Olistek N.V. (the “Company”)

KYC POLICY

VERSION CONTROL

Version	Version Date	Approved By
1.0	29 January 2025	The Board

CONTENTS

1. PREAMBLE 5
THE POLICY 5
2. CUSTOMER REGISTRATION, VERIFICATION, BANKING AND MANAGEMENT 6
2.1 TERMS GOVERNING CUSTOMER ACCOUNTS 6
2.2 CUSTOMER REGISTRATION AND ACCOUNT RECOVERY 6
2.3 CUSTOMER IDENTIFICATION AND VERIFICATION 7
2.4 CUSTOMER FUNDS ON ACCOUNT 9
2.5 CLOSING ACCOUNTS 10
2.6 CUSTOMERS AT RISK 11
2.7 ACCEPTING WAGERS 12
2.8 CUSTOMER COMPLAINTS 12

ABBREVIATIONS

AML ..... Anti Money Laundering

CDD ..... Customer Due Diligence

DD ..... Due Diligence

KYC ..... Know Your Customer

MLRO ..... Money Laundering Reporting Officer

PEP ..... Politically Exposed Person

STR ..... Suspicious Transaction Report

T&C ..... Terms and Conditions

TF ..... Terrorist Financing

1. PREAMBLE

THE POLICY

The Policy outlines the general unified KYC standards and procedures which must be adhered to by Olistek N.V. (Hereinafter — «the Company») its directors, officers and employees, as an important integral part of Company's operations. Due to non-face-to-face nature of remote betting services, properly establishing customer identity is one of the paramount objectives for Company to mitigate AML, TF and Fraudulent Activity risks. The Company management, officers and employees liaising with customers must study and have proper working knowledge of the Policy set herein.

2. CUSTOMER REGISTRATION, VERIFICATION, BANKING AND MANAGEMENT

2.1 TERMS GOVERNING CUSTOMER ACCOUNTS

During the registration process, each customer is required to review and accept the T&C. In the event of any updates, modifications, or amendments to the T&C, customers are responsible for familiarizing themselves with the latest version. Agreement with the updated T&C is automatic and requires no further action from the customer.

All customer's data are processed according to the T&C, which are accepted by each Customer during the registration. No processing of data is done for unregistered users. Only authorized employees have access permissions to the data. Access and disclosure of the stored data to third parties is prohibited by internal rules and policies. All data is stored with compliance of the National Ordinance Personal Data Protection (Landsverordening bescherming persoonsgegevens, National Gazette 2010, Consolidated text no. 84) and the GDPR, which is not only relevant to businesses established in the European Union but also to international businesses established in Curaçao.

2.2 CUSTOMER REGISTRATION AND ACCOUNT RECOVERY

Each person who wishes to use the services offered by the Company is required to register his or her personal account. The registration of the personal account requires a confirmation that the customer has completed the age of 18 years' old. During the initial account creation stage the user provides only basic information, however, at a later stage he or she will need to provide additional information, with some, or all data mentioned below:

- Name and surname: as specified in passport/ ID of the customer;
- Place and date of birth;
- Nationality;
- Country, city, place of residence;
- Number and series of the identification document;
- E-mail address;
- Mailing Address;
- Phone number.

If the customer didn't fill all the necessary fields in the registration form, the system will not allow him or her to proceed with completing the registration process. Information provided in the registration form are reviewed using the according to the AML Policy (ML & TF Risk assessment). After confirming the registration by clicking on the verification link in the invitation sent to the email address of the Customer, the Customer can access the account by entering account's login and password created during website registration. The password can be changed by the Customer at any time on the website, after the authorization procedure.

Safety of the customers' account relies firstly on the secret password, which no one knows except for the customer and also the unique ID number. If the customer has any suspicious that the account was hacked, he or she must contact the support team, which will immediately block the account till proper investigation is done and the customer will be satisfied that his or her account is verified. Also, the Operational Department constantly reviews the activity of the customer, verifying details such as:

- The IP addresses the Customer has accessed the website;
- Types of games and style of bets;
- Payment Systems used by the Customer.

If any unusual behavior is identified by the employees of the Operational Department, they will proceed with blocking the activity on the customer's account for a short period of time in order to check whether the customer performs actions by himself or there are indications of fraud. As for the internal controls, the Operational Department on a daily basis generates the Manual adjustment report and review any manual changes that were done to the customer's account.

If the customer forgets his/her Password, ID or is asking about some specific information through the Support chat, he/she is required to submit to the Support team his/her registered name and surname, have an access to his/her registered email and be ready to answer the secret question, or provide additional evidence to confirm the account ownership (a selfie with the declaration and / or personal ID or passport).

After the successful restoring, the customer will receive an automatic email with new link for the activation of his/her account and new password.

2.3 CUSTOMER IDENTIFICATION AND VERIFICATION

The Company will proceed with verifying the identity of the Customer and the information he/she has submitted during the registration before the his/her first bet. Initial verification is carried out by the Company in order to confirm that the gaming account has been registered on real data and that the Customer had reached the age of 18 years old.

At its discretion the Company may require additional proof of identity of the Customer at all times, regardless of that the Customer has passed the initial verification. The list of additional documents may include (but is not limited to) a digital photo of the Customer holding his or her:

- Passport;
- Identity card;
- Birth certificate;
- Utility bill;
- Bank statement for the account/card;
- etc.

The Customer can provide these documents by sending an email to the support email address mentioned on the website. Under normal circumstances, verification of the betting account holder identity is processed within 24 hours from the date of submission of the documents confirming the identity of the Customer. Registration of the account on the website for any other than a physical individual is prohibited.

The full DD Procedures, include Verification, Identification procedures, AML & TF Policy are developed using the risk- based approach described in AML Policy. In order to perform the DD controls, employees use automatic controls, manual reviews and electronic registers.

Enhanced Customer verification could be done in any time of the customer's activity, starting from the registration process and continuing through all further processes – deposits, bets, withdrawals.

Enhanced controls include full document verification plus any additional requirements until the employee of the special department standards are met. For example – at least two documents, which confirms the address, photo with his or her ID in hands etc.

If the employee from the relevant Department of the Company suspects that there is a PEP application, the Compliance Officer is notified, who communicates and agrees further actions with the Management of the Company or on his/her sole decision.

In certain cases, the Company's employees responsible for the customers, use Third Party databases to check the customers.

Following databases could be used:

- United bookmakers' databases which include list of fraudulent players;
- Payment systems data offering reconciliation to the records of the customers;
- Black lists of non-trustful customers;

Payment systems have a good developed DD and customer identification procedure. That's why Operational and Payment departments, who perform controls often refer to the data provided by the Payment systems in order to reconcile information provided by the customer in his registration form with the information recorded in Payment System database. In the blacklists employees who perform controls can find list of persons, which were blocked according to the certain reasons. And finally, Payment Systems send automatic or manual notifications, if they detect any suspicious transaction. All these notifications are checked and assessed by the responsible employees of the Company.

The Company can use additional databases, as mentioned below:

- Risk Intelligence database (for example, World-Check, KYCAID);
- Any other public source of information and databases.

According to the Company's T&C, one customer is allowed to have no more than one account.

The customer is responsible for the proper notification and update of any changes to his/her submitted registration data. The changes are processed according to the following procedure:

- The customer sends the request for update of his/her submitted data from his/her registered email. The customer must include his/her User ID number to the description;
- The Support Department upon receiving the e-mail and after reviewing the request, forwards the email to the Operational (Factoring and Monitoring) Department;
- Operational Department checks the correctness of the initial information and compares it to the registered customer's data;
- If everything is correct, the Operational Department reviews the request for changes and requests for any additional supporting documents if needed;
- Customer's data is updated in the System;
- Customer receives an email with the confirmation of changes;

The control includes also internal check of any manual changes done by the employees of the Company.

The company employs an ongoing onboarding procedure for the customers in order to identify new risks which arise during the relationship with the customer. All the customers are attentively monitored throughout any actions that they perform on the website controls on customers, controls on deposits, controls on bets, withdrawals by the fraud detection team. An ongoing review is performed according to a Risk-based approach described in the AML policy. Should a customer not be able to adequately complete CDD to the requirements of the Company the company will terminate its relationship with the customer. On a case-by-case bases, the Company will review failed CDD to determine the need for the filing of a STR (with the relevant Governmental entity). Enhanced CDD is required when unusual activity is discovered by the fraud team. An annual audit of CDD cases is performed to ensure ongoing compliance with CDD.

2.4 CUSTOMER FUNDS ON ACCOUNT

The Company does not accept cash, checks by mail etc. from players. Should a player have an unusual activity that further warrants suspicion (unusual changes in address, deposits or gambling activity) as determined by the Anti- Fraud Department, then enhanced CDD will be performed. These are following accepted ways for deposit in the gaming account:

- Through electronic systems (e-wallet, electronic money);
- By credit card (VISA/MasterCard);
- Prepaid cards;
- Other alternative payment methods.

The customer visits the website and after the successful log-in to his/her account, he can navigate to the web-page where he can make the deposit. The payment system list will appear for selection and the customer will choose the payment method to make his/her request. On the page with the payment method, the customer can also check the percentage of the commission for each payment type.

If the customer selects electronic system, he/she has the possibility to make the payment on the webpage of the private wallet of the payment system. One payment system wallet can be used for deposits of only one customer's account. In addition, the Payment System checks the legality of the funds, according to the agreements with each Payment system. When the customer makes the deposit by credit card - the customer's data are checked with the data submitted to his/her Payment System.

The company allows customers to have more than one active deposit mechanisms. Checks described above are performed for any type of deposit payment method. The risk of such customers is increased according to the risk-based approach concerning their withdrawals. The customer should select for withdrawal the payment system among those he had made the deposit. Further controls developed to mitigate higher risk for multiple deposit mechanisms are described further.

The Company is not liable in case where the customer’s account will not be credited within a specified time by fault of third parties (banks, payment processors, communication channels, etc.) or due to force majeure.

The Company doesn’t allow wagers based upon non-guaranteed funds. The system does not permit credits or loans to the customers.

After the customer has placed a bet, the system debits the amount of wager to the customer's account. The Company review the results calculated after each match for their correctness, as their performance is linked to the result. The correctness of the match result is checked by the relevant department. The system then credits the funds into the customer's account after the event/match is completed. Customers' funds are not transferred to any associates. All transactions on the account are recorded in the trading platform system. Records are maintained on the Company's servers and instantaneous back-up is performed.

The Customer initiates the request for withdrawal in his personal account and fills a special form. Each withdrawal is done to the same source from which the payment was made. Withdrawal from the customer's account is available only after verifying that the personal data of the owner of the gaming account also match and/or correspond to the personal data of the owner of the account of the payment method used for the deposit. Money transfers in favor of other persons are strictly prohibited regardless of the degree of kinship with the Customer.

Additional detailed information regarding the deposit and withdrawal of funds is mentioned in the T&C of the Company. No customer to customer transfers are possible within the system.

In case of fraud suspicion (multi-accounting, using of any software for automated betting, arbitrage betting, if the player's account is not used for betting and other products offered by the Company, abuse of loyalty programs, etc.) the Company reserves the right to suspend operations and / or the payments to player account at the time of player activity verification until its completion.

If the Operational Department discovers any unusual transaction (ie a rejected transaction) they will notify the MLRO for appropriate measures to be undertaken. A suspicious transactions report can be filled with Financial Investigation Unit of Curaçao.

2.5 CLOSING ACCOUNTS

The Company and monitors and keeps a register of all the inactive accounts. After the Customer registers on the website, a notification is being generated and sent via the registered email address to the Customer. In addition, it is possible to contact the account owner via phone. All inactive accounts that have a transaction history are note removed from the system.

The Operational Department permanently monitors the Customer's transactions. If an employee of the relevant Department detects unusual and/or suspicious activity, then the customer's account may be blocked for a limited period so as to investigate it. Moreover, the Company has the right to cancel bets, forfeit winnings, and deduct bonuses from all relevant betting accounts.

The Company considers the following activities as suspicious:

- The Customer is opening more than one betting account (for example, using same or similar names, address, telephone, emails, same or similar dynamic IP address, computers or other devices, etc.); and/or
- The Customer is acting as a part of syndicate (using same or similar names, address, telephone, emails, same or similar IP address, computers or other devices, acting on same or similar pattern).

After suspending the account, a notification appears on the customer's page and the Support Team requires information and/or documents in order to check the suspicious action. Also additional information may be requested from affiliates who are processing deposits and withdrawals from the betting account, in order to obtain information about the origin of the funds.

The customer still has the possibility to access his/her personal account during the investigation process but the funds will remain frozen and no transactions will be allowed until the investigation is completed.

All investigation steps are recorded in the system. If the investigation is completed successfully, the relevant Department will unblock the account and the customer will be able to manage his/her funds again. If there were no response to the notification or the customer did not provided enough data to complete the investigation - the account will remain blocked until the requested documents are received.

2.6 CUSTOMERS AT RISK

According to the KYC Policy and T&C of the Company, individuals under age of 18 years old are not permitted to register and play.

The Customer bares the personal responsibility for providing false information. If the Company discovers that the Customer has provided any false information, then the Company is entitled to take all necessary measures as described in the KYC Policy and T&C of the Company.

If it is discovered that a minor is using the gaming account, then the said account will be blocked immediately and all transactions in processing will be cancelled. Any funds remaining in this account will be returned to the owner of the account. Should it be discovered that an underage player has deposited funds, the balance of those funds will be returned to the minor.

There are 3 ways of identification of the gambling problems and the respective following steps for each type of it:

- The customer informs the Support team by himself about his gambling problem through e-mail or live chat or telephone. The Operational Department evaluates and takes all necessary actions towards the account. The customer is notified about the changes done to his account via e-mail;
- While communicating with the customers, the Support Team identifies the problematic gambling customers. Usually, such customers are harassing the Support Team or other customers or exhibit compulsive gambling behavior;
- Operational Department performs constant Operational and AML analysis of all the customers' actions. One of the triggers that is monitored by the department is problem gambling trigger. The Support department contacts the customer and proposes to the customer to set up self-limitation with the most comfortable and suitable conditions for the customer.

After identifying a problem gambling customer through the above-described ways, the customer received the "Problem gambling" status in the Company's system.

In order to adhere to the principles of Responsible Betting, the Company obliges to always accept and enact electronic requests for player self-limitation. The customer is entitled to limit their gambling spend, set time limits or even take a pause by sending respective request to the Company via electronic mail or through his/her gaming account including their User ID and specific type, amount and time period of limitation. Customers seeking better understanding of the types of limitations that can be enforced are encouraged to contact the Company's Support Team.

2.7 ACCEPTING WAGERS

Wagers can only be accepted from registered customers, that have passed the DD process and have registered their personal account for the website. Wagers can be accepted in any circumstances, except were:

- There are not enough funds in the customer's account;
- The customer was required to perform enhanced additional DD, but hasn't finish it yet;
- The Operational Department has shortly blocked the account based on unusual and/or suspicious actions until the customer confirms that everything is correct.

2.8 CUSTOMER COMPLAINTS

In the event of a dispute, it is advisable that the Customer lodges a written complaint to the Company through the Customer Support service.

The complaint must contain clear and unequivocal information about the complainant's identity and shall give all the relevant details that gave rise to the complaint, including the relevant financial documents confirming the payment of the placed bet(s).

The Customer and the Company should do their utmost to reach an amicable settlement within a reasonable time.

Any dispute or claim arising out of or in connection with the T&C, KYC Policy or its subject matter, whether of a contractual or non-contractual nature, shall be governed by and construed in accordance with the laws of Curacao.

If for some reason the customer is not satisfied with the resolution of the complaint by the Company, he/she can lodge a complaint with the local regulatory authority of Curacao.

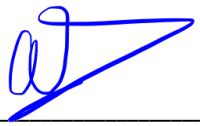
3. CONCLUSION

In conclusion, this KYC policy serves as a critical framework to safeguard our organization, customers, and the broader financial ecosystem against risks associated with identity theft, fraud, and money laundering. By adhering to rigorous verification processes, maintaining accurate records, and continually updating our compliance practices, we demonstrate our commitment to ethical business standards and regulatory compliance. This policy is designed to create a safe and transparent environment for all stakeholders, supporting trust and security in our operations. As part of our ongoing efforts, we will regularly review and update this policy to reflect changes in regulatory requirements and best practices, ensuring our approach to customer verification remains robust, effective, and adaptable to emerging risks.

4. RATIFICATION

The Policy will be valid for a period up to its annual or required reviewing.

In witness whereof, Olistek N.V. has caused this Policy to be duly executed this day of 29 January 2025.



1/29/2025

_____

Director eMagnus Curacao B.V.

Andrea Engelhardt

