

Anti-Money Laundering Policy

CODEX B.V.
(2025)

1. AML POLICY OVERVIEW

1.1. Policy Objectives and Scope

As part of its continuous improvement implementations, CODEX B.V. is dedicated to putting in place the necessary steps needed to ensure that all employees, full-time or contractual, participate actively in preventing any of the Company's services and/or outlets for the sole or partial purpose of money laundering and/or the financing of terrorist undertakings.

Money laundering (ML) and the use of legal or illegal monies for the purpose of terrorist financing have become ever growing threats - CODEX B.V. (referred to herein as the "Company") is fully committed to playing its role in assisting the international fight against such organized crime and terrorism.

The Company has therefore incorporated the following Anti-Money Laundering and Terrorist Financing Policy ("Policy") as part of its internal process. The Company has applied this Policy to all its employees and adheres to the highest of the industry's best practices in its mission to prevent any possible criminal activity through money laundering.

The Company's AML program is designed to be compliant among others and with the following:

- Directive 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering.
- EU Regulation 2015/847 on information accompanying transfer of funds.
- Various EU Regulations imposing sanctions or restrictive measures against persons and embargo on certain goods and technology, including all dual-use goods.
- European Business Law of 18 September 2017 on the prevention of money laundering limitation of the use of cash.

1.2. Money Laundering Defined

Money Laundering is the terminology used for several illegal offences encompassing money obtained from certain crimes, (such as extortion, insider trading and drug trafficking) as "dirty" and needs to be "cleaned" to appear to have been derived from legal activities, so that banks and other financial institutions will deal with it without suspicion. Money can be laundered by many methods that vary in complexity and sophistication. Whether it be through conversion, transfer of property, concealment, disguise, acquisition, or possession of funds derived from criminal activity or the participation/assistance of the movement of funds derived from criminal activity in order to appear legitimate – are all forms of money laundering.

1.3. Distribution of the AML Policy

This AML Policy is provided to all staff (frontline, leads, managers and The Board) and is redistributed as updated.

The Compliance Officer is responsible for providing a report to the Executive Management team for review not less frequently than once every twelve (12) months as to the effectiveness of the Policy and related operational procedures and shall provide recommendations to management as to proposed operational or policy enhancements.

The Executive Management team shall review the content of this Policy for necessary revisions or updates not less frequently than once every twelve (12) months. Recommendations and feedback will be given to the Compliance Officer.

Except for directives from relevant authorities, any proposed amendments to the Policy require the review and approval of the Compliance Officer, the Executive Management team, and legal counsel.

2. COMPLIANCE OFFICER – MONEY LAUNDERING REPORTING OFFICER (MLRO)

2.1. Appointment of the Compliance Officer/MLRO

A qualified senior employee shall be always appointed as Compliance Officer. The Compliance Officer has been identified and the Compliance Officer's contact details made available to all staff and applicable staff of service providers.

2.2. Reporting Structure and Independence

The Compliance Officer holds no other position within the organization or any affiliated company or supplier and operates independently from all other functions within the organization to ensure that actual or perceived conflicts of interest do not occur. Subject to oversight by the CEO, the Compliance officer has the authority to act independently from other functions within the organization to fulfil his/her below noted roles and responsibilities. The compliance officer has the full and public support of the executive management team in executing his duties. All staff are required to assist the Compliance Officer (and the nominated officer, as appropriate) in fulfilling their duties.

2.3. Duties and Responsibilities of the Compliance Officer/MLRO

- The Compliance Officer is responsible for oversight and management of all compliance related functions within the Company and within its affected suppliers, including the protocols described in this Policy. Compliance Officer/MLRO duties include (but not limited to) the following:

- Ensure that procedures are in place to ensure compliance with all applicable legislation, regulations and all associated guidelines, codes of practice and Company policies and procedures.

- Report to the CEO and inform senior management the result(s) of any remedial action taken.

- Attend regular Compliance Meetings with selected senior management, prepare an agenda therefor, and to take, circulate and maintain the minutes thereof.

- Update and maintain any compliance-related policies, including this Policy.

- Plan and co-ordinate training activity for all departments to include key regulatory areas including the significance of regulatory compliance, ID and age verification, fraud, anti-money laundering, and problem gambling.
- Be the point of contact with the involved Regulator(s).
- Investigate and report any breaches of the applicable laws, regulations, guidelines, codes of practice and company policies and procedures to senior management and, as appropriate, to the Regulator.
- Plan and co-ordinate training activity for all departments to include key regulatory areas including the significance of regulatory compliance, ID and age verification, fraud, anti-money laundering, and problem gambling.
- Consult with staff representatives and attend staff meetings on compliance topics.
- Manage regular reviews of Company's internal control system to ensure that it accurately reflects the then current operation of the business – and report any discrepancies/oddities to relevant senior management.

3. FIRM POLICY AND COMMITMENT

The Company will ensure it has appropriate policies and procedures in place to complement this AML policy, in compliance with applicable regulations and monitoring of adherence to those policies will also take place. Staff members are trained in AML processes and procedures and will actively participate in preventing the services of the Company from being exploited by criminals for money laundering or terrorist financing purposes.

The objectives of this and related policies are:

- Ensuring the Company is compliant with all applicable laws, statutory instruments of regulation.
- Protecting the Company and its staff as individuals from the risks associated with breaches of the law, regulations and supervisory requirements.
- Preserving the good name of the Company against the risk of reputational damage presented by implication in money laundering and terrorist financing activities.
- Making a positive contribution to the fight against crime and terrorism.

4. SCREENING AND MONITORING

4.1. Account Screening

Upon a customer's creation of a new account, a preliminary screening both automated and manual is conducted to identify potentially linked or other suspect account activities. Such screening searches for potentially suspect elements, including:

- Accounts that may depict similar information.

- Two or more accounts utilizing the same email address upon creation and/or the same IP address.
- Customer has more than one account
- Any other suspicious information / activity identified or suspected by the Fraud or Financial Services teams.

If any of the foregoing screening identifies potential issues, the Financial Services team is notified automatically and will investigate and apply applicable business rules accordingly. Such business rules may result in a variety of potential risk mitigation steps, including closure of account, escalation to the Fraud team for enhanced diligence, limitation of deposit or withdrawal methods, imposition of deposit limits, etc.

4.2. Enhanced Due Diligence (EDD)

In certain cases, there is the possibility certain customer relationships demonstrate heightened AML or fraud risks to the Company. In such instances and in addition to its regular customer due diligence protocols, the Company shall carry out enhanced due diligence (EDD).

During the enhanced due diligence process, the Company will take additional required steps to aid in identifying a potential customer, including (but not limited to) personal and financial background. This may involve obtaining additional evidence in verifying the individuality of the client.

This may include obtaining evidence to verify aspects of the customer's identity and verified confirmation in order to establish the source of funds of the customer. The Company's Fraud Detection agents have access to a variety of tools through its suppliers and databases which are used to verify submitted documentation (e.g. Drivers Licenses, and Passports).

The circumstances that may trigger additional concern and may require Enhanced Due Diligence (EDD) are noted below:

- The customer or potential customer is situated in a country or territory that does not apply to the Company's geographical market.
- The customer or potential customer is or appears to be a Politically Exposed Person (see below).
- Any other circumstances as Company reasonably perceives to be a heightened risk money laundering or terrorist financing.

The company associates solely with trusted and approved Payment Service Providers whom all have effective AML policies in place as to prevent the large majority of suspicious deposits from taking place without proper execution of KYC procedures onto the potential customer.

4.3. PEP – Politically Exposed Person

A PEP or Politically Exposed Person is an individual who currently or previously held a prominent public function in any country. A wide range of persons may be considered as PEPs, including heads of state, senior members of the judiciary, senior military officers, and immediate family members of such persons.

A PEP generally presents a higher risk for potential involvement in bribery and corruption by virtue of their position and the influence that they may hold. If an account is identified as a potential match to a PEP list, the account shall be immediately frozen pending escalation and review.

The Compliance Officer is immediately notified, and a further assessment is made.

The Compliance Officer will reach out to the appropriate department and offer his/her recommendations regarding the account.

4.4. Reporting

If for any reason the Company reasonably suspects that a client and/or account may be involved in any form of activity that amounts to money laundering, the Company will immediately inform the required and appropriate external authority, namely the Local Financial Intelligence Unit in Curacao. If the Company believes that some degree of suspiciousness after a transaction has taken place and after an internal investigation confirms as such - the Company will freeze the account and will inform the relevant authorities immediately and disclose the necessary information required by law to do so. The Compliance officer or an authorized staff member will take ownership and report the activity through the appropriate AML reporting form and submit it to the Regulator. Additional reporting procedures are put in place to mitigate the Company's exposure to various forms of money laundering. These consist of in-house and third-party reporting/monitoring tools that run daily and weekly. Furthermore, AML reporting procedures such as Suspicious Activity Reporting (SARs) and Significant Transaction.

Reports (STRs) will be conducted and submitted when needed to the Regulators and if necessary, the appropriate law enforcements.

4.5. Ongoing and Continuous Monitoring

The Company implements and monitors all activity of clients and/or staff, to ensure that all activity – whether it be transactional or instructional, be consistent and given the required attention for the detection of possible money laundering or terrorist financing. The Compliance Officer/MLRO will supply the appropriate AML training (which may consist of in-class, video conference or literature) to provide involved staff, guidelines and direction on:

- The process in reporting suspicious activity.
- The type of activity that should be considered significant and critical in detecting possible money laundering – these may be given in class or reading materials.
- Distinguishing specific incidences that may require cause for re-assessment of a risk-based approach.
- The Company consistently implements monitoring processes with the addition of potentially new and future products and/or services it provides to its clients.
- Implementations and assessments are put in place (and adjusted if need be) to mitigate any possible risk of money laundering or terrorist financing where the use of new products and/or services may be vulnerable to. These include (but not limited to):

- Overview analysis of transactions over specific periods.
- Overview analysis of new services/products used by the client.
- Applying limits to activities on new products/services used by the client for a given time.
- Requests for justification of noticeable irregular activity from the client.

5. TERMS & CONDITIONS WHICH THE PLAYER HAVE TO ACCEPT

The below Terms & Conditions are post on the CODEX B.V.'s websites and every user shall accept this to use the services of the Company.

Nobody can use the Company's services without accepting the Terms & Conditions.

5.1. Opening Account

In order to place a bet or play a game using the Services on the website (s), a person will need to open an "Account", by click on "Join Now" and/or "Sign Up" on the Website and follow the on-screen instructions.

When the person opens the Account, the person will be asked to provide personal information, such as Full Name, Date of Birth, and appropriate contact details, including an address, telephone number and e-mail address and will be approved as a "User".

The User may update its Contact Details from time to time by contacting Customer Services and/or through the My Account management page on the Website and/or or by such other method as shall, from time to time, be offered by the Company.

In opening Account, the User shall warrant that he understands and accept the followings:

- The risk that, by using the Services, he may, as well as winning money, lose money.
- He is over 18 years of age and/or above the age at which gambling or gaming activities are legal under the law or jurisdiction that applies to him (the "Relevant Age").
- Gambling is not illegal in the territory where he resides.
- He is legally able to enter contracts.
- He has not been excluded from gambling.
- He has not already had an Account closed by Company for any reason.
- The Account must be registered in his own, correct, name and personal details and it shall only be issued once for him and not duplicated through any other person, family, household, address (postal or IP), email address, Access Device, or any environment where Access Devices are shared (e.g. schools, workplaces, public libraries, etc.) and/or account in respect of the Services.
- Any other accounts which the User open with us, or which are beneficially owned by him in relation to the Services shall be "Duplicate Accounts" and we may close any Duplicate Account (but shall not be obliged to do so). If we close a Duplicate Account:
 - All bonuses, free bets and winnings accrued from such bonuses and free bets obtained using that Duplicate Account will be void and forfeited.

◦ We may, at our entire discretion, void all winnings and refund all deposits (less amounts in respect of void winnings) made in respect of that Duplicate Account and, to the extent not recovered by us from the relevant Duplicate Account, any amounts to be refunded to us by him in respect of a Duplicate Account may be recovered by us directly from any other of his Accounts (including any other Duplicate Account), or

◦ We may, at our entire discretion, allow usage of the Duplicate Account to be deemed valid in which case all losses and stakes placed by or for him through the Duplicate Account shall be retained by us.

5.2. Verification of Account

The User must accept and warrant the followings:

- The name and address which were provided when opening the Account are correct.
- He is the rightful owner of the money which at any time is deposited in the Account.

By agreeing to the Terms of Use the User, authorizes the Company to undertake any such verification checks from time to time to confirm some facts. The User agrees that from time to time, upon company's request (including requests from Payment processor), he may be required to provide additional details in respect of any of such information he have provided to the company, including in relation to any deposits which he have made into his Account.

Whilst the company is undertaking any Checks from time to time, this may restrict User from withdrawing funds from his Account and/or prevent access to all or certain parts of the Website.

Please note that the company may from time to time re-perform the Checks for regulatory, security or other business reasons. If any such restrictions cause a problem, contact can be made with the company. All the contacts details with company are posted on the website.

In certain circumstances the company may have to contact the User and ask him to provide further information, directly in order to complete the Checks. For this purpose, the company requires a three step account verification of all of our users and customers in order to ensure that the details of the person registered are correct and the deposit methods used are not stolen or being used by someone else.

– Verification Steps

The following three steps should be carried out as follows:

- **Step One Verification:** Step one verification must be done by every user and customer to withdraw. Regarding of the choice of payment, the amount of payment, the amount of withdraw, the choice of withdraw and nationality of the user/customer step one verification must be done first. Step one verification is a document that must be filled out by the user/customer himself. Following information's must be filled in: first name, second name, date of birth, country of usual residence, gender, and full address.

The basic document for this procedure is accessible via the setting page on the website(s)

Every user must fill out the following information:

1. Full Name
2. Nationality
3. Gender
4. Date of Birth

The document will be saved and created by an AI. An employee may perform additional checks, if necessary, based on the occasion.

- **Step Two Verification:** Step two verification must be done by every user which deposit over €2000 (two thousand Euros) or make any withdraw (our users are not allowed to send any amount to another account or change their playing currency). Until step two verification is done the withdraw, tip or deposit will be hold. Step to verification will lead the user or customer to a subpage where he must send in his ID. The user/customer must take a picture of his ID. While a paperclip with a six-digit random generated number is next to his ID: Only an official ID may be used for ID verification, depending on the country the variety of accepted IDs may be different. There will also be an electronic check if the filled in Data from the step one verification is correct. The electronic check will check via two different databanks to ensure the given information's matches with the filled document and the name from the ID: If the electronic test fails or is not possible the user/customer is required to send in a conformation of his current resident. A certificate of registration by the government or a similar document is required.

- **Step Three Verification:** Step three verification must be done by every user which deposit over €10000 (ten thousand Euros) or withdraws over €5000 (five thousand Euros). Until step three verification is done the withdraw, tip or deposit will be hold. For step 3, a user/customer will be asked for a source of wealth (SOW). Examples of SOW include the following:

1. Ownership of business
2. Employment
3. Inheritance
4. Investment
5. Family

It is critical that the origin and legitimacy of that wealth is clearly understood. If this is not possible an employee may ask for an additional document or prove.

The account will be frozen if the same user deposits either this amount in one go or multiple transactions which amount to this. An email will be sent to them manually to go through the above and an information on the website itself.

Also asks for a bank wire/credit card to further insure the Identity of the user/customer. It also gives additional information about the financial situation of the user/customer.

It is an offence for persons under the Relevant Age to make use of the Website.

If the Company will be unable to confirm that the User have the Relevant Age, then the Company may suspend the User's Account until such time that the Company is able to confirm that Users have the Relevant Age.

If subsequently it is proven that the User has been under the Relevant Age at the time which made any gambling or gaming transactions with the Company, then:

- The Account will be closed.
- All transactions made whilst User where underage will be made void, and all related funds deposited by User will be returned by the payment method used for the deposit of such funds, wherever practicable.
- Any deposits made whilst the User were under the Relevant Age will be returned and

- Any winnings which User have accrued during such time when he was under the Relevant Age will be forfeited by him and he will return to company on demand any such funds which have been withdrawn from User's Account.

All the necessary documents that may be requested according to the three-step account verification need to be provided by User to Company in 7 (seven) days after opening of the account or if requested from User by support – in 7 (seven) days after date of respective request.

The Company will review Your document(s) in 7 (seven) daytime after receipt of the respective document(s).

In case that User fail to provide the requested documents document(s) in due time the Company may suspend use of User account or decline User withdrawal request (as applicable).
Already covered by the three-step account verification

6. RISK MANAGEMENT

In order to deal with the different risks and different states of wealth in different regions on the earth we will categorize every nation in three different regions of risk.

6.1- Region one: Low Risk

For every nation from the region one the three-step verification is done as described earlier.

6.2- Region two: Medium Risk

For every nation from the region two the three-step verification will be done at lower deposit, withdraw and tip amounts. Step one will be done as usually. Step two will be done after depositing €1000 (one thousand Euros), withdrawing €1000\$ (one thousand Euros). Step three will be done after depositing €2500 (two thousand five hundred Euros), withdrawing €2500\$ (two thousand five hundred Euros). Also, users from a low-risk region that change crypto currency in any other currency will be treated like user/customers from a medium risk region.

6.3- Region three: High Risk

Regions of high risks will be banned. High risk regions will be regularly updated to keep up with the changing environment of a fast-changing world.

6.4- Enterprise-wide risk assessment

As part of its risk-based approach, the company has conducted an AML "Enterprise-wide risk assessment" (EWRA) to identify and understand risks specific to the website(s) and its business lines. The AML risk policy is determined after identifying and documenting the risks inherent to its business lines such as the services the website offers. The Users to whom services are offered, transactions performed by these Users, delivery channels used by the bank, the geographic locations of the bank's operations, customers and transactions and other qualitative and emerging risks.

The identification of AML risk categories is based on the website(s) understanding of regulatory requirements, regulatory expectations and industry guidance. Additional safety measures are taken to take care of the additional risks the world wide web brings with it.
The EWRA is yearly reassessed.

7. KNOW YOUR CLIENT POLICY

Formal Identification of users and customers on registration and entry into commercial relations is mandatory both for the regulations and legislation relating to money laundering and for the KYC policy.

The Company requires this procedure as it forms part and parcel of gambling responsibly – and the applicable law requires it. Also are some requirements which help the company to avoid people who want to involve in Money Laundering activities.

When you sign up for a new account, the Company check that you are over 18 and they verify that you are who you say you are, (a process called Know Your Customer ‘KYC’). It’s part and parcel of gambling responsibly, and the Company is obliged by Law to perform it.

7.1- Identification Procedure

A picture of a copy passport, ID card or driving license, each shown alongside a handwritten note mentioning six random generated numbers. Also, a second picture with the face of the user/customer is required. The user/customer may blur out every information, besides date of birth, nationality, gender, first name, second name and the picture to secure their privacy.

NOTE: All four corners of the ID must be visible in the same image and all details has to be clearly readable besides the named above. We might ask for all details if necessary.

An employee may do additional checks, if necessary, based on the situation.

7.2- Proof of Address

Proof of address will be done via to different electronic checks, which use two different databases. If an electronic test fails, the user/customer has the option to make a manually proof.

A recent utility bill sent to your registered address, issued within the last 3 months or an official document made by the government that proofs your state of residence.

To make the approval process as speedy as possible, please make sure the document is sent with a clear resolution where all four corners of the document is visible, and all text is readable.

For example: An electricity bill, water bill, bank statement or any governmental post addressed to you.

An employee may do additional checks, if necessary, based on the situation.

The website registration page checks the User details as the User enters the site and will let him know if there is a problem, so he can make any changes he need to before he clicks on the ‘Create My Account’ button.

For legal reasons when travelling abroad the User may not be able to access his account.

The Company is unable to accept accounts or offer any of its products or services to client’s resident in certain countries. On the website there is always posted a list of game providers and territories, from potential Customers are not accepted. This list may be amended time from time.

8. MANAGEMENT OF COMPLIANCE AND AML POLICIES

It is the Company’s policy to monitor its compliance program with legal and regulatory AML/CFT requirements. The Policy will be reviewed annually, and amendments added accordingly when new products, implementations are applied and/or changes to relevant legislation have been implemented.

The effectiveness of the Company's AML/CFT program is regularly evaluated to ensure it remains current and is aligned with business activities, regulatory developments, industry standards and best practices. By doing so, the Company adheres to all applicable laws and regulatory requirements in the jurisdictions in which it operates.

By: CODEX B.V.

DocuSigned by:

BFFB053659204B9...

Kurason Trust Curaçao N.V.
Managing Director
Represented By: Mr. Jonathan Heymans

Dated: August 13th, 2025