

WinHolding B.V

Player Registration and KYC Procedures

DOCUMENT HISTORY

Version	Date
0.1	01.04.2026

Table of Contents

Introduction.....	3
Identification and Verification.....	4
Identification	4
Verification triggers	5
Threshold Approach.....	5
PEPs – Politically exposed persons	5
VIP customers.....	6
Methods of Verification.....	6
Sources for verification.....	7
Additional Documents	7
Customer Details Renewal Procedure	8
Ongoing Monitoring.....	8
Obligations	8
Transaction Monitoring.....	9
Enhanced Due Diligence	11
Record Keeping	11
The Client account file	11
Politically Exposed Person (PEP) records.....	12
Suspicious Activity Report (SAR) records	12
Risk Assessment.....	12
Client Risk Assessment.....	13
Products, Services and Delivery Channels	13
Geographic Locations and Areas of Operation.....	13
Customer Relationships	14
Regulatory risk.....	15
Risk Matrix / Categorisation of Players.....	15

Introduction

As part of ensuring compliance with regulatory requirements, maintaining integrity and managing business risk, WinHolding B.V (hereinafter referred to as “the company”) seeks to carry out a confirmation of its customer’s identity details during the life of the player’s account. This process is

called KYC process and is based upon the risk-based methodology that is current best practice in anti- money laundering and compliance guidelines. It seeks to check the identity of customers at the point when an account “trips” a risk-based trigger. A web of triggers is made to cover all elements of risk- related activity based upon financial, betting or account activity and is continually reviewed and amended to ensure that it continues to cover all elements of possible risk.

The methods used to complete the KYC process use the best available information for each country. The standard of information and identity checking services varies significantly from country to country, so there are a wide variety of methods to complete an identity check. The methods are continuously reviewed new data sources sought to improve the confidence in the results and reduce the burden upon the customers where possible.

KYC (also known as CDD – customer due diligence) comprises identifying the customer and verifying their identity on the basis of documents, data or information obtained from a reliable and independent source in addition to other measures listed below.

CDD includes:

- a) customer’s account registration process preventing underage players from creating accounts and verifying the customer’s email
- b) identifying the customer and verifying their identity on the basis of documents, data or information obtained from a reliable and independent source
- c) identifying the beneficial owner and taking reasonable measures to verify that person’s identity so that the obliged entity is satisfied that it knows who the beneficial owner is
- d) assessing and obtaining information on the purpose and intended nature of business relationship
- e) undertaken throughout the course of that relationship to ensure that the transactions are consistent with the obliged entity’s knowledge of the customer, the business and risk profile, including where necessary the source of funds and ensuring that all data kept is up to date

Identification and Verification

Identification

In order to place a bet, the customer must register an account providing valid personal details: Name, Date of Birth, Address, Phone number and Email. The option to choose a date of birth making the customer underage is automatically blocked (checking day/month/year). After submitting all personal details, the customer receives an email with a verification link (sent to the one in the registration form) in order to complete their account registration.

Every time the customer is trying to access his/her account, he/she is being identified by his email address and password. Based on the customer’s overall account activity, WinHolding B.V.

seeks to identify any suspicious patterns and mismatches to protect its customers from fraud and ensure business continuity.

Where the Company is not able to apply CDD to a customer, it must not establish a business relationship or carry out occasional transactions with that customer. It must terminate any existing relationship with the customer and consider whether it is required to make a disclosure to the relevant authorities.

Verification triggers

Customer will undergo customer due diligence (CDD) or enhanced due diligence (EDD) when:

1. Reaching the threshold
2. Deemed a PEP (EDD)
3. Considered a high roller (EDD)

Threshold Approach

The Company utilizes the threshold approach which it applies to all customers. Moreover, CDD must be applied when there are suspicions for ML or CFT regardless of any threshold.

When the threshold stated above is met:

- The Company block the customer's withdrawals until CDD measures are completed
- Once CDD is completed, the business continues as normal
- If it cannot be completed, then the Company will terminate the business relationship with the customer
- If money is to be paid, then the amount paid should consist of the money deposited on the customer's account up to this point (no cash deposits are permitted) which money should be always refunded to the originating account and where appropriate MLRO will submit SARs or seek consent to proceed further with that customer
- There will be ongoing monitoring of the account and if necessary, reporting any findings

PEPs – Politically exposed persons

A PEP is a person entrusted or who was entrusted within the last year with one of the following prominent public functions:

- heads of state, government, ministers and deputies
- members of parliament

- members of governing bodies
- members of courts
- ambassadors
- members of management of state-owned enterprises
- family members of PEPs
- close associates to PEPs

At account opening and/or in cases provided by the applicable legislation WinHolding B.V will determine whether a customer relationship involves a Politically Exposed Person (“PEP”) by using the services of <https://sumsub.com/>.

If the customer is determined to be a, PEP the account will be referred to senior management prior to entering into an ongoing relationship with the account applicant.

A self-disclosure question about being a PEP is included during customer sign up, however, regardless of the selected answer, WinHolding B.V will screen all prospective customers (and existing customers) on an ongoing basis utilizing a third-party service provider which utilizes a credible source of commercially or publicly available information.

PEPs will be ranked as high risk, subject to Enhanced Due Diligence (“EDD”), and no account will be opened, or large transaction proceed without the express authority of the MLRO.

When deciding whether a person is a known close associate of a PEP, the company need only have regard to any information which is in their possession, or which is publicly known.

WinHolding B.V. will have:

- appropriate risk-based procedures to determine whether a customer is a PEP;
- obtain appropriate senior management approval for establishing a business relationship with such a customer;
- take adequate measures to establish the source of wealth and source of funds which are involved in the business relationship; and
- conduct enhanced ongoing monitoring of the business relationship.

VIP customers

Any customer who on average deposits 5,000 EUR per month or more is considered a VIP.

Methods of Verification

Verification can be completed on the basis of documents, data or information obtained from a reliable and independent source. This means that there are numerous ways we can verify the customer's identity including:

- Obtaining or viewing original documents
- Conducting electronic verification
- Obtaining information from other regulated persons
- Instructing a suitably qualified third party to undertake verification
- Proof of deposit through bank statement, E-wallet screenshot showing recent transactions to the website.

Sources for verification

Evidence of Identity can include:

- Identity documents such as passports and photo cards driving license
- National identity card issued by any EEA member states

It is considered a good practice when obtaining evidence of ID to have one government issued document which verifies full name and address or name and date of birth.

The following sources may be useful for verification of customers:

- Birth certificate
- Residence permit
- Council tax bill
- Utility bill
- Bank, building society or credit union statement containing current address

Additional Documents

Additional documents may be requested from customers to substantiate their activities or to better understand their patterns:

- **Proof of Bank Account** – This may be a screenshot or copy of the bank statement stating the customer's name and IBAN and the name of the bank (for instances when a customer requests a withdrawal to be deposited to a bank account);

- Proof of Payment Card – This may be a photo or copy of the front side of the card in question or a bank statement that will include both the card details and the name of the customer (for instances when suspicious deposit patterns are identified) –
 - To protect the customer's card data, WinHolding B.V. informs them that they may obfuscate some of the card details, however, the customer's name, as well as the first and last four digits of the card number must be visible.
- Bank Statements and Payslips – These may be requested from customers displaying potentially problematic gambling patterns and when external information available on the customer does not validate the amounts being gambled. In such cases WinHolding B.V. would ask its higher volume customers for documents which would support the funds being spent on gambling.

Customer Details Renewal Procedure

Once the identity of a customer has been concluded, it does not have to be redone again. However, if there is any doubt about the information held, then that identification will be obtained again, including the identification of the customer.

WinHolding B.V. may review the customer documentation and then update it as appropriate. Any changes to identification such as a change of name of the customer would require new documents to be obtained.

Ongoing Monitoring Obligations

Ongoing monitoring means monitoring customer relationships on a periodic basis, keeping a record of the measures taken to monitor the relationship and the information obtained, keeping a record of the purpose and intended nature of the business relationship and reviewing and updating this information periodically.

The risk assessment of the customer determines how frequently we will monitor each business relationship and how frequently that business relationship information is to be kept up to date. All customer relationships need ongoing monitoring, but high-risk customers will be monitored more frequently.

Ongoing monitoring of each business relationship is intended to:

- detect suspicious activity that must be reported;
- keep customer identification up to date;
- reassess the level of risk associated with the customer's transactions and activities;
- determine whether the transactions or activities are consistent with the information previously obtained about the customer, including the risk assessment;

- understand customer's activities over time so that any changes can be measured to detect high risk
- Monitoring high-risk situations may include measures such as:
- reviewing transactions based on an approved schedule that involves management sign-off;
- developing reports or performing more frequent review of reports that list high-risk transactions, flagging activities or changes in activities from expectations and elevating concerns as necessary;
- setting business limits or parameters regarding accounts or transactions that would trigger early warning signals and require mandatory review;
- reviewing transactions more frequently against suspicious transaction indicators relevant to the relationship.

Where ongoing monitoring finds that a business relationship is high risk, then the risk assessment will treat that customer as high risk. This means more frequent monitoring of the business relationship with that customer, updating their customer identification information more frequently, and adopting any other appropriate enhanced monitoring measures (as listed below).

The frequency of monitoring will vary depending on the risk assessment of the customer, but the ongoing monitoring obligation is to monitor all business relationships.

The current scheduled frequency of review (monitoring the business relationship and updating customer identification information) is that high-risk customers will be reviewed annually, moderate risk customers will be reviewed within two years and low-risk customers will be reviewed within three years.

Transaction Monitoring

There are certain automated controls in place to monitor customer activities, for example:

- First time deposits;
- Cash-out alerts for cash-outs greater than €1,000;
- Activity alerts when customer deposits, or bet/wager €2,000 during any period of 24 hours;
- Credit Card BIN alerts (when Credit Card country differs from player account country/IP);

In addition, all cash-out requests are processed manually by the Risk and Fraud Team and are reviewed on a daily basis. Every request undergoes security checks before approval in order to determine that

If any suspicious activity has been monitored the customer service team is advised to contact the responsible Department (Fraud/Supervisor).

For example, the Sports and Casino Traders must be contacted if the customer has a high percentage of winning betting slips or suddenly a high amount of balance. The Traders will control the account, set the customer risk level for his betting behavior and leave the evaluation note on the customer account.

The Sports and Casino Traders can also be of assistance to the Customer Service department on other tasks. We can see this daily, where the Sports Traders are contacted by Agents for assistance regarding several events. These events include:

- Getting more information about a specific match. (Cancelled, Abandoned etc.)
- Checking of “Bonus hunters” – users who try and cheat their way to use bonuses by the means of duplicate bets on the same event.
- Late bets – users who try and bet on a pre-match that has already ended.
- Overall checking of a particular user’s betting slip and betting history.
- Various information that the Customer Service team does not have access to.

The RPF Team is responsible for processing of KYC Documents and for the Verification of Customers. The RPF Team will assess documents needed from a customer on a case by case basis, balancing Risk, Compliance Requirements and Business interest.

From a Compliance point of view, customers who request a withdrawal above (or in cumulative amount) €2000 must:

1. Verify his Identity;
2. Verify his Address;
3. Funds should be returned to the Deposit method where possible.

Customer Service Agents may support RPF Team by uploading documents received during customer’s interactions into the Customer Management.

CS Agents however are not authorized to verify documents nor apply changes in the Verification Status of clients.

CS Agents should not upload Card Copies which disclose all the digits of the card. Only the first 6 and last 4 digits can be visible as per the below figure. It is very important that the required digits are covered before saving the document.



Enhanced Due Diligence

Where the risks of money laundering or terrorist financing are higher, the customer will be classified as high risk and WinHolding B.V will conduct enhanced customer due diligence (“EDD”) measures, consistent with the risks identified. A non-exhaustive list of enhanced measures that will be taken to mitigate the risk in cases of high-risk business relationships is listed below:

- obtaining additional information on the customer (e.g. occupation, volume of assets, information available through public databases, internet, etc.);
- updating more frequently the identification documents of the customer;
- obtaining information on the source of funds or source of wealth of the customer;
- obtaining the approval of senior management to enter into or maintain the business relationship;
- identifying patterns of transactions that need further examination;
- increased and more frequent monitoring of transactions;
- establishing more stringent thresholds for ascertaining identification;
- gathering additional documents, data or information; or taking additional steps to verify the documents obtained;
- establishing transaction limits customised to the nature, scale and complexity of the customer;
- increasing internal controls of high-risk business relationships;
- obtaining the approval of senior management at the transaction level for products and services that are new for that customer;
- obtaining regular credit reports.

Record Keeping

The Client account file

During business WinHolding B.V creates 'Client Account Files' for all customers with whom it has an ongoing service agreement. The Client Account File consists of:

- the initial registration information, i.e. customer's name, address and other personal data;
- all documents used for identification of the customer including copies of individual identification documents;
- customer transaction data (including, but not limited to deposits, withdrawals, actions when gambling, etc.), that will be kept for ten years after the transaction.
- internal memoranda and correspondence, which includes any memo, note, email, message or similar communication that is created or received in the normal course of business, about the services provided to the customer

The Company will keep records of all customer business relationships for 5 years after the end of the relationship (the closing of the account).

This includes all customer identification information, documentary evidence of identity, risk-rating classifications and ongoing monitoring records.

Politically Exposed Person (PEP) records

Once a PEP transaction has been reviewed by senior management a record will be kept of:

- the office or position of the individual who is a PEP;
- the source of the funds (wealth and income), if known, that were used for the transaction;
- the date it was determined the individual to be a PEP;
- the name of the member of senior management who reviewed the transaction;
- the date the transaction was reviewed.

Suspicious Activity Report (SAR) records

All SARs submitted including correspondence with FIAU (or any other government agency) will be kept for an unlimited period of time.

Internal reports of suspicions will be kept for five years.

Risk Assessment

WinHolding B.V is required to and will analyse potential threats and vulnerabilities to money laundering and terrorist financing to which the business may be exposed to in a risk assessment.

The risk assessment will document and consider the following:

- Products, services and delivery channels
- Geographic locations and areas of operation

- Customers

The risk assessment may identify high-risk situations for which risk mitigation controls and monitoring may be required. The risk assessment is not static and will change over time.

When a customer is identified as high-risk, they are subject to more frequent ongoing monitoring and updating of customer identification information, as well as any other appropriate enhanced measures.

WinHolding B.V shall perform an initial risk assessment at the beginning of a new customer relationship and for existing customers on an ongoing basis.

Client Risk Assessment

Products, Services and Delivery Channels

WinHolding B.V will identify products and services or combinations of them that may pose an elevated risk of money laundering or terrorist financing. For example, products and services that support the movement and conversion of assets into, through and out of the financial system pose a high risk. Certain services have also been identified by financial regulators, governmental authorities or other credible sources as being potentially high-risk for money laundering or terrorist financing.

- wire transactions;
- transactions involving third parties;
- non-face-to-face business relationships.

Geographic Locations and Areas of Operation

Certain geographic locations potentially pose an elevated risk for money laundering and terrorist financing. These have been described by the FATF and by other resources such as Transparency International.

Clients from, or identified as linked to these countries will be regarded as high risk:

- any country subject to sanctions, embargoes, or similar measures;
- any country identified by credible sources as providing funding or support for terrorist activities, or that have designated terrorist organisations operating within their country;
- any country known to be a tax haven, source of narcotics or other significant criminal activity;
- any country identified by the Financial Action Task Force (FATF) as non-cooperative in the fight against money laundering or terrorist financing or subject to a FATF statement;
- any country identified by credible sources as lacking appropriate money laundering or terrorist financing laws and regulations, or as having significant levels of corruption.

WinHolding B.V does not do business with or provide services to anyone in any country belonging to a list of select countries subject to comprehensive international sanctions (the “Sanctions List”).

Customer Relationships

The risk assessment requires to know your customers (“KYC”). This is not limited to identification or record keeping, but it is also about understanding the customers – including their activities, transaction patterns, and how they operate.

Examples of the factors that will be considered are:

- how long we have known the customer and had a business relationship;
- customers wanting to carry out large transactions;
- customers with regulatory or enforcement issues;
- customers with multiple online complaints;
- customers whose identification is difficult to verify;
- customers whose who are politically exposed.

A tiered approach is applied to identification and risk assessment of customers, both at the start of the relationship and on an on-going basis.

- If a player has not reached the €2,000 threshold of deposits or withdrawals the risk assessment to be carried out at this early stage will be based on the information obtained at registration such as the jurisdiction of residence of the player and on information obtained from searches and screening carried out on the player.
- Once the €2,000 threshold is met, the player will be re-assessed. During this re-assessment – WinHolding B.V obtains comprehensive information in relation to the purpose and intended nature of the business relationship for each player (this is further defined in the WinHolding B.V KYC Policy and Procedure). The collected information is factored into the customer risk assessment. Furthermore, the information obtained on the customer’s deposit method and game play between registration and the reaching of the threshold is also reflected in the re-assessment of the customer.

Each customer is risk-rated as either posing a low, medium or high risk of money laundering and/or terrorist financing. The rating given at the beginning of the business relationship may be adjusted after the re-assessment and may change over time. The level of customer due diligence will vary depending on the risk rating of the customer at the beginning of the relationship and as it changes. For all high- risk players, enhanced due diligence (“EDD”) is applied right away.

Regulatory risk

Regulatory risk means not meeting our obligations under applicable legislation. Examples of breaches of regulatory obligations include:

- customer identification not done properly;
- failure to train staff adequately;
- not having an anti-money laundering and anti-terrorist financing (AML/CFT) program;
- failure to report suspicious transactions;
- not having an MLRO;
- failing to keep complete customer records.

Risk Matrix / Categorisation of Players

For ongoing monitoring, all customers are classified with a risk tier. The risk tier can be offset by a lower risk factor in certain circumstances:

- Customers will initially be risk ranked according to the following:
 - Products and services they use
 - Their geographic location
 - The payment types they use
- The MLRO will define high risk customer types, geographic locations and payment types and risk thresholds following regulatory guidance and will report the risk rules to Senior Management for approval
- High risk status due to being a Politically Exposed Person ("PEP") cannot be offset if the connected person is still a PEP
- Higher and moderate risk customers can be classified as moderate or lower (one tier down) if the geographic location is LOW risk
- Higher and moderate risk merchants can be classified as moderate or lower (one tier down) if they have been a customer for over five years and if no issues were identified during that time.
- The ongoing monitoring may give rise to factors which will allow an amendment of the risk tier of a customer
- Some customers may be prohibited from using WinHolding B.V products and services (for reasons that include but are not limited to age restrictions and self-exclusions). Restricted status cannot be offset, but for clarity, a "restricted" customer is not necessarily a high-risk customer.
- High risk status applies to PEPs, non-face-to-face relationships, certain geographic locations and certain types of payment
- Moderate risk status applies to certain geographic locations.

- Generally, countries which are EEA members and FATF members, will be classified as of low geographic risk, as will countries which are usually regarded as being “equivalent jurisdictions”
- The MLRO will include in their annual report to Senior Management the relative customers and volumes in each risk tier. There will be an annual review of the risk scoring by Senior Management and the MLRO to determine ongoing risk policy as part of the annual AML/CFT Risk Assessment