

ORAKUM N.V.

CUSTOMER ACCEPTANCE (KYC) POLICY

APPROVED BY THE BOARD OF DIRECTORS

YELOVATSKYI SERHII / DIRECTOR

A handwritten signature in blue ink, appearing to be 'S. Yelovatskyi', written over a horizontal line.

EFFECTIVE DATE: 29.07.2026

NEXT REVIEW: 28.07.2027

1. STATEMENT OF THE POLICY

Orakum N.V., a company incorporated under the laws of Curaçao with Company Number 141651, registred at Abraham Mendez Chumaceiro Boulevard 03, Willemstad, 4750, Curacao, and licensed by the Curaçao Gaming Authority to offer games of chance under license number OGL/2024/586/0786, has adopted this Customer Acceptance Policy to define the principles, procedures, and standards that govern the approval of customers using its online gaming and betting platform. The purpose of the policy is to protect the company from being exploited for money laundering, terrorist or proliferation financing, sanctions evasion, fraud, or other unlawful activities. It also ensures strict compliance with Curaçao's legal and regulatory framework, including the National Ordinance on Identification when Rendering Services (NOIS), the National Ordinance on the Reporting of Unusual Transactions (NORUT), the Sanctions National Ordinance (SNO), the Kingdom Sanction Act, and the National Ordinance on Games of Chance (LOK).

The policy is aligned with the guidance of the Curaçao Gaming Control Board and is embedded within Orakum N.V.'s broader Anti-Money Laundering (AML), Counter-Terrorist Financing (CTF), and Counter-Proliferation Financing (CPF) program. It also incorporates recognised international standards such as the recommendations of the Financial Action Task Force (FATF) and the European Union's Anti-Money Laundering Directives.

This policy applies to all directors, officers, employees, contractors, and third parties involved in onboarding and customer verification. No customer may deposit, withdraw, or engage in gaming activities until all acceptance requirements have been fulfilled and mandatory verification and screening procedures have been completed.

2. SCOPE OF THE POLICY

This Customer Acceptance Policy applies to all individuals or entities registering an account with Orakum N.V., regardless of the channel through which registration takes place. This includes direct sign-ups through the company's official website, mobile applications, affiliate arrangements, or third-party integrations.

The scope covers the full customer lifecycle, starting from the initial application and extending through account use until closure or termination. It applies to all products and services offered by Orakum N.V. under its Curaçao gaming licence OGL/2024/586/0786.

3. COMPLIANCE WITH CURAÇAO'S LEGAL FRAMEWORK

Orakum N.V. recognises that this Customer Acceptance Policy is an integral part of its wider Anti-Money Laundering (AML), Counter-Terrorist Financing (CTF), and Counter-Proliferation Financing (CPF) framework. The policy is designed to operate in full compliance with Curaçao's legislative and regulatory obligations, including the National Ordinance on Identification when Rendering Services (NOIS), the National Ordinance on the Reporting of Unusual Transactions (NORUT), the Sanctions National Ordinance (SNO), the Kingdom Sanction Act, and the National Ordinance on Games of Chance (LOK).

Meeting these obligations is considered a priority in the company's daily operations. Customer acceptance processes are fully embedded into the compliance framework to ensure that due diligence does not stop at onboarding but extends throughout the customer relationship. This enables the company to promptly detect and respond to any significant changes in a customer's risk profile, behaviour, or jurisdiction.

Employees engaged in customer onboarding and verification are required to complete specialised training that covers Curaçao's legislative framework and the company's internal compliance policies. Training focuses on the practical application of the Risk-Based Approach, identifying and escalating high-risk indicators, and adhering to escalation procedures to the Compliance Officer or senior management.

In addition, Orakum N.V. commissions independent audits at least annually to evaluate the effectiveness of the Risk-Based Approach and the practical enforcement of this policy. These reviews assess key areas including identity verification, sanctions and PEP screening, Enhanced Due Diligence (EDD), and the ongoing monitoring of customer activity. The results are reported to the Board of Directors, and any deficiencies are addressed through corrective actions within agreed timelines to ensure continuous compliance and operational resilience.

4. CUSTOMER ACCEPTANCE

Orakum N.V. accepts only those customers who fully comply with all legal, regulatory, and internal requirements. Every applicant must be verified to confirm they meet the minimum legal gambling age, which is eighteen (18) years or higher where required by the laws of their country of residence. Applicants must also provide accurate and verifiable personal information, including their full legal name, date and place of birth, nationality, and current residential address.

The company does not allow the onboarding of customers who are resident in, accessing services from, or conducting transactions in jurisdictions restricted under Curaçao's legislation, international sanctions regimes, or Orakum N.V.'s own list of prohibited jurisdictions. As part of the verification process, all applicants are screened against international and domestic sanctions lists, including those issued by the United Nations, the European Union, the U.S. Office of Foreign Assets Control (OFAC), the U.K. Office of Financial Sanctions Implementation (OFSI), the Sanctions National Ordinance, the Kingdom Sanction Act, and any applicable lists maintained by the Curaçao Gaming Control Board.

All funds used for betting or gaming must be derived from legitimate and lawful sources. Where a customer presents an elevated risk, additional documentation may be required to confirm the origin of funds and, when applicable, the source of wealth. Orakum N.V. also reserves the right to deny services to individuals or entities with a history of fraud, chargebacks, bonus abuse, regulatory violations, or self-exclusion due to gambling-related issues.

5. APPLICATION OF THE RISK-BASED APPROACH

Orakum N.V. applies a structured Risk-Based Approach (RBA) during both the onboarding process and throughout the ongoing relationship with each customer. This approach ensures that the level of due diligence is proportionate to the customer's specific risk profile.

In assessing risk, the company considers multiple factors, including the customer's personal and financial background, the types of products and services being accessed, geographic connections, and the risks associated with the technologies or channels used to engage with the platform.

5.1 Customer Profile Risks

Orakum N.V. conducts a detailed evaluation of each prospective customer to determine their exposure to risks such as money laundering, terrorist financing, or proliferation financing. This ensures that the level of due diligence applied matches the customer's overall risk classification.

Low-risk customers are those who present a transparent and well-documented source of income, maintain stable employment in low-risk industries, and show betting or transaction activity that is consistent with their declared financial circumstances.

Medium-risk customers are classified as such when certain elevated factors are present, though not severe enough to meet the high-risk threshold. Examples include income that is legitimate but harder to verify, employment in industries with moderate exposure to AML/CTF risks, or occasional discrepancies between declared income and observed activity. These customers are subject to standard CDD with additional verification and closer oversight.

High-risk customers are identified where factors such as multiple or unclear income streams, employment in sectors with heightened AML exposure (such as cryptocurrency or unregulated financial services), activity inconsistent with declared income, or classification as Politically Exposed Persons (PEPs), including their family members and close associates, are present. Such customers must undergo Enhanced Due Diligence (EDD), which involves deeper verification, extra documentation, and continuous monitoring.

Key triggers for enhanced review include:

- Customers with multiple sources of income, who must provide documentation for each, such as paylips, tax filings, business records, or investment statements.
- Cases of irregular or seasonal income, which require confirmation of lawful origin and ongoing monitoring for unusual activity.
- PEPs and their associates, who are automatically treated as high risk, requiring senior management approval, comprehensive checks on both source of funds and wealth, and continuous monitoring.
- Customers engaging in unusually large or frequent betting, who must prove their funds are legitimate, supported by income or bank statements.
- Spending that appears disproportionate to declared income, which prompts additional checks and supporting documentation.
- Sudden, unexplained spikes in betting behaviour, particularly among casual or tourist players, which lead to reclassification and closer oversight.
- The use of third parties to deposit, gamble, or withdraw funds, which results in immediate investigation and verification of all involved parties.
- Attempts to operate multiple accounts, which are flagged as suspicious, consolidated, and subject to full review.
- Redemption of significant chip volumes without verifiable gambling history, which requires full identity and source-of-funds checks before processing.
- Customers linked to junket operators, who are automatically treated as high risk, with EDD applied to both the individual and the operator, including a full review of financial structures and funding sources.

5.2 Geographic Risks

Orakum N.V. uses a structured geographic risk framework to evaluate potential risks linked to the customer's country of residence or the origin of their funds. This framework is regularly updated using internationally recognised sources, including Financial Action Task Force (FATF) public statements, advisories issued by the Caribbean Financial Action Task Force (CFATF), the European Commission's list of high-risk third countries, sanctions lists maintained by the U.S. Office of Foreign Assets Control (OFAC), the U.S. Department of State's International Narcotics Control Strategy Reports, and Transparency International's Corruption Perceptions Index.

Customers from sanctioned jurisdictions are strictly prohibited. Clients from high-risk jurisdictions may only be accepted after Enhanced Due Diligence (EDD) has been completed and formally approved by senior compliance officers.

A jurisdiction is classified as high risk where one or more of the following apply: weak or ineffective AML/CFT frameworks and limited enforcement capacity, systemic corruption that heightens the likelihood of illicit funds entering the platform, international sanctions tied to terrorism, proliferation of weapons of mass destruction, or other criminal activities, and the presence of or links to terrorist organisations. In such cases, customers must provide extensive evidence verifying both the source of funds and source of wealth, and their accounts are subject to strict and continuous monitoring. Exceptional cases require explicit senior management approval alongside comprehensive EDD measures.

To ensure the reliability of its assessments, Orakum N.V. refers to authoritative and regularly updated sources, such as FATF's lists of high-risk and monitored jurisdictions, CFATF public statements, European Commission AML/CFT deficiency lists, OFAC sanctions databases, annual U.S. State Department reports, Transparency International corruption indices, and other credible reports concerning countries associated with terrorist financing or harbouring terrorist entities.

If a customer's country of residence or funding source is flagged as high risk or sanctioned, their application is escalated to the Compliance Officer. Should onboarding proceed, EDD becomes mandatory and includes detailed identity verification, an in-depth review of sources of funds and wealth, and enhanced transaction monitoring throughout the business relationship.

5.3 Product, Service, and Transaction-Related Risks

A customer's risk classification is also shaped by the products, services, and transactions they use. Certain activities present higher inherent risks because they limit transparency and traceability. Examples include peer-to-peer transfers, purchasing or exchanging gaming tokens, or funding accounts through anonymous or semi-anonymous payment channels such as prepaid cards or certain cryptocurrencies.

Accounts that appear to be used primarily for financial movement rather than genuine gaming—for instance, large deposits followed by little or no play before withdrawal—are treated as high risk and subject to closer review. Similarly, the use of payment instruments not registered in the name of the account holder is flagged as suspicious and requires further verification.

Orakum N.V. identifies and addresses key risk factors in this category as outlined below:

Risk Factor	Description	Company Response
-------------	-------------	------------------

Proceeds of crime	Deposits may stem from illegal activities such as fraud, trafficking, or theft.	Customers must provide verifiable proof of lawful fund sources. Any suspicious transaction is reported to the FIU.
Anonymous payment methods	Prepaid cards, virtual assets, and other semi-anonymous channels pose traceability issues.	Apply Enhanced Due Diligence (EDD); origin of funds must be verified and documented.
Improper account use	Accounts used only for deposits and withdrawals without genuine gameplay.	Immediate review; accounts may be suspended pending investigation.
Third-party payments	Accounts funded with payment instruments not in the customer's name.	Both customer and third party are verified; relationship and legitimacy of funds confirmed.
Transfers between accounts	Moving funds between customer gaming accounts.	Generally prohibited; exceptions require Compliance Officer approval with full documentation.
Multiple accounts or wallets	Customers maintaining more than one account or wallet, including across platforms.	Internal systems detect and link accounts; activity is consolidated for review.
Frequent payment method changes	Repeated switching of bank accounts or payment instruments.	Detailed review triggered; EDD applied if necessary.
Identity fraud	Use of stolen identity or financial information to fund gaming.	Strong identity verification and document checks applied; suspected cases reported to authorities.
Electronic wallets	Providers based in weak jurisdictions or allowing anonymous deposits, which obscure fund flows.	Funding sources verified; provider licensing and regulatory oversight confirmed before approval.

5.4 Channel and Technology Risks

The way customers access Orakum N.V.'s services and the technologies used in the process play an important role in determining their risk profile. Remote onboarding is particularly sensitive, as it carries an elevated risk of impersonation or identity fraud. To address this, the company employs advanced

digital Know Your Customer (KYC) systems, including biometric verification, document authenticity checks, geolocation tools, and multi-factor authentication.

Prior to introducing any new technology, payment method, or platform feature, Orakum N.V. conducts a structured pre-launch risk assessment to confirm that it cannot be exploited for money laundering, terrorist financing, fraud, or other unlawful activity.

Certain scenarios require heightened safeguards:

- **Anonymous channels:** Methods of access that enable customers to remain anonymous are categorised as high risk. In such cases, stricter identification measures are enforced, including biometric verification, document validation, and real-time screening against sanctions and Politically Exposed Person (PEP) lists.
- **Remote interactions:** Although standard in the industry, remote onboarding still requires robust protection against impersonation and fraud. Orakum N.V. applies secure technologies such as biometric validation, liveness detection, and automated document verification during both onboarding and transactions.
- **Third-party involvement:** When customer interaction is facilitated by a third party, particularly if the intermediary is not subject to AML/CFT obligations, the risk level increases. The company therefore conducts due diligence on both the customer and the intermediary, confirming the intermediary's regulatory standing, assessing its AML/CFT framework, and verifying that all information is accurate, complete, and reliable.

5.5 Risk Indicators

Orakum N.V. applies a structured set of risk indicators to assess the overall exposure associated with each customer relationship. These indicators are central to the Risk-Based Approach (RBA) and help ensure that due diligence measures are applied in proportion to the level of risk identified.

Category	Examples of Risk Indicators	Company Response
Customer Profile	Multiple or irregular income sources; designation as Politically Exposed Person (PEP) or close associate; high or disproportionate spending; sudden unexplained spending increases; use of third parties; multiple accounts; chip redemptions without verifiable play; links to junket operators.	Apply risk-based due diligence ranging from additional verification to full Enhanced Due Diligence (EDD), depending on severity.
Products, Services & Transactions	Use of criminal proceeds; anonymous or unregulated payment methods; misuse of accounts; reliance on third-party funding; frequent payment method changes; identity fraud; use of prepaid cards; operation of multiple e-wallets.	Apply Standard CDD or escalate to EDD as required; block prohibited methods; report suspicious transactions to the Financial Intelligence Unit (FIU).

Geographic Risk	Customers located in jurisdictions with weak AML/CFT systems, systemic corruption, active sanctions, or terrorist links; jurisdictions flagged by FATF, CFATF, OFAC, or Transparency International.	Reject applicants from sanctioned jurisdictions; apply EDD and obtain senior management approval for high-risk countries; maintain continuous monitoring.
Channels & Technology	Access through anonymous methods; remote onboarding without effective safeguards; reliance on unregulated third-party intermediaries.	Strengthen verification by applying biometric checks, liveness detection, document validation, and multi-factor authentication.

6. ONBOARDING

Orakum N.V. applies a structured, compliance-focused onboarding process to ensure that only customers who meet the company's acceptance criteria are permitted access to its platform. No account is activated until all mandatory steps of identification, verification, and sanctions screening have been successfully completed.

6.1 Identification Requirements

Applicants must provide their full legal name, date and place of birth, nationality, current residential address, and an official identification number, such as a valid passport or national identity card.

6.2 Sanctions and PEP Screening

Every new applicant undergoes screening against international sanctions lists and Politically Exposed Person (PEP) databases. Automated tools are used to guarantee wide coverage, while all alerts or possible matches are carefully reviewed by compliance staff to confirm accuracy and eliminate false positives.

6.3 Enhanced Checks for High-Risk Customers

Where a customer is identified as high risk at the onboarding stage, additional verification requirements are enforced. These customers must submit documentation that demonstrates the lawful origin of their funds and, where relevant, their source of wealth. Acceptable evidence includes recent bank statements, company financial records, tax filings, property sale agreements, or investment account statements. These enhanced measures ensure that high-risk customers are subject to thorough vetting in line with both regulatory obligations and the company's internal standards, thereby protecting the platform from misuse.

7. ENHANCED DUE DILIGENCE

Orakum N.V. applies Enhanced Due Diligence (EDD) to customers who present a heightened risk profile. This group includes Politically Exposed Persons (PEPs), along with their family members and close associates, individuals residing in or funding accounts from high-risk jurisdictions, customers

conducting unusually large, complex, or unexplained transactions, and those whose financial activity does not align with their declared income or business background.

7.1 Measures and Verification

EDD involves a deeper level of scrutiny than standard due diligence. The process requires a thorough review of the customer's source of funds and source of wealth, supported by reliable and independent evidence. It may also include searches of public registries and corporate records to confirm beneficial ownership, verification of employment or business ownership, analysis of audited financial statements, and comprehensive adverse media and reputational checks across multiple credible sources.

7.2 Approval and Oversight

Onboarding any high-risk customer must be approved by senior management. In especially sensitive or complex cases, approval from the Board of Directors may also be required.

7.3 Monitoring after Onboarding

Customers accepted under EDD are subject to stricter monitoring measures once onboarded. These include lower thresholds for triggering transaction reviews, enhanced scrutiny of transaction activity, and more frequent risk profile reviews. Such measures ensure that high-risk customer relationships are closely supervised and remain consistent with both regulatory expectations and the company's internal compliance framework.

8. ONGOING MONITORING

Orakum N.V. recognises that customer acceptance is not confined to onboarding but requires continuous oversight. Ongoing monitoring ensures that customer activity remains consistent with the profile established at registration and that any anomalies are promptly detected and addressed.

8.1 Automated Monitoring of Transactions

The company uses automated systems to flag unusual or potentially suspicious activity. Alerts may be triggered by deposits or withdrawals inconsistent with the customer's declared profile, rapid transfers of funds without substantial gaming activity, reliance on multiple or unusual payment methods, or patterns indicative of collusion, chip-dumping, or other prohibited conduct. Each alert is reviewed by compliance staff, who assess the context and decide whether escalation or further investigation is appropriate.

8.2 Periodic Reviews and Risk Reassessment

In addition to real-time monitoring, Orakum N.V. conducts periodic reviews of customer profiles in line with their assessed risk level. These reviews ensure classifications remain accurate and reflective of the customer's behaviour. Material changes—such as relocation to a high-risk jurisdiction, significant growth in transaction volumes, or new funding patterns—prompt immediate reassessment. Where necessary, enhanced monitoring or additional safeguards are introduced to address newly identified risks.

9. TERMINATION OF CUSTOMER RELATIONSHIPS

Orakum N.V. reserves the right to suspend or terminate any customer relationship where required under regulations, internal policies, or risk considerations. Termination may occur if a customer fails to provide the necessary identification or supporting documents within thirty calendar days, if their behaviour raises suspicion of money laundering, terrorist financing, or proliferation financing, or if they

engage in activities that breach applicable laws, regulatory requirements, or the company's Responsible Gambling Policy.

9.1 Handling of Funds and Reporting

When termination is connected to suspected criminal activity, Orakum N.V. files a report with the Financial Intelligence Unit (FIU) in line with the National Ordinance on the Reporting of Unusual Transactions (NORUT). Any remaining funds in the customer's account are returned to the original source of payment, unless a freeze or seizure is legally required while investigations are ongoing. All termination decisions are documented in detail, with records kept for at least five years, including the justification and supporting evidence.

9.2 Grounds for Refusal or Termination

A customer will be refused service or have their account terminated if they:

- Are residents of, transacting from, or accessing services in prohibited or sanctioned jurisdictions.
- Fail to provide requested documents or information within the prescribed timeframe.
- Submit false, misleading, or incomplete details during registration or verification.
- Cannot demonstrate the legitimate source of funds or wealth.
- Are involved in, or suspected of, money laundering, terrorist financing, or other criminal activities.
- Are Politically Exposed Persons (PEPs) whose risk cannot be reduced to an acceptable level.
- Engage in fraudulent behaviour, bonus abuse, collusion, or other prohibited gambling practices.
- Attempt to use third parties to transact on their behalf without disclosure and verification.
- Have self-excluded or been excluded due to responsible gambling measures.
- Seek to redeem large amounts of chips or request withdrawals without verifiable gambling activity.
- Are under the legal gambling age applicable in their jurisdiction.

10. INTEGRATION WITH RESPONSIBLE GAMBLING

Orakum N.V. ensures that its Customer Acceptance Policy is fully aligned with the company's Responsible Gambling framework. Protecting customers from gambling-related harm is an essential element of both compliance and operational practices.

10.1 Indicators of Gambling Harm

If a customer shows behaviours suggesting gambling-related risks—such as deposits that appear disproportionate to their financial capacity or excessively long gaming sessions—the company may take immediate action. Possible measures include applying deposit or wagering limits, temporarily suspending the account, or, where necessary, refusing service altogether in order to protect the individual.

10.2 Self-Exclusion and Account Restrictions

Requests for self-exclusion are processed promptly and applied to all accounts linked to the customer, preventing attempts at circumvention. These restrictions remain effective for the duration specified by the customer or for as long as required under regulatory rules.

10.3 Staff Training and Awareness

All employees in customer-facing roles undergo training to recognise early warning signs of problem gambling. This training is incorporated into both the onboarding process and ongoing monitoring, ensuring that staff are able to identify risks and intervene quickly when necessary.

10.4 Connection with the Risk-Based Approach

Responsible Gambling oversight is embedded into the company's broader Risk-Based Approach. Behavioural indicators such as unusual spending patterns, excessive play time, or self-exclusion requests are assessed alongside financial, geographic, and technological risk factors. This integration ensures that gambling-related vulnerabilities are monitored with the same diligence as financial crime risks, reinforcing both customer protection and regulatory compliance.

11. RECORD KEEPING

Orakum N.V. retains all records connected to customer acceptance for no less than five years after the termination of the business relationship, in accordance with applicable regulatory requirements. These records include identification and verification documents, proof of address, evidence of the customer's source of funds and source of wealth, transaction monitoring alerts and investigation reports, Enhanced Due Diligence (EDD) files, internal compliance reviews, and documentation of account suspensions or terminations.

All records are safeguarded using encryption and maintained under strict access controls to preserve confidentiality and data integrity. Access is granted exclusively to authorised personnel, with all activity logged and subject to periodic review to ensure full compliance with both internal procedures and data protection standards.

12. REVIEW AND APPROVAL

Orakum N.V. conducts a review of this Customer Acceptance Policy at least once every twelve months to ensure it remains current, effective, and compliant with applicable legislation, regulatory guidance, and established industry best practices. The review process also considers any developments in the company's risk profile, emerging customer behaviour patterns, and technological advancements that may introduce new vulnerabilities.

Any proposed amendments are prepared by the Compliance Officer and submitted to the Board of Directors for approval before implementation. All revisions are fully documented, and relevant staff members are informed and trained to guarantee that the updated policy is applied consistently throughout the organisation.