



XZ Solutions B.V.

KYC Policy

Version 1.3.

Version Approval

Date
30.04.2025

Version
1.3

1. Purpose

This Know Your Customer (“KYC”) Policy sets forth the procedures and controls implemented by XZ Solutions B.V. (“the Company”) to identify and verify the identity of its customers in order to prevent money laundering, terrorist financing, fraud, and other illicit activities. This Policy is a component of the Company’s broader Anti-Money Laundering and Counter-Terrorist Financing (AML/CTF) compliance framework.

The purpose of this Policy is to ensure that the Company conducts appropriate due diligence on its customers at the onboarding stage and throughout the duration of the business relationship. The Company shall ensure that it is able to form a reasonable belief that it knows the true identity of each customer and is capable of detecting and mitigating risks associated with illegal financial activity.

2. Scope and Applicability

This Policy applies to:

- All natural and legal persons who seek to establish a business relationship with the Company;
- All employees, officers, and agents of the Company who interact with customers or process customer information;
- Any third-party service providers engaged to assist in the execution of KYC obligations on behalf of the Company.

3. Risk Based Approach

The risk-based approach recognizes that the ML/FT risks faced by each sector and each subject person are different and allows for resources to be invested and applied where they are most required. The risk-based approach envisages the application of checks that are proportionate to the assessed risk. The cornerstone of the risk-based approach is the risk assessment which must be carried out at different stages of a subject person’s activities. This assessment allows the subject person to identify its ML/FT vulnerabilities and the ML/FT risks it is exposed to. On this basis, the subject person will be able to draw up, adopt and implement AML/CFT measures, policies, controls and procedures that address any identified risks.

4. KYC Procedure

Know Your Customer Procedures are followed to achieve the following objectives:

- Allowing only legitimate customers to register an account (Ex: Minors, Sanctioned Persons or Players from Sanctioned countries are not allowed to register a gaming account).
- Build the risk profile associated with the customer.
- Confirming that customers are who they say they are.
 - Monitoring customer accounts and transactions for illegal activities.
 - Blocking duplicate accounts.
 - Identifying possible PEP & Sanctioned customers.

4.1. Registration

Before being able to play on the site a customer needs to first register an account. On the registration page the customers are asked for the following details:

- Email address. In order to validate the email address of the player and email with a link to validate the email address will be sent to the email address listed in the registration. A player will not be allowed to withdraw funds unless the email is validated.
- Mobile number
- Full name
- Date of Birth
- Address

Once the above information is received the fraud department will screen the information for any false or suspicious information, possible duplicate/Self-excluded accounts, Politically Exposed Persons and sanction lists.

The IP address from where the traffic originated is tracked by the Company's back office software. Should traffic originate from countries which are on the list of restricted countries, the account will be blocked.

Should the checks (Manual or automatically done by the system) indicate that a duplicate account has been registered, the account is suspended until further checks are made to determine whether this is indeed a duplicate account. If the checks prove that the account is indeed a duplicate account, the account will be closed.

4.3. Age Verification

No customers under the age of 18 can register an account. The system does not allow persons under 18 to register an account.

The Company uses SumSub tool for age verification processes.

4.4. Duplicate accounts

Players are only allowed to hold one account. When a player registers, the details are checked for possible duplicate accounts. Should the checks indicate that a duplicate account has been registered; the account is suspended until further checks are made to determine whether or not this is indeed a duplicate account. If the checks prove that the account is indeed a duplicate account, the account will be closed.

Should the fraud management department have any doubts about any of the information submitted at registration stage or have any doubts whatsoever, further identification verification should be carried by requesting supplementary documents from the player. The documents requested are:

- scan of identification document e.g. id card or passport
- scan of credit card (if required)
- valid proof of address e.g. utility bill (not older than 6 months)

Should the fraud department still not be satisfied, they should ask for further documents. If in doubt the MLRO should be consulted.

4.5. Due Diligence

Player KYC and due diligence shall be ongoing and conducted on a risk-sensitive basis in situations, which by their nature, represent a higher risk of Money Laundering or Financing of Terrorism. The Fraud & Payments Manager is responsible for setting out a matrix which scores

risk according to criteria which influence the risk rating.

4.6. Standard Due Diligence

The following events will trigger the standard due diligence procedures and the account will need to be verified further:

- *Request to change account details like address, email etc.*
- *Attempts to withdraw using a method other than the one used to fund the account*
- *Accumulated transactions (Deposits and/or Withdrawals) above 2,000 Euro or 4,000 NAF*
- *Customer's activity raises suspicion.*
- *There are doubts about the veracity or adequacy of previously obtained customer identification data.*

Verification will take place by either of the following:

1. *Third party verification*
2. *Submission of the following documents:*
 - *scan of identification document e.g. id card or passport.*
 - *valid proof of address e.g. utility bill (not older than 6 months)*
 - *Proof of payment method ownership*

4.7. Enhanced Due Diligence

In cases where players, products or transaction are deemed to be of higher risk Enhanced Due Diligence (EDD) procedures should apply. The following events should trigger the EDD procedures:

- Player is a PEP (Politically Exposed Person)
- duplicate IPs
- IP shifting
- country of origin associated with higher credit card fraud
- attempts to create multiple accounts
- attempting to withdraw funds without using the funds to play
- splitting a withdrawal in several lower amount withdrawals in order to avoid hitting the verification threshold etc.
- Sudden changes in account activity
- For every account deemed as High Risk an Enhanced Ongoing Monitoring of the business relationship will be conducted.
- Player is deemed as VIP.
- The registered country is not part of the FATF white list.

In situations where EDD check is required the customer has to submit ID, utility bill and bank statement and proof of the source of funds for Enhanced ID Check within 30 days. If the customer does not send these documents within 30 days, the gaming account will be blocked from all transactions.

4.8. Record Keeping

The Company will keep the following records:

- transaction documents
- due diligence information

- information relating to suspicious transactions
- MLRO reports
- training in relation to AML matters, and
- policies and procedures

This information could be required on a timely basis by regulatory authorities. The documents as outlined should be kept for 5 years from the date of the transaction or the date of completion of any related transaction. Customer due diligence information, or copies thereof, must also be kept for a minimum of 5 years from the date the person concerned ceases to be a registered customer or from the date of the customers most recent activity. These records can be kept in documentary or electronic format.

4.9. Politically Exposed Persons (PEPs)

A Politically Exposed Person is someone who has been entrusted with a prominent public function, such as a senior political figure. Individuals who are closely related to this person, for instance, immediate family members and close associates, are also considered as PEPs. PEPs are classified as a money laundering risk since they may be exposed to property that has been generated by corruption and bribery because of their position.

As a general rule within the daily work flow every client that has been identified as high-risk, EDD measures will be applied, and also additional checks are made to identify if the client is a PEP. EDD measures are applied to the customer identified as PEP and the close associates, in compliance with the directive.

The current PEP lists are consulted in order to identify a customer as PEP. Once established as PEP, the following steps are taken:

- Obtain the approval from risk management to maintain the business relationship.
- EDD measures are applied.
- Ongoing monitoring of the customer's / business partner activity.

5. Employee Training and Screening

5.1. Training

It is imperative that staff receive appropriate and regular training as to their responsibilities with regard to:

- customer due diligence measures
- record-keeping procedures
- internal reporting procedures
- policies and procedures on internal control, risk assessment, risk management, compliance management and communications that are adequate and appropriate to prevent the carrying out of operations that may be related to money laundering or the funding of terrorism
- relevant regulation in each jurisdiction where a license is held; and
- the recognition and handling of transactions carried out by, or on behalf of, any person who may have been, is, or appears to be engaged in money laundering or the funding of terrorism.

Records are kept of all training given to staff together with confirmation that they have reached

the necessary level of understanding and competence.

5.2. Screening

Staff who are dishonest present a fraud and business risk to remote gambling operators. The Company ensures that there is in place appropriate procedures for due diligence when hiring employees.

This could include reference checks, credit record checks and other vetting measures including verification of information given during the recruitment phase, and confirmation of identity.

To summarize, employees should:

- be identified and verified
- be screened to ensure their probity
- receive appropriate training

6. Additional Monitoring Tools

Covary Solution

The Company applied tools provided by Covary Solution to protect its online business from various types of fraud and reduces operational overhead. Covary Solution brings together event chain analysis, feature engineering, rule management and machine learning to obtain the most accurate results. Covary Solution analyzes the global base of fraudulent and reliable identifiers and makes an automated decision whether an event should be accepted, rejected or whether it requires individual attention.

SumSub and Identomat System

The Company applied tools provided SumSub and Identomat Systems for lawful purposes of remote identity verification, fraud prevention, enforcement of AML/CFT laws and regulations, internal risk management and due diligence procedures, and other similar purposes (including AML Screening: International Sanctions, PEPs, Watchlists and Adverse Media).

7. Know Your Business – KYB

The Company applies KYB procedures in order to verify the identity of the business partners. This includes checks on background of business partner, its directors and the beneficial owners (and all individuals/entities in a holding structure of the business partner), with whom the Company contract or intend to contract.

The Company requests from each suppliers, providers and contractors with the KYB procedure:

- Company corporate ownership chart indicating all companies in the shareholding structure up to UBO/UBOs. If ownership is exercised through one or more companies, it is necessary to provide company certificates for each company up to UBO/UBOs;
- Extract from Register of equivalent document (corporate certificates) indicating directors, shareholders, registered address;
- Memorandum and Articles of Association of the company;
- Passport copies in regard to all UBOs and Directors indicated in the corporate structure;

- Utility bills or other evidence of residential address not older than 3 months in regard to all UBOs and Directors indicated in the corporate structure.

The Company reserves the right to request further documentation and information that the MLRO considers necessary to identify background of the suppliers, providers and contractors.

8. Reporting

The Nominated Money Laundering Reporting Officer is responsible to ensure that, when appropriate, the information or other matter leading to knowledge or suspicions, or reasonable grounds for knowledge or suspicion of money laundering is properly disclosed to the relevant authority. The MLRO will liaise with the relevant law enforcement agency on the issue of whether to proceed with a transaction or what information may be disclosed to customers or third parties.

The MLRO acts independently.

Any member of staff that has a suspicion that a customer is engaged in money laundering should report the matter to MLRO whose task is to decide whether it should be reported to authorities, which can also provide guidance on how to deal with suspicious customers. These reports will be delivered via an internal form, which will be kept on record even though the MLRO decide to not take the reported activity further.

The Board will also be responsible for ensuring this policy is implemented and that risk assessment is regularly updated. The Board complies as a minimum yearly report covering operation and effectiveness of the Company' policies and procedures to overcome the threat of ML. The Board should respond promptly to any reasonable requests for information made by a Regulator or law enforcement authorities.