequency and number of cancelled withdrawals;
 - Limits placed by the customer and related activity, does the customer keep slowly upping the limits, this may indicate the customer is not in control;
 - Has the customer self-excluded since being on-boarded or since the last review;
 - Theft of employer / company money to fund gambling – as such, illegitimate funds are being used so consider money laundering also;
 - Customer-led interaction, such as wellbeing comments, indicators gambling is being used as a source of income or complaints about losing money; and
 - Vulnerability, such as cognitive impairment or bereavement.
- Any inconsistencies or concerns should give rise to refreshed EDD:
 - Resend the Safer Gambling Questionnaire;
 - Re-send the Source of Wealth / Source of Funds Questionnaire; and
 - Any other checks, such as adverse media that are deemed appropriate given the results of the review.

For concerns with gambling harm, appropriate customer interaction should occur, and support offered. Customers should also be referred to safer gambling tools. The customer's risk profile should also change to high. Where the harm is considered to be severe, such as the customer seems to have no control over their activity, the account should be closed.

For concerns regarding potential money laundering, this should be escalated to the MLRO for review. Customers for whom a SAR is submitted should have their account closed, in accordance with the Escalation Procedures.

- Once you have concluded the review, complete the Review Checklist at Appendix 5. Where the customer's risk profile is deemed to have changed, ensure this is actioned and documented in the Checklist.

10.4 Escalations from the First Line of Defence

All customer gaming activity is reviewed as part of Riotech N.V.'s on-going monitoring. This is performed by the first line of defence, and referred to the financial crime team when necessary.

When a customer is referred to the financial crime team for review, the customer's file must be reviewed depending on the customer's risk profile.

11.

ORMANT ACCOUNTS

A customer account is considered dormant when there has been no activity for a period of 12 months. To clarify, this means, in the preceding 12 months, the customer has not:

- Played / wagered in any games; or
- Made a deposit.

A dormant account check is performed on a monthly basis. This entails running a monthly inactivity report.

Dormant accounts are to be closed and a notification sent to the customer, that the account has been closed due to inactivity for 12 months.

Customers are able to reactivate their accounts, but must undergo the CDD procedure beforehand.

12.

SCALATION PROCEDURES

All escalations must be accompanied by a rationale, including any concerns that also pertain to responsible gambling.

When reviewing the escalation, all of the following must be considered:

- Scrutiny of transactions undertaken throughout the course of the relationship, including review of any transaction monitoring alerts for the customer.
- Assessing whether there is a risk of money laundering or terrorist financing, factors to consider include:
 - Whether the customer transacts with significant amounts of cash;
 - Does any of the provided documentation appear false, forged or stolen;
 - Indicators that the customer operates with multiple gambling operators, particularly where this is across multiple geographical areas;
 - Inconsistencies in the declared salary / income with the amount be gambled;
 - Are sums being deposited with little or none used for gambling, before it is withdrawn;
 - Are they betting in arbitrage, so as to never lose (e.g. equal amounts on both red and black in roulette);
 - Attempts to withdraw sums to a different bank account from which the deposit was made;
 - Theft of employer / company money to fund gambling – as such, illegitimate funds are being used;
 - Any linked accounts indicating possible mule accounts, i.e. are there accounts for other people all linked to one address; and
 - Possible connections to jurisdictions that are considered high-risk for the purpose of money laundering and terrorist financing.

Consideration should also be given to whether there is fact, or also, a gambling harm issue.

- Assessing whether there is a risk of gambling harm, factors to consider include:
 - Affordability issues, such as inconsistencies in the declared salary / income with the amount be gambled;

- Information / statements indicating that the customer is experiencing financial difficulties;
- Betting behaviour;
- Withdrawal behaviour, frequency and number of cancelled withdrawals;
- Limits placed by the customer and related activity, does the customer keep slowly upping the limits, this may indicate the customer is not in control;
- Has the customer self-excluded since being on-boarded or since the last review;
- Play indicators, such as chasing losses and erratic betting patterns;
- Theft of employer / company money to fund gambling – as such, illegitimate funds are being used so consider money laundering also;
- Customer-led interaction, such as wellbeing comments, indicators gambling is being used as a source of income or complaints about losing money; and
- Vulnerability, such as cognitive impairment or bereavement.

If in conclusion, there is a suspicion of potential money laundering or terrorist financing, an SAR must be promptly prepared, either by the MLRO or provided to the MLRO for review, in accordance with the template at Appendix 6.

Once the MLRO has completed their review, they will decide whether or not a SAR should be submitted to the FIU. The MLRO is responsible for submitting the SAR, or instructing a delegate to do so.

All escalated customers must have their risk rating reassessed and documented accordingly.

12.1 SAR Log

All escalations to the MLRO, irrespective of whether they result in a SAR to the FIU, must be recorded on the SAR Log. All applicable columns are to be populated.

12.2 Account closure

Following the submission of a SAR, a customer's account can be permanently closed. The fact a SAR has been submitted should not be placed on the customer account as this source is open to all lines of defence, nor must the same be communicated to the first line of defence.

13. SUSPICIOUS ACTIVITY REPORTING POLICY

13.1 Reporting Obligations

Riotech N.V. is obligated to submit a Suspicious Activity Report (SAR) to the FIU Curaçao for any unusual or suspicious activity. This includes activity that provides reasonable grounds to suspect involvement in ML, TF, or other financial crimes. The submission of SARs aids in the freezing of assets and supports the investigation of financial crimes.

13.2 Indicators of Unusual Transactions

The following indicators may trigger internal reporting and further investigation:

- Transactions reported to police or judicial authorities as potentially linked to ML/TF.
- Intended transactions involving natural or legal persons listed on UN or EU Sanctions lists.
- Transactions equal to or exceeding EUR 2,500, including:
 - Bank transactions.
 - Sale of chips or credits.
 - Payment of prizes.
- Any transaction that suggests possible ML or TF involvement, such as:
 - Establishing multiple betting accounts with deposits below the reporting threshold, followed by rapid withdrawals.
 - Regularly depositing or transacting similar cash amounts.
 - Funding accounts with various payment methods (e.g., credit cards, prepaid cards, checks, cryptocurrency) followed by payout requests.
 - Unexplained income inconsistent with the customer's financial situation or profile.
 - Claiming machine credits/payouts without a jackpot.
 - Associations with multiple accounts under different names.
 - Frequent betting transactions or cash deposits/withdrawals just below reporting thresholds.

13.3 Reporting Procedures

- **Internal Reporting:** Employees must report unusual or suspicious activities to the Compliance Officer within 24 hours of identification.
- **Compliance Officer Review:** The Compliance Officer will conduct relevant research and due diligence within 10 working days of receiving the report.
- **External Reporting:** If the Compliance Officer determines that the transaction presents a reasonable presumption of ML/TF, they must report it to the FIU within 48 hours.
- **Submission Method:** SARs must be submitted via the GoAML portal at <https://portal.fiucuracao.cw> in English.

13.4 Compliance and Review

This policy will be reviewed periodically to ensure continued compliance with applicable laws and regulations. Employees are required to familiarize themselves with this policy and adhere to its provisions.

14. BUSINESS RISK ASSESSMENT

This Business Risk Assessment (BRA) is designed to identify, assess, and mitigate risks associated with Money Laundering (ML), Terrorist Financing (TF), and Proliferation Financing (PF) within Riotech N.V., an online gaming company. This BRA aligns with regulatory requirements and industry best practices to ensure compliance and maintain the integrity of our operations.

14.1. Identification of Risks

14.1.1. Money Laundering (ML) Risks

- **Transaction Volume and Value:** High volume and value transactions typical in online gaming present significant ML risks.
- **Customer Base:** The global reach of online gaming platforms increases exposure to customers from high-risk jurisdictions.
- **Payment Methods:** The use of various payment methods, including cryptocurrencies, increases the risk of ML.

14.1.2 Terrorist Financing (TF) Risks

- **Geographic Exposure:** Operations in or interactions with customers from jurisdictions known for terrorism financing.
- **Anonymous Transactions:** The potential for anonymous or pseudonymous transactions can conceal the true identity of customers.

14.1.3 Proliferation Financing (PF) Risks

- **Product and Service Offerings:** The nature of gaming services may be exploited for PF, especially when involving high-risk jurisdictions.
- **Customer Demographics:** The diverse customer base may include individuals or entities connected to PF activities.

14.2. Risk Assessment

14.2.1 Money Laundering (ML)

- **Likelihood:** High, due to the nature of the business and the high volume of transactions.
- **Impact:** Severe, given the potential regulatory fines, reputational damage, and operational disruptions.

14.2.2 Terrorist Financing (TF)

- **Likelihood:** Medium, with a higher likelihood in regions with known TF activities.
- **Impact:** Severe, considering the legal implications and potential for regulatory sanctions.

14.2.3 Proliferation Financing (PF)

- **Likelihood:** Low to Medium, dependent on the company's engagement with high-risk jurisdictions.
- **Impact:** High, particularly concerning regulatory compliance and international sanctions.

14.3. Mitigation Measures

14.3.1 Enhanced Due Diligence (EDD)

- Implement EDD procedures for customers from high-risk jurisdictions or with high transaction volumes.
- Conduct regular reviews of customer profiles and transactions to identify unusual or suspicious activities.

14.3.2 Transaction Monitoring

- Employ advanced transaction monitoring systems to detect suspicious activities in real-time.
- Regularly update the monitoring system to incorporate new ML/TF/PF typologies and regulatory changes.

14.3.3 Employee Training and Awareness

- Provide ongoing training for employees on recognizing and reporting ML/TF/PF risks.
- Ensure staff are aware of the latest regulatory requirements and internal policies related to risk management.

14.3.4 Reporting and Record Keeping

- Maintain comprehensive records of all customer interactions, transactions, and due diligence efforts.
- Establish clear procedures for reporting suspicious activities to the relevant authorities in a timely manner.

14.3.5 Regular Risk Assessments

- Conduct regular assessments of the company's risk exposure to ML/TF/PF, adjusting policies and procedures as necessary.
- Engage external experts periodically to review and enhance the BRA framework

14.4. Risk Appetite

14.4.1 Defining Risk Appetite

Riotech N.V. establishes a clear risk appetite framework to determine the level of risk it is willing to accept in its business operations. The risk appetite is aligned with the company's strategic goals, regulatory obligations, and ethical standards.

14.4.2 Tolerance Levels for ML/TF/PF Risks

- **Low Risk Appetite:** The company has a low tolerance for risks related to non-compliance with anti-money laundering (AML), counter-terrorist financing (CTF), and anti-proliferation financing (APF) regulations. Strict measures are in place to prevent and mitigate these risks.
- **Medium Risk Appetite:** The company may accept moderate risks associated with new markets or customer segments, provided robust controls and monitoring systems are in place.

- **High Risk Appetite:** The company is unwilling to engage in high-risk activities that could significantly impact its reputation, legal standing, or financial stability.

14.4.3 Aligning Risk Appetite with Business Strategy

The risk appetite is integrated into the decision-making processes across the organization. This ensures that the company's strategic initiatives are pursued within acceptable risk boundaries, particularly concerning ML, TF, and PF.

14.4.4 Risk Appetite Review and Monitoring

The risk appetite is reviewed annually or whenever significant changes occur in the business environment. The Board of Directors and senior management are responsible for ensuring that the company's risk appetite remains aligned with its evolving risk profile and regulatory requirements.

15. SUPPLIER POLICY

Riotech N.V. (the Company) is committed to working with suppliers to ensure that its business activities are not interrupted and that high standards are maintained. The Company is committed to being a responsible and valuable partner in the supply chain, continuing to build a sustainable business that serves its customers, employees and the communities we operate in, as set out in this Supplier Policy ('the Policy').

The purpose of this Policy is to describe the Company's approach to engaging suppliers and applies to all members of staff at Riotech N.V. Although the Company performs most of the services needed – some services are required due to lower costs, greater expertise, economies of scale or freeing up internal human resources for core functions of Riotech N.V.

The Policy should be read in conjunction with relevant procedures and guidelines for your role. If you are uncertain what action you should take or think you cannot comply with the Policy, or understand anything in it, you must speak with the Director without delay. Ignorance or misunderstanding of the Policy (and any procedures you have been provided with) will not be an acceptable excuse for failure to comply.

Failure to comply with the Policy could bring financial and reputational damage to the Company, including regulatory censure, fines and enforcement action. It could also result in disciplinary action.

15.1. Suppliers Minimum Requirements

15.1.1 Business criticality

The Company undertakes all vital business operations internally and typically avoids outsourcing them. Before engaging with any suppliers, a thorough review is conducted to ensure that no crucial business activities will be outsourced and that anything deemed critical will remain internal.

15.1.2 Due Diligence

All suppliers expecting expenditure exceeding 5000 EUR must undergo due diligence. At a minimum, the following steps must be taken:

- Verification of the supplier's market presence;
- Confirmation of the supplier's registration as a company;
- Assurance of the supplier's compliance with relevant employment and human rights legislation;
- An open-source check.

Additional checks may be necessary as instructed by the Head of Legal Operations.

15.1.3 Review and approval

When engaging a supplier, it is important to review the conditions, services and suitability of the service provider to ensure there are no potential risks to the Company's information security and processes. In order to ensure this, this Policy together with the Service Level Agreement (SLA) in question will be reviewed by the authorized person (Head of Legal Operations) of the Company prior to approval and every year (if relationships are continuous) or on demand (if a new agreement is made or changed) thereafter.

The Company acknowledges that suppliers can present an additional risk to the overall business security and continuity, due to the additional layers while providing the main services of the Company. Such risks might arise from miscommunication, technical faults, attacks against the supplier, unforeseen disasters at the providers premises and so on. The Company takes into account such possibilities and ensures that the danger to business continuity or information security is minimised.

Before entering into an agreement with any service provider, the Company shall analyse the proposal and ensure that potential risks are controlled by the provider itself as well as evaluate the potential damage that can be done in case the provider fails to manage its risks.

If the scope of the services (ongoing or potential) falls out of the competences of the authorised person – this shall be brought up to an appropriate person within the Company

(Chief Financial Officer, Chief Technical Officer, Chief Operating Officer etc.) with adequate understanding of the service and potential risks in question. After determining possible risks (either by the authorised person or by the appropriate specialist within the Company) – only services that propose a tolerable level of potential risks shall be accepted/continued.

All service providers are obliged to comply with all relevant Information Security policies of the Company.

15.1.4 Standard clauses

Although the Company does not plan for any particular clauses that are mandatory for an SLA, it is expected that an SLA will clearly point out the safeguarding measures that ensure a continuous supply of the service in question, as well as provisions regarding what happens if the continuous supply of a service is interrupted.

Technical SLAs (e.g., the Data Center SLA) shall contain exact technical parameters of a service, in order to ensure technical data availability while performing audits, licensing checks, disaster recoveries etc.

15.1.5 Monitoring

The authorised person shall check for any changes (e.g., ownership, financial and operational) that could present risks to the Company or in any other way compromise its processes, security or reputation. This is done to ensure that the service is provided in a fit and proper manner, thus ensuring risk management and business continuity.

Particularly, the authorised person shall look for any essential ownership changes where the new owner has a previous history of relevant criminal charges, unlawful or irresponsible activities that might be deemed causing risk by the Company or by the Regulator. This shall be monitored by overviewing official freely available information.

Additionally, the authorised person shall check the suitability of the service provider, evaluating the competences, capabilities and overall technical fitness to provide the service in question without creating any additional risks to the Company. This might be done by direct communication with potential service providers or by overviewing the provider's current/valid documentation of proof (e.g., ISO certificates).

Finally, the financial stability of the service provider shall be checked, to ensure that the provider has adequate financial security to ensure continuous provision of agreed services. This is done by overviewing the providers yearly financial reports as well as analysing publicly available information about the provider.

These monitoring checks shall be done together with the yearly revision of any SLA agreement or, if there is any reason to believe it is needed sooner, on demand by any Regulator or the Company's own initiative.

15.2. Governance, Review

The Director is responsible for supervising the Company's compliance framework, which encompasses this policy. The Head of Legal Operations has primary responsibility for the day-to-day operation and effectiveness of Riotech N.V.'s supplier engagement within the compliance framework.

16. RECORD KEEPING POLICY

16.1 Purpose

The purpose of record-keeping is to ensure that there is an audit trail that could assist in any financial investigation by a law enforcement body. These records are also important for when the Regulator is conducting an investigation for compliance purposes.

Where record-keeping obligations are not observed, Riotech N.V. may be subject to prosecution, regulatory sanctions, or disciplinary enforcement.

16.2 Retention Period and Requirement

The record-keeping retention period is five years.

The type of information Riotech N.V. is required to maintain as a remote gambling operator is:

- Details of how compliance has been monitored;
- Delegation of compliance activities;
- Reports and management information to senior management;
- Information or other material concerning possible money laundering or terrorist financing not acted upon by the MLRO, with reasoning why no further action was taken;
- Customer identification and verification information;
- Supporting records in respect of customer relationships and due diligence (including record of all the attempts made to get the necessary information and documentation during CDD and/or EDD) ;
- Customer deposit, withdrawal and gambling history;

- Monitoring of customer activity and reviews;
- Employee training records;
- Internal and external suspicious activity reporting (SARs), including decisions and actions taken; and
- Contact between the Company and law enforcement or the Regulator.

Employees of Riotech N.V. must ensure all records are saved on Riotech N.V. servers, and not on personal drives.

16.3 Expiry of Retention Period

Upon expiry of the five-year retention period, personal data must be deleted unless:

- Riotech N.V. is required to retain records by law for other purposes, such as due to regulatory review or investigation, or legal proceedings;
- There are reasonable grounds to believe that records contain data that need to be retained for the purpose of legal proceedings; or
- The subject of the data has agreed to the retention of the data for longer (this would be unusual and would need the rationale for requesting longer retention).

To clarify, the expiry for the five-year retention period for customers, is from the date the relationship ended.

17. MLRO CONTACT DETAILS

The MLRO at Riotech N.V. is Maksym Fedorenko, MLRO. Email: compliance.dept@riobet.com.

Appendix 1 – Safer Gambling Questionnaire

SAFER GAMBLING QUESTIONNAIRE	
Question	Notes
What are your motivations to gamble?	Any answer that is not “for fun” or “for personal enjoyment”, in particular any answer that suggest gambling to pay debts, supplement or be an income, chase losses, indicated possible gambling harm
How many times in the past year have you borrowed to gamble?	Any answer except “none” or “zero” is a risk
How often do you wake up at night to gamble?	Any answer except “never” is a risk
Do you play on your own behalf or on behalf of any third party? Playing on behalf of your own means that you are playing using your own funds, and any profit gained from the gambling remain yours. Playing on behalf of a third party means that you are using funds provided by someone else with the purpose to gamble and share the profit with this person	Any answer except “on my own” or similar is a risk
How many times in the past year have you “timed out” or self-excluded from other on-line gambling operators?	Any answer except “none” or “zero” is a risk
What other online gambling sites do you use frequently?	A long list (5 or more) is a possible sign of problem gambling and maybe indicative of someone who has been suspended by other operators.
Would you like to set a daily/weekly/or monthly deposit limit?	No risk factors but if the answer is “yes”, then discuss with the customer around what limit they would like to set.

	Depending on the nature of the customer's other answer, it may be prudent to simply apply limits, even when not requested.
How much money can you afford to gamble each week?	Consider veracity, e.g. do bank statements show funding levels that far exceeds the customer's declared/known income and/or amount being wagered. Are there often large and irregular payments being made into an account? Does the customer appear to be in debt or suffering financial hardship (and is perhaps turning to gambling for income)? Is additional documentation needed to support customer spend?

Appendix 2 – Source of Funds / Source of Wealth Questionnaire

SOURCE OF FUNDS / SOURCE OF WEALTH	
Occupation	
Annual Salary	Is this in line with income specified at registration
Other Source of Income (please specify) Rental Income Pension Stock/shares/investments/dividends Other gambling operators	The use of gambling as an income is a flag for gambling harm.
Other Sources of Wealth (please specify) Sales of property Sale of other assets (own business) Inheritance Gifts Borrowings Insurance pay out Lump sum from pension	Borrowing is a flag for gambling harm
Please upload supporting documentation, such as payslips or bank statements. These must be no older than 3 months.	Consider veracity, e.g. do bank statements show funding levels that far exceeds the customer's declared/known income and/or amount being wagered. Are there often large and irregular payments being made into an account? Is additional documentation needed to support customer spend?

Appendix 3 – EDD Checklist

ENHANCED DUE DILIGENCE CHECKLIST	
EDD performed by	Name of AML analyst
Registration Date	
Customer name	
Customer reference	
Identification reverified	Yes / No Any comments
Any screening hits (e.g. PEP, sanction etc.)	If yes, specify
Adverse media check (not mandatory for medium risk customers)	Yes / No
If applicable, any negative news	If yes, specify
4 eye-review	Name of an analyst
Any other comments	
Onboarded	Yes / No (if rejected)
Onboarding / rejection date	
Customer risk profile	Medium / High

Appendix 4 – Low Risk Customer Review Checklist

LOW RISK CUSTOMER REVIEW CHECKLIST	
Review performed by	Name of an analyst
Onboarding date	
Customer name	
Customer reference	
Review due date	
Identification and verification refreshed	Yes / No Any comments
Any screening hits (e.g. PEP, sanction etc.)	If yes, specify
Account history reviewed	Yes / No
Any financial crime or gambling harm risks identified?	Yes / No If yes, specify and complete EDD
Adverse media check	Yes / No
If applicable, any negative news	If yes, specify
Safer gambling questionnaire	Yes / No Any comments
Source of Wealth / Source of Funds Questionnaire	Yes / No Any comments
4 eye-review	Name of an analyst
Any other comments	E.g. the application of limits to the account.
Date of review	
Customer risk profile following review	Low / Medium / High / Closed

Appendix 5 – Medium / High Risk Customer Review Checklist

MEDIUM / HIGH RISK CUSTOMER REVIEW CHECKLIST	
Review performed by	Name of an analyst
Onboarding date	
Customer name	
Customer reference	
Current customer risk profile	Low / Medium / High
Review due date	
Identification and verification refreshed	Yes / No Any comments
Any screening hits (e.g. PEP, sanction etc.)	If yes, specify
Account history reviewed	Yes / No
Any financial crime or gambling harm risks identified?	Yes / No If yes, specify
Adverse media check (not mandatory for medium risk customers)	Yes / No
If applicable, any negative news	If yes, specify
Safer gambling questionnaire – reviewed / refreshed	Yes / No Comments
Source of Wealth / Source of Funds Questionnaire	Yes / No Comments
4 eye-review	Name of an analyst
Any other comments	
Date of review	
Customer risk profile following review	Low / Medium / High / Closed

Appendix 6 – SAR Report

This is an internal suspicious activity report on [NAME] following concerns that the funds used to deposit into [his/her] online gaming account may be criminal property.

Account Information:

Account ID:	
Login:	
Name:	
Date of Birth:	
E-mail:	
Address:	
Account Registration Date:	
Deposits:	
Winnings:	

FACTUAL BACKGROUND (DO NOT INCLUDE OPINIONS HERE, FACTS ONLY)

Reasons for suspicion:
(RATIONALE / REASONS FOR SUSPICION INCLUDED HERE)

Appendix 7 – High-risk products, services and payment methods

This is a list of products, services and payment methods that are considered as high-risk by Riotech N.V.

No	Name of product	Comment
1	Crypto wallets	
2	Prepaid cards	

No	Name of service	Comment

No	Name of payment method	Comment