

KYC POLICY

Last updated: 15 October 2025

KYC Policy

In order to open an account to use the Website services, you should provide your e-mail address, choose a password and fill in the information required to complete the registration by providing us the personal information, including your name, date of birth and phone number.

We follow the rules of KYC procedures ("Know Your Customer"). Your name on Your Account shall match your true and legal name and identity. To verify your identity, the Company reserves the right to request at any time satisfactory proof of identity (including but not limited to copies of a valid passport / identity card and/or any payment cards used). If you fail to supply the information and documents requested, we shall be entitled to suspend the activity of your account until the provision of the information requested and/or close your account. The Company reserves the right to review the documents within 30 (thirty) calendar days.

You hereby certify and agree that you have provided accurate, complete and true information about yourself upon registration and you shall maintain the accuracy of that information by promptly updating it if there are any changes. Failure to do so may result in account closure, account limitations or voiding transactions (bonus, winnings).

You shall only open a single account at the Website. In all cases, only one account per customer, per address, per shared computer and per shared IP address shall be allowed. Any other account you open on the Website shall be considered as the duplicate account. You shall inform the Company that you wish to create a duplicate account due to the original account access loss or any other important reason and receive a permission from the Company before the creation of the duplicate account. In any other cases all duplicate accounts may be immediately closed by the Company and:

- all transactions made from the duplicate account shall be considered null and void;
- any returns, winnings or bonuses which you have gained or accrued within the use of the duplicate account shall be forfeited from you and a return may be claimed by us. Any funds withdrawn from the duplicate account shall be returned to us on demand;
- the Company shall not compensate any funds from both bonus and real money balances of the duplicate account. The Company reserves the right, at its sole discretion, to claim the return of any lost funds that were used for bets effected via the duplicate account;
- the Company shall not accept any requests on fund returns which have been lost or initially deposited on the duplicate account provided that the duplicate account was created with intention to receive bonuses and other promo offers from the Company, as well as if a number of duplicate accounts was created with a purpose of receiving a return of the first deposits made on previously created duplicate accounts, which is considered to be an abuse. If the Company at its sole discretion assumes that the duplicate accounts were created only with a purpose of fraud and/or abuse of hereunder, then the funds deposited on this duplicate account shall not be returned to the player.

When a user makes an aggregate lifetime total of deposits exceeding EUR 2000 (or its equivalent in other currency) or requests a withdrawal of any amount inside the 1red.com Platform, then it is compulsory for them to perform a full KYC process.

During this process, the user will have to input some basic details about themselves and then upload

- 1) A copy of Government Issued Photo ID (in some cases front and back depending on the doc)
- 2) A selfie of themselves holding the ID doc
- 3) A bank statement/Utility Bill

Once uploaded, the user will get a "Temporarily Approved" Status and the documents will now be on our side, and the "KYC Team" will have 24hrs to go over them and email the user about the outcome:

- Approval
- Rejection
- More information needed – No change in Status

When the user is on "Temporarily Approved" Status then

- They can use the platform normally
- They cannot deposit more than EUR 500 in aggregate total
- They cannot complete any withdrawal.

Guideline for the KYC Process

1) Proof of ID

a. Signature Is there

b. Country is not a Restricted Country: Aruba, Australia, Austria, Bonaire, Curacao, France, Saba, Statia, St. Maarten, Singapore, Spain, Israel, Lithuania, Dutch West Indies, Gibraltar, Jersey, Greece, Angola, Hungary, Albania, Iraq, Cuba, Jamaica, Uganda, Pakistan, Iran, Panama, Lebanon, Zimbabwe, Mauritius, Nicaragua, Yemen, Czech Republic, Central African Republic, Côte d'Ivoire, Sudan, Liberia, Syria, Cayman Islands, Somalia, Republic of the Congo, Democratic Republic of the Congo, North Korea, Eritrea, Haiti, Sierra Leone, Serbia, Ethiopia, Myanmar, South Sudan, the Netherlands, Burkina Faso, Libya, Mali, Barbados, Rwanda, the United Kingdom, the USA, Ukraine, Romania, Russia, Cyprus and any other jurisdiction that the Central Government of Curacao deems online gambling illegal. This includes all of the named Nations' Territories and Possessions.

c. Full Name matches the user's name

d. Document does not expire in the next 3 months

e. Owner is over 18 years of age

2) Proof of Residence

a. Bank Statement or Utility Bill

b. Country is not a Restricted Country: Aruba, Australia, Austria, Bonaire, Curacao, France, Saba, Statia, St. Maarten, Singapore, Spain, Israel, Lithuania, Dutch West Indies, Gibraltar, Jersey, Greece, Angola, Hungary, Albania, Iraq, Cuba, Jamaica, Uganda, Pakistan, Iran, Panama, Lebanon, Zimbabwe, Mauritius, Nicaragua, Yemen, Czech Republic, Central African Republic, Côte d'Ivoire, Sudan, Liberia, Syria, Cayman Islands, Somalia, Republic of the Congo, Democratic Republic of the Congo, North Korea, Eritrea, Haiti, Sierra Leone, Serbia, Ethiopia, Myanmar, South Sudan, the Netherlands, Burkina Faso, Libya, Mali, Barbados, Rwanda, the United Kingdom, the USA, Ukraine, Romania, Russia, Cyprus and any other jurisdiction that the Central Government of

Curacao deems online gambling illegal. This includes all of the named Nations' Territories and Possessions..

- c. Full Name matches the user's name and is same as in proof of ID.
- d. Date of Issue: In the last 3 months

3) Selfie with ID

- a. Holder is the same as in the ID document above
- b. ID document is the same as in "1". Make sure photo/ID number is the same

Notes on the KYC Process

- 1) When the KYC process is unsuccessful then the reason is documented and a support ticket is created in the system. The ticket number along with an explanation is communicated back to the user.
- 2) Once all proper documents are in our possession then the account gets approved.

Other AML measures

- 1) If a user has not passed full KYC then they cannot make additional deposits or withdrawals of any amount.
- 2) If a user has passed the KYC process successfully then
 - a. There is a deposit limit per transaction (max EUR 2 000)
 - b. Prior to any withdrawal there is a detailed algorithmic and manual check on the activity and balance of the user to see if the amount withdrawn is a result of proper activity in the platform.
- 3) Under no circumstances may a user transfer funds directly to another user.

Personnel Training

The Company appoints an AML Compliance Officers Mr. Boriss Pančenko and Anna Viktor Glam. who are fully responsible for the Company's compliance with CFT and AML policies, establishing and maintaining the Company's AML program, AML training employees, receiving, investigating and maintaining internal suspicious activity reports.

All the employees, managers and directors of the Company are suitably trained while entering into employment.

Employees who are dealing with clients or are involved in any AML checking, verification or monitoring undergo AML training. Each new employee has to follow an AML training plan. The AML training program includes suspicious transactions identification training as well as training in prevention, detection and reporting of money laundering and terrorism financing crimes.

Any violation of the AML policy must be reported to the AML compliance officer, unless the violation implicates the AML Compliance Officer, in which case an employee must report the violation to the CEO.

Where the Company relies on third-party service providers for customer due diligence, screening, or verification services, the Company will ensure that:

A written agreement or Service Level Agreement (SLA) is in place defining responsibilities, performance standards, and reporting obligations.

The third party is regulated and/or reputable, and subject to independent audits.

Ultimate responsibility for compliance with AML/KYC obligations remains with the Company, and not the third party.

Beneficial Ownership and Corporate KYC for the Corporate Entities Partners

For legal entity partners, the Company will identify and verify the Ultimate Beneficial Owners (UBOs) who directly or indirectly own or control 25% or more of the entity, or otherwise exercise control.

Documentation may include corporate registries, shareholder registers, and certified ownership declarations.

The Company will ensure that the corporate structure is transparent, and that UBO information is kept updated throughout the relationship.

Risk Assessment

A money laundering and terrorist financing risk assessment attempts to identify, analyse and understand money laundering and terrorist financing risks. It serves as the first step in addressing the risks and, ideally, involves making judgments about threats, vulnerabilities and consequences. The Company shall identify the threats (persons, or groups of people, objects or activities with the potential to cause harm, including criminals, terrorist groups and their facilitators, their funds, as well as past, present and future money laundering or terrorist financing activities), vulnerabilities (things that can be exploited by the threat or that may support or facilitate its activities and means focusing on the factors that represent weaknesses in AML or CTF systems or controls or certain features of a country, particular sector, financial product or type of service that make them attractive for money laundering and terrorist financing), consequences (this refers to the impact or harm that money laundering or terrorist financing may cause, including the effect of the underlying criminal and terrorist activity on financial systems and institutions, the economy and society more generally. The Company adopts an approach that attempts to distinguish the extent of different risks to assist with prioritizing mitigation efforts, rather than being a generic box-ticking exercise. That is why the Company performs the identification (the identification process begins by developing an initial list of potential risks or risk factors when combating money laundering and terrorist financing. Risk factors are the specific threats or vulnerabilities that are the causes, sources or drivers of money laundering and terrorist financing risks), analysis (analysis involves consideration of the nature, sources, likelihood, impact and consequences of the identified risks or risk factors. The aim of this stage is to gain a comprehensive understanding of each of the risks, as a combination of threat, vulnerability and consequence, in order to assign a relative value or importance to each of them. Risk analysis can be undertaken with varying degrees of detail, depending on the type of risk, the purpose of the risk assessment, and the information, data and resources available), evaluation (the evaluation stage involves assessing the risks analyzed during the previous stage to determine priorities for addressing them, taking into account the purpose established at the beginning of the assessment process. These priorities can then contribute to development of a strategy for the mitigation of the risks). The Company pays special attention to country and geographic risk (some countries pose an inherently higher money laundering and terrorist financing risk than others. In addition to considering their own experiences, there should be taken into account a variety of other credible sources of information identifying countries with risk factors in order to determine that a country and customers from that country pose a higher risk. Customers that are associated with higher risk countries, as a result of their citizenship, country of business or country of residence may present a higher money laundering and terrorist financing risk, taking into account all other relevant factors. We check customer location because of the additional risks which arise from cross-border operations. The country or geographic risk can also be considered in conjunction with the customer risk).

We also assess customer risk (determining the potential money laundering and terrorist financing risks posed by a customer, or category of customers, is critical to the development and implementation of an overall risk-based framework. We seek to determine whether a particular customer poses a higher risk and the potential impact of any mitigating factors on that assessment. Application of risk variables may mitigate or exacerbate the risk assessment. Categories of customers whose activities may indicate a higher risk include: customers who are PEPs, family members of PEPs or known close associates of PEPs, high spenders – the level of spending which will be considered to be high for an individual customer will vary among casino operators, and among casinos managed by the same operator, disproportionate spenders – we obtain information about customers' financial resources so that they can determine whether customers' spending is proportionate to their income or wealth, casual customers – this includes tourists, participants in junkets and local customers who are infrequent visitors, regular customers with changing or unusual spending patterns, improper use of third parties – criminals may use third parties or agents to avoid CDD undertaken at the threshold or to buy chips, or they may be used to gamble so as to break up large amounts of cash, junkets – junkets can pose several higher risks, including criminal control of the junket operator or participants, the movement of funds across borders which obscures the source and ownership of the money gambled by participants and their identities, and structuring, refining and currency exchange risks. Transaction risk is a very important risk factor assessed by the Company as well as a product risk. Many customers carry a lower money laundering or terrorist financing risk. These might include customers who are regularly employed or who have a regular source of income from a known source which supports the activity being undertaken. This applies equally to pensioners, benefit recipients, or to those whose income originates from their partner's employment or income. Conversely, many customers carry a higher risk of money laundering. These may include known criminals, customers who are not regularly employed or who do not have a regular source of income from a known source which supports the level of activity being undertaken, or problem gamblers.

EDD Procedure

The Company follows the following EDD rules' recommendations:

- The Company scrutinizes customers' risk profile;
- The Company obtains additional information where necessary;
- The Company conducts extensive background checks and monitors transactions;
- The Company organizes and secures its data in line with compliance standards;
- The Company keeps the data available for regulators.

The Company obtains additional identifying information from a wider variety or more robust sources and using the information to inform the individual customer risk assessment:

- Carrying out additional searches (for example, verifiable adverse media searches) to inform the individual customer risk assessment;
- Commissioning an intelligence report on the customer or beneficial owner to understand better the risk that the customer or beneficial owner may be involved in criminal activity;
- Verifying the source of funds or wealth involved in the business relationship to be satisfied that they do not constitute the proceeds from crime;
- Seeking additional information from the customer about the purpose and intended nature of the business relationship.

Sanctions Screening

The Company has implemented due diligence and sanctions screening procedures. The Company shall screen and identify persons and transactions subject to and/or prohibited by the following: US

OFAC SDN List; UK HMT Consolidated List of Persons and Ukraine List of Persons; UN restrictive measures; and the EU Consolidated List. The Company utilizes Thomas Reuters World-Check (World-Check) and Refinitiv to conduct sanctions screening, which allows the Company to screen all relevant sanctions lists using a single search function. The following internal documents should be cross-referenced to effectively carry out sanctions screening: 1) Screening Request Form; 2) Partnership Appraisal Form; 3) Screening Procedures Matrix; 4) Due Diligence and Partnership Appraisal Map; and 5) Thomson Reuters World-Check User Guide.

Due Diligence and Partnership Appraisal Screening Process

The first phase of sanctions screening requires fact gathering due diligence and partnership appraisal process. This requires completion of Screening Request Form and/or Partnership Appraisal Form (depending on the type of transaction). Staff should cross-reference the Screening Procedures Matrix to determine which form(s) require completion. In accordance with the Due Diligence and Partnership Appraisal Map, Programmes/POC carries out the fact gathering process in conjunction with new and potential partners. These forms are intended to capture information necessary to conduct effective screening utilizing World-Check. Essential information to be captured includes names and aliases, addresses, date of birth (individuals), and ownership structure and identification (trustees, directors, decision-makers, and shareholders). Pertinent data fields are noted in the Screening Request Form and Partnership Appraisal Form, respectively. Once the fact gathering process is complete, the information is forwarded to internal audit staff (Finance). Internal audit staff screens persons and organisations utilizing World-Check.

Risk Rating

The next phase of sanctions screening requires the Company to assign a risk rating. A risk rating is assigned by internal audit staff and is documented on the Screening Request Form and/or Partnership Appraisal Form. A risk rating will be assigned to any person or organisation subject to sanctions screening procedures. Persons and entities subject to sanctions in the US, UK, UN or EU are automatically assigned a high-risk rating. Persons and entities identified as Politically Exposed Persons (PEPs) on World-Check will automatically be rated as medium or high-risk depending on the level of exposure. High-risk is defined as a transaction that poses or allows for a significant reputational risk to the organisation. It is Company's policy not to engage with any person, entity or financial institution deemed high-risk. Medium-risk is defined as transaction that poses or allows for a greater than average reputations risk to the organisation. This may include persons and entities identified as PEPs. Company's general policy is to not engage with parties deemed medium-risk unless a dispensation is received from the Director. Parties deemed medium-risk are subject to rescreening annually. Low-risk is defined as a transaction that poses or allows for an average reputational risk to the organisation. This may include persons or entities with exposure to PEPs but may still be deemed acceptable to work with once all due diligence steps have been carried out. Parties deemed low-risk are subject to rescreening every two years. No-risk is defined as a transaction that does not pose any reputational risk to the organisation. Parties with no identified risks are subject to rescreening every five years.

Decision Making and Escalation

The final phase of sanctions screening requires the Company to decide whether to move forward with an engagement, contract, or transaction. The decision is documented on the Screening Request Form and/or Partnership Appraisal Form and retained in the person or organisation's file.

All transactions where a sanctions risk is deemed present (low, medium or high) are automatically forwarded to the Director for review and potential investigation. The Director and compliance specialist will review the transaction before the party and/or services can be approved. After performing necessary due diligence, and where it is determined that a person, partner, or transaction implicates a potential sanctions risk, the Director must compile a complete packet of all relevant documents and information, and note the decision made whether to proceed.

The Director and compliance officer are the authorities on sanctions compliance for the Company.

The Company reviews the sanctions list stipulated herein above every day.

The Company shall inform in accordance with the applicable rules and regulations on the suspected criminal activities and on any information on the transactions with the persons/organizations in the one of the sanction lists discovered during the stipulated procedures.

Reporting of Suspicious and Unusual Transactions (SAR / UTR)

The Company maintains robust procedures for the identification, internal escalation, and external reporting of any transaction or activity that gives rise to knowledge, suspicion, or reasonable grounds to suspect money laundering, terrorist financing, or any other criminal activity.

All employees are obliged to remain vigilant for suspicious behaviour and to immediately report such instances to the designated Money Laundering Reporting Officer (MLRO).

Internal reporting procedure

- Any staff member who identifies a transaction or pattern of activity that appears unusual or inconsistent with a customer's known profile must complete an Internal Suspicious Activity Report (ISAR) and forward it to the MLRO without delay.
- The ISAR must contain the relevant facts, observations, and any supporting documentation.
- The MLRO will acknowledge receipt, conduct a preliminary review, and determine whether the activity warrants further investigation or external reporting.
- All ISARs, whether escalated or not, will be recorded in the Internal Suspicious Activity Register and retained for at least five (5) years.

External reporting to competent authorities

- If, following internal review, the MLRO determines that a suspicion is justified, the MLRO will file a Suspicious Activity Report (SAR) or Unusual Transaction Report (UTR) with the Financial Intelligence Unit of Curaçao (FIU Curaçao) via the prescribed reporting channel.

- Where required by law or the Curaçao Gaming Authority (CGA), the MLRO may also notify the CGA that a SAR/UTR has been filed.

- The report must include sufficient details of the customer, transactions, and reasons for suspicion, in accordance with the FIU's guidelines.

- The MLRO will maintain copies of all filed reports, acknowledgment receipts, and related correspondence in a secure, access-restricted environment.

Prohibition of "tipping off"

Under no circumstances may any employee inform the customer or any unauthorised third party that a report has been filed, or that an investigation into their activities is underway. Breach of this confidentiality requirement constitutes a serious disciplinary and legal offence.

Record keeping and audit

The MLRO ensures that all reports and related analyses are retained for a minimum of five (5) years from the date of reporting, and are made available to the FIU or CGA upon request. Periodic reviews will be conducted to verify that the reporting process remains effective and compliant with applicable legislation.

Scope and Applicability

This Policy applies to all brands, domains, and online gaming platforms operated by Bets Entertainment N.V. under its Curaçao gaming license. All authorized domains operate under the same KYC, AML, and Responsible Gaming framework as described herein, ensuring consistency of compliance across the group.

Governance and Policy Review

This Policy will be reviewed at least annually, or sooner where triggered by:

- Material changes in AML/CFT legislation or FIU Curaçao requirements
- Significant changes in business operations or risk exposure
- Regulatory feedback or audit findings

All updates will be version-controlled, approved by senior management, and documented in the Policy Register. Training logs will be updated to ensure staff are made aware of revisions.



(SMES) Solutions for Management and Employment Support N.V.

Managing Director

21.10.2025