

Know Your Counterparty (KYC) Policy

1. INTRODUCTION

In our Know Your Counterparty (KYC) Policy, we recognize the importance of preventing money laundering and terrorism financing and we commit to high standards of business integrity.

2. RISK ASSESSMENT

The Company is required to assess on a yearly basis the risks of Money Laundering and Terrorist Financing, taking into account risk factors:

- Governance;
- Customers/Partners;
- Countries or geographic areas of operation;
- Employees;
- Products or services; and
- Payments.

The purpose of AML risk assessment is to identify, analyze, assess and mitigate any potential ML/FT risks and any other associated risks that the Company may be exposed to in relation to laundering of proceeds of crime and financing of terrorism.

Applying Risk-based Approach means that the Company has to:

- Assess the risks that Money Laundering or Terrorist Financing may occur within its organization beforehand;
- Design and implement appropriate policies, procedures and controls to manage and mitigate the identified and assessed risks;
- Monitor and improve the effective operation of these policies, procedures and controls;
- Record the risk assessments, including everything that has been done and the reason for this being done.

The steps of the risk assessment methodology are as follows:

- Identification
- Analysis and Assessment
- Taking appropriate actions to ensure effective minimization or mitigation of identified risks.

This approach also allows Company to prioritize its actions and focus on risks presenting greater severity and likelihood of materialization.

The Company will collect certain Customer's identification information from each Customer; utilize risk-based measures to verify the identity of each Customer; record Customer identification information and the verification methods and results; and compare Customer identification information with government-provided and other public resources.

The Company will collect certain Partner identification information from each Partner:

- For the Partner and corporate shareholder of the Partner:
 - a) Certificate of Incorporation/Registration;
 - b) Certificate/Corporate Register of Directors;
 - c) Certificate/Corporate Register of Shareholders;
 - d) Memorandum and Articles of Association;
 - e) Certificate of Good Standing (not older than 6 months);
 - f) Operating License Certificate;
 - g) Corporate Structure.
- For each Individual Director the copies of the following:
 - a) Passport or ID card (Certified copy);
 - b) Copy of the utility bill (not older than 3 month).



- For each Corporate Director:
 - a) Certificate of Incorporation/Registration;
 - b) Certificate/Corporate Register of Directors;
 - c) Certificate/Corporate Register of Shareholders.
- For each Beneficial Owner:
 - a) Passport of ID card (Certified copy);
 - b) Copy of the utility bill (not older than 3 month).

The Company complies with local and international regulatory requirements, sanctions lists of competent authorities (FATF, UN, EU, OFAC) against countries, legal entities, financial institutions and natural persons.

The screening procedure, taking place at first deposit and throughout the course of the Business Relationship, includes screening against Sanctions Lists, PEP Lists.

Wherever a match with a sanctioned individual is determined to be a true match, the following steps will take place:

- Relationship with the Customer are terminated or not established;
- Compliance Officer informs Management;
- Compliance Officer shall file a report to relevant FIU, if apart from Customer/Partner being sanctioned, there is also knowledge or suspicion on AML/CFT; and,
- Compliance Officer shall report to the respective governmental agencies for further guidance in relation to blocking and freezing of funds.

Wherever a PEP is identified, the following steps will take place:

- Senior management approval to service the PEP should be obtained;
- Source of wealth and, where applicable, their source of funds should be established;
- Enhanced on-going monitoring of the Customer's activity should be conducted.

3. KNOW YOUR CLIENT

Customer Identification and Verification:

The Company has established standards regarding KYC. These standards require due diligence on each prospective Customer before entering into a Business Relationship:

- via identification and verification of his identity and, as the case may be, his representatives on the basis of documents, data or information obtained from a reliable and independent source compliant with the domestic and European anti-Money Laundering legislation and regulations;
- via obtaining information on the purpose and intended nature of the Business Relationship.

Prior to opening an account for the Customer, the Company will collect the following information for all accounts for any person that is opening a new account and whose name is on the account (Preliminary identification):

- a) the Customer's full name;
- b) the Customer's permanent residential address;
- c) the Customer's IP address;
- d) date of birth;
- e) place of birth;
- f) nationality;
- g) identity number.

The Company does not allow its Customers to open anonymous accounts. In low risk scenarios the Company may limit identification to the personal details set out in (a) to (g) above.

The Company does not allow its Customers to make any Transactions or money withdrawal from the accounts till Complete identification (hereinafter – the "Complete identification").

Prior to allowing any Transactions or money withdrawal from the account for the Customer the Company will conduct Simplified Due Diligence and collect the following information about the Customer:



- the name (name confirmation);
- date of birth (confirmation);
- an address, which will be a residential or business street address (for an individual), or residential or business street address of next of kin or another contact individual (for an individual who does not have a residential or business street address); and
- an identification number or one or more of the following: a taxpayer identification number, passport number and country of issuance, alien identification card number, or number and country of issuance of any other government-issued document evidencing nationality or residence and bearing a photograph or other similar safeguard; and
- phone number.

The Company has developed a list of documents, the provision of which is necessary for a Customer for the purpose of Complete identification, namely:

- color passport copy (first and second pages with photo, as well as a page with data of registration);
- color copy of a document, which is proper for Customer's identity verification under the law of the country of residence;
- a copy of driver's license (upon the Company's request);
- a receipt of payment of utility bills to confirm the place of residence of the Customer (upon the Company's request);

Also, the verification process involves mandatory confirmation of Customer's phone number.

Based on the risk, and to the extent reasonable and practicable, the Company will ensure that it has a reasonable belief that it knows the true identity of the Customer by using risk-based procedures to verify and document the accuracy of the information it gets about Customers. The Company will analyze the information it obtains to determine whether the information is sufficient to form a reasonable belief that the Company knows the true identity of the Customer (e.g., whether the information is logical or contains inconsistencies).

The Company will verify Customer identity through documentary means, non-documentary means or both. The Company will use documents to verify Customer identity when appropriate documents are available. In light of the increased instances of identity fraud, the Company will supplement the use of documentary evidence by using the non-documentary means described below whenever necessary. The Company may also use non-documentary means, if it is still uncertain about whether the Company know the true identity of the Customer. In verifying the information, the Company will consider whether the identifying information that it receives, such as the Customer's name, street address, zip code, telephone number, date of birth and ID number, allow us to determine that the Company has a reasonable belief that it knows the true identity of the Customer (e.g., whether the information is logical or contains inconsistencies).

The Company understand that it is not required to take steps to determine whether the document that the Customer has provided to the Company for identity verification has been validly issued and that the Company may rely on a government-issued identification as verification of a Customer's identity. If, however, the Company notes that the document shows some obvious form of fraud, the Company must consider that factor in determining whether it can form a reasonable belief that the Company knows the Customer's true identity. The company can ask to provide any other documents which can be necessary and appropriate for AML policy.

The Company will use the following non-documentary methods of verifying identity:

- Independently verifying the Customer's identity through the comparison of information provided by the Customer with information obtained from a consumer reporting agency, public database or other source [identify reporting agency, database, etc.];
- Checking references with other financial institutions; or
- Obtaining a financial statement;
- Phone calls to the Customer.

If a potential or existing Customer either refuses to provide the information described above when requested, or appears to have intentionally provided misleading information, the Company will not open a new account and, after considering the risks involved, consider closing any existing account.

4. KNOW YOUR BUSINESS

Partner Identification and Verification:

The Company has established standards regarding KYB. These standards require due diligence on each prospective Partner before entering into a Business Relationship if:

- an occasional Transaction with the Partner amounts to €15,000 or more when the Transaction is carried out in a single operation or in several operations that appear to be linked.

The Company will collect certain Partner identification information from each Partner:

- For the Partner and corporate shareholder of the Partner:
 - a) Certificate of Incorporation/Registration;
 - b) Certificate/Corporate Register of Directors;
 - c) Certificate/Corporate Register of Shareholders;
 - d) Memorandum and Articles of Association;
 - e) Certificate of Good Standing (not older than 6 months);
 - f) Operating License Certificate;
 - g) Corporate Structure.
- For each Individual Director the copies of the following:
 - a) Passport of ID card (Certified copy);
 - b) Copy of the utility bill (not older than 3 month).
- For each Corporate Director:
 - a) Certificate of Incorporation/Registration;
 - b) Certificate/Corporate Register of Directors;
 - c) Certificate/Corporate Register of Shareholders.
- For each Beneficial Owner:
 - a) Passport of ID card (Certified copy);
 - b) Copy of the utility bill (not older than 3 month).

A "Beneficial Owner" is defined for the purposes of this Policy as any individual who: (i) exercises ultimate control over the management of the body corporate; (ii) who ultimately owns or controls (in each case whether directly or indirectly), more than 10% of the shares or voting rights in the body corporate; (iii) who holds the right, directly or indirectly to appoint or remove a majority of the Board of directors; or (iv) has the right to exercise, or actually exercises, significant influence or control over the body corporate.

Where it is not possible to identify the Beneficial Owner of a body corporate after taking all necessary reasonable measures, the Company will verify the identity of the senior managing official.

The 10% threshold stated here applies without prejudice to the right of the Company to decide that a lower percentage may be indicative of ownership and control in relation to any particular Partner.

5. RECORDKEEPING

Records of personal data obtained for the purposes of the prevention of Money Laundering and Terrorist Financing are processed and kept in accordance with the EU and local requirements and shall not be further processed in a way that is incompatible with those purposes.

Company shall maintain the below-listed documents for at least 5 years, unless a longer period is specified by special national legal requirements or as required by the FIU, relevant supervisory authorities or law enforcement agencies when necessary for the purposes of the prevention, detection, analysis and investigation of ML/FT activities. Should the latter be the case, the period required by can never exceed 10 years.

The following documentation to be kept are:

- Documents containing information on the identification and knowledge of the Customer/Partner;
- Records with full details of Customers/Partners or groups of connected Customers/Partners;
- Register of all cases of prospective Customers/Partners for which the Company declines the establishment of Business Relationship;
- Register of terminated Customers/Partners;
- Investigations and Reports made to the government authorities concerning suspicious Customer/Partner activity relating to possible Money Laundering and/or Terrorist Financing, accompanying with supporting documents;
- Records of all courses and training given on the prevention of Money Laundering and Terrorist Financing; and,
- Any other documents and registers required to be retained by the special provisions of the local AML laws and regulations.

Documentation held may either be in physical format, electronically or both. In cases where documents certified by third parties, the physical document bearing the original third-party certification should be retained on file and not a copy thereof.

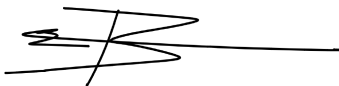
Annex 1: KYC procedures and checks (CONFIDENTIAL, FOR INTERNAL USE ONLY)

Customer pre-checks procedures	
Name	Description
IP address analysis	Analysis of an Applicant's IP address using multiple factors (whether it belongs to public/private ranges, residential proxy, anonymous VPN providers or anonymous networks, or Tor exit nodes). The geodata attributed to the IP address (e.g., country, city, coordinates) is extracted, and the IP address itself is assigned a risk label.
Identity Enrichment using email and/or phone number linked data	By analyzing the email and phone number provided by the applicant, we can find the data linked to this email and phone number. It returns DoB, Gender, Name, and address based primarily on telco and social media data.
Phone Risk Assessment	Opportunity to screen applicant's phone number to get the risk labels based on its registrations on the web, domain name, delivery option and other parameters. The risk label can be used as a condition for further checks.
Email Risk Assessment	Opportunity to screen applicant's email address and get the risk labels based on its registrations on the web, domain name, delivery option and other parameters. The risk label can be used as a condition for further checks.
Video Identification	
Name	Description
Video Identification	Platform (third party service) to carry out identity verification procedures (incl. collection of documents) via video interviews conducted by operators engaged by the Company.
Fraud Network Detection	
Name	Description
Fraud Network Detection	Continuous monitoring of Applicants' personal data, behavior and connections to detect potentially fraudulent networks, reviewing potentially fraudulent networks of Applicants and, where the suspicion is confirmed, presenting the investigation results. The Platform (third party service) groups suspicious Applicants based on shared facial images, documents, proof of address templates, IPs and device fingerprints, geo-location and address, personal information, or behavioral patterns.
Payment Method Check	
Name	Description
Payment Method Check	Verification that a bank card, crypto wallet, online payment platforms, and wire transfer truly belong to a user. Chargebacks, fraudulent Transactions, sending funds to third parties, and sending funds from suspicious accounts are eliminated by identifying the payment source before Transactions are made.

KYC	
Name (Steps)	Description
Identity Document Verification	Determination of whether an identity document is authentic, legitimate, and free of forgery or alteration.
Ongoing ID document monitoring	Daily re-check of the validity of an identity document previously submitted by the Applicant, based on its expiry date. This includes sending automated requests for replacements if a document expires.
Additional fields extraction	Extraction of custom fields, depending on regulatory requirements and/or business needs. These may include gender, tax number, address, additional number, etc.
Liveness & Face match	Biometric analysis of an Applicant's facial movements compared with photographs on the submitted identity documents in order to ensure that the Applicant is alive and present at the time of the identity verification.
Known face search	Determination of whether an Applicant's facial data is already present in the Company's databases.
Proof of Address Verification	Verification of address and residency through analysis of the following documents:- IDs bearing residential address;- Tax bills;- Utility bills;- Voter rolls;- Bank statements;- Other documents commonly accepted as proof of address.
Geolocation as Proof of Address Check	Detection of an Applicant's location using geolocation data from their device and verifying it against the pre-set rules.
AML Screening: PEPs, sanctions, watchlists and adverse media	Determination of an Applicant's presence on or absence from global sanctions lists, PEP lists, watchlists, blocklists, or adverse media (OFAC, UN, HMT, EU, DFT etc.). The results of this Check are solely based on potential matches between an Applicant's personal data and the data contained in databases available.
Ongoing AML monitoring (KYC)	Daily re-check of an Applicant's full name and date of birth against the available sanctions lists, PEP lists, adverse media, and other data sources as specified in the AML Screening description.
Email Verification	Verification of email addresses to ensure whether they are valid and belong to a real person. This includes:- Authentication with a code to ensure that the Applicant has access to their mailbox;- Cross- validation of the Applicant's name, email address, IP address country and phone number country;- Duplicate search, where possible (e.g. different persons have the same email address);- Review whether an Applicant with this email address was involved into a fraudulent activity, where possible;- Overall risk assessment of the email address, scored on a scale of zero to one.
Phone Verification	Verification of phone numbers to ensure whether they are valid and belong to a real person. This includes:- Authentication with a code to ensure that the Applicant can be reached at this phone number;- Cross-validation of the Applicant's name, email address, IP address country and phone number country;- Duplicate name search, where possible (e.g. different persons have the same phone number);- Review whether an Applicant with this phone number was involved into a fraudulent activity, where possible;- Overall risk assessment of the phone number, scored on a scale of zero to one.
Face Authentication	Biometric analysis of a person's facial movements that is compared with photographs on submitted ID documents or previous selfies. This is to ensure that a person is alive and



	to make sure of their presence at the time of the authentication.
Facial Age Estimation	The third-party solution automatically gives an approximate estimate of an Applicant's age based on the results of the Liveness Check previously passed by that Applicant. Received age estimate can be compared to the internal age limit established by the Company for its service (if any).
Document Processing	
Name	Description
ID data extraction	Automated extraction of data from identity documents for further processing. Five fields are extracted: First name, Last name, Date of birth, Document number, Date of expiry.
Bank card data extraction and sensitive data masking	Automated extraction of data from bank cards, including third-party technology that protects sensitive data in accordance with data privacy and protection laws and PCI DSS.
Proof of Address data extraction	Automated extraction of address data from documents for further processing. By default, three fields are extracted: Full name,- Address,- Date of issue.
Fraud Prevention	
Name	Description
Higher-risk applicant control and alert	Where identity theft is suspected or proven for the following reasons: Document forgery (physical or digital); Documents of another person; Stolen/leaked documents; Deepfake; Account abuse from one device; Registration coerced by another person; Account registration without the document owner's knowledge, etc.
Duplicate search	Search for Applicants with the same personal data
Behavioral risk score	Calculation of an Applicant's behavioral risk score based on various parameters: Device Fingerprinting (IP, country),- Data inconsistency,- Suspicious behavior factors.
Anti-photoshop check	Checking if graphic editors were used to change the data on the submitted images.
Security features check	Checking various parameters of a document to identify fraud patterns: fonts,- holograms,- comparing a document with its template,- reviewing the required elements of the document.



22-05-2026
Ecorpp Management N.V.
Boy Hendriks

