

WHITE FOX N.V.

**Anti-Money Laundering and Financing of Counter-Terrorism
Financing ('AML-CTF') Policy**

Document Version: 3.0.

Document Classification: Confidential

Table of Contents

Document Control	2
1. Glossary	3
2. Introduction	5
3. Policy Statement	5
4. Purpose and Objective	6
4.1. Applicable laws and regulations	6
4.2. Definitions	7
5. Policy Implementation	8
5.1 Business Risk Assessment	9
5.2. Customer Risk Assessment	11
5.3. Customer Acceptance Policy	12
5.4. Customer Due Diligence	13
5.5. Customer Ongoing Monitoring	14
6. External reporting	15
7. AML Compliance program	17
8. Consequences of non-compliance	17
9. Record keeping	18
10. Policy reviews	18
11. Contact Information	19

Document Control

Document Classification	Confidential
Distribution List	All employees, contractors and third-party suppliers
Document Owner	Legal & Compliance
Document Reviewer	Jennyfer Cubelles Torres - HRC Francesca Grech - SCO Lena Sammut - CLCO

Revision History

Version	Date	Author	Role	Desc./ Summary of Changes
1.0	21-Apr-2021	G.H.	Director	Creation and approval
2.0	24-Jun-2022	G.H.	Director	Amendment and approval
3.0	25-Apr-2025	J.C.T & F.G.	HC & SCO	Updated AML Policy in line with CGA's requirements

Document Approval Log

Version	Date	Document Approver	Role/Position
1.0	21-Apr-2021	Gouloud Hammoud	Director
2.0	24-Jun-2022	Gouloud Hammoud	Director
3.0	8-May-2025	Veysel Demir	Director

1. Glossary

Abbreviation	Term
AML	Anti-money laundering
API	Application programming interface
B2B	Business-to-business
B2C	Business-to-client
BRA	Business Risk Assessment
CAP	Customer Acceptance Policy
CDD	Customer Due Diligence
CFT	Countering the Financing of terrorism
CGA	Curaçao Gaming Authority
CRA	Customer Risk Assessment
EDD	Enhanced Due Diligence
FATF	Financial Action Task Force
FIU	Financial Intelligence Unit
KYC	Know Your Customer
MLRO	Money Laundering Reporting Officer

ML	Money laundering
NORUT	National Ordinance on the Reporting of Unusual Transactions
NOIS	National Ordinance on Identification when rendering Services.
OT	Occasional Transaction
PEP	Politically Exposed Person
RBA	Risk-based Approach
SAR	Suspicious Activity Report
SDD	Simplified Due Diligence
SoF	Source of Funds
SoW	Source of Wealth
TF	Terrorist financing
UBO	Ultimate Beneficial Owner

2. Introduction

White Fox N.V., herein referred to as “the Company”, is a limited liability company incorporated and domiciled under the laws of Curaçao on the 16th January 2017, holding company registration number 142472. The Company’s principal business activity is that of a business-to-business (‘B2B’) service provider, providing platform, products and software to business-to-client (‘B2C’) gambling operators, which includes services related to the organisation, marketing, promotion, management, support and operations. The platform offers B2C operators with the provision of a number of sought-after verticals and solutions. This includes casino games content aggregator featuring slots, live casino and bingo aggregations, a sportsbook solution, in addition to the availability of fantasy sports and lottery products via one single application programming interface (‘API’). The Company has an ongoing licence application (*application number: OGL/2024/741/0852*) with the Curaçao Gaming Authority (‘CGA’).

3. Policy Statement

The Company is committed to preventing its services from being used to facilitate money laundering (‘ML’), terrorist financing (‘TF’), or any other financial crime. This Policy applies to all business activities conducted. White Fox N.V. ensures compliance with applicable Anti-Money Laundering and Countering the Financing of Terrorism (‘AML/CFT’) laws, fostering a culture of integrity, regulatory adherence, and corporate responsibility. This Policy applies to all employees, contractors, and third-party suppliers of White Fox N.V involved in establishing and maintaining relationships with business customers.

4. Purpose and Objective

The objective of this Policy is to set out the policies, procedures, systems, and controls necessary for the Company to meet its obligations regarding AML/CFT in the context of its B2B service provision to B2C companies. This Policy sets out how management achieves this and educates the Company's employees, contractors and third-parties on the Company's AML/CFT framework.

White Fox N.V. is committed to preventing misuse of its services for financial crime including ML/FT by ensuring strict compliance with all applicable regulations. To achieve these objectives, the Company will:

- every staff member shall meet their personal obligations as appropriate to their role and responsibilities;
- commercial considerations cannot take precedence over White Fox's regulatory obligations and license commitments.

4.1. Applicable laws and regulations

The following section outlines the Curaçao Ordinances, laws, regulations, directives and international standards applicable and/or observed by White Fox N.V.:

- National Ordinance Identification when rendering Services ('NOIS')
- National Ordinance Reporting Unusual Transactions ('NORUT')
- Indicators for detecting and reporting Unusual Transactions (PB 2015, nr 73)
- National Ordinance on Games of Chance (Landsverordening op de kansspelen, P.B. 2024, no. 157) ('LOK')
- Sanctions National Ordinance
- Kingdom Sanction Act
- GCB Regulations for the combating of ML/FT and Proliferation of weapons of mass destruction

- FATF 40 Recommendations
- EU AML/CFT Directives and Guidelines

4.2. Definitions

For the purpose of this Policy, the following definitions apply:

- **Business Client:** Refers to the legal entity or business with which White Fox N.V. establishes or maintains a business relationship for the provision of its B2B gambling services.
- **CDD:** The process of identifying and verifying the identity of a business customer and its beneficial owner/s, and obtaining information on the purpose and intended nature of the business relationship.
- **EDD:** More thorough identification, verification and ongoing monitoring measures – applicable for clients flagged as ‘high risk’.
- **FIU:** The authority in Curaçao responsible for receiving and analyzing unusual transaction reports.
- **KYC:** Identifying and verifying the Business Client, including associated individuals like beneficial owners and representatives.
- **NORUT:** The Curaçao national ordinance governing the reporting of unusual transactions.
- **NOIS:** The Curaçao national ordinance governing customer identification when rendering services.
- **Occasional Transaction:** A transaction with a one-off customer where no ongoing relationship is expected.
- **PEP:** Individuals who are or have been entrusted with prominent public functions, including domestic PEPs, foreign PEPs, and persons in prominent functions by international organizations, as well as their family members and close associates.

- **Sanctions National Ordinance:** N.G. 2014 no. 55.
- **Kingdom Sanction Act:** N.G. 2016 no. 54
- **Source of Funds:** Refers to how the funds for a particular transaction were obtained by the business customer.
- **Source of Wealth:** Refers to the origin of all the money a legal entity or its beneficial owner has accumulated over time.
- **Threshold Transaction:** A financial transaction (deposit or withdrawal) equal to or above NAf. 4,000, including linked transactions.
- **UBO:** Ultimate Beneficial Owner – natural person/s ultimately owning or controlling a customer.
- **Unusual transaction:** A transaction meeting specific indicators per NORUT Article 10, including transactions of NAf. 5,000 or more, transactions by sanctioned persons, and presumed ML/TF transactions.

5. Policy Implementation

This Policy is implemented through documented procedures, with key responsibilities assigned, following a risk-based approach ('RBA') as required by the CGA. The Company will strictly comply with all applicable AML/CFT rules and regulations with specific emphasis on:

- creating and promoting a culture for the prevention of financial crime and ML/FT;
- ensuring that B2B customers are onboarded and monitored throughout the customer relationship via customer verification measures in line with KYC requirements; ensuring that customers adopt and employ acceptable measures and procedures for the prevention of financial crime, AML/CFT,

KYC procedures and fraud prevention measures in line with regulatory and license requirements; and

- adequately training and providing awareness to its staff regarding legal and regulatory obligations, including the reporting of suspicious, illegal and/or fraudulent activity using the appropriate channels.

5.1 Business Risk Assessment

White Fox N.V.'s policies, procedures and controls are consistent with the FATF's recommendation to adopt a RBA. Through the carrying out of a Business Risk Assessment ('BRA'), the Company is able to first identify its main sources of risk, as well as its nature and quantity, and then to focus adequately its resources on the highest areas of risk and ensure necessary controls are put in place. White Fox N.V. has an active interest in identifying risks for a number of reasons, including:

- to ensure compliance with its regulatory and license obligations;
- to prevent license suspension and/or removal, the imposition of fines and/or potential criminal prosecution; and
- to prevent reputational damage and/or adverse media attention.

The Company has reviewed and assessed the risks which it is exposed to in the course of the carrying out of its business activities as being mainly:

- **Distribution channel risks:**

White Fox N.V. does not always meet its customers face-to-face, with the majority of interaction taking place via industry-related events and video conferencing tools. The Company relies on the use of strong KYC procedures and ongoing monitoring mechanisms to verify the identity and integrity of its B2C customers, directors and UBOs. This requires prospective customers to complete B2B DD Forms (an onboarding questionnaire) together with supporting certified, translated (*if/where necessary*) documents, and open-source searches from

official sources, as well as ongoing PEP and sanction screening through third-party tools.

A detailed list of the documents requested by White Fox N.V. to all third parties, including its B2C clients, is attached to this Policy and marked as [Annex A; B2B Due Diligence Form & Documentation Request](#).

- **Customer risks:**

Additional risk factors considered include: the length of the business relationship, the customer's regulated history (i.e. whether the customer and/or its officers and/or UBO is or was subject to regulatory or enforcement action), customer's internal policies and procedures (e.g. AML policy), the payment methods used to transact with White Fox N.V. in return for service delivery, and intended targeted markets and the legality of online gaming in those jurisdictions.

- **Geographical risk:**

In line with the CGA's requirements, the Company is continuously carrying out jurisdiction risk assessments ('JRAs') to evaluate ML/FT risks using a wide variety of sources and publications, including but not limited to: United Nations Security Council ('UNSC'), the EU and OFAC consolidated sanctions lists, FATF and CFATF Public Statements, countries on the European Commission's ('EC') list of third countries having strategic deficiencies in their AML/CFT regime, Corruption Perception Index by Transparency International, countries identified as Jurisdictions of Concern or Primary Concern in the Narcotics Control Strategy Report ('INCSR'). This assessment allows the Company to adopt a RBA when assessing jurisdictional risks vis-a-vis its client base, in turn allowing it to risk rate jurisdictions.

- **Service provision risk:**

As a result of the provision of its services, White Fox's customers operate B2C online gaming websites which can be used by end users for ML/FT, fraud and other criminal offences and illegal acts. To mitigate this, White Fox N.V. ensures via

its rigorous onboarding process that it accepts as clients companies having in place appropriate AML/CFT Policies, reflecting their business models and operations. It verifies the authenticity of any licenses, approvals and certifications submitted to it by potential clients; and contractually obliges its clients to implement security measures to safeguard the Licensed Software from access or use by any unauthorised person, to prevent fraud, ML/TF and to maintain adequate AML/CFT policies and procedures, including having a Designated Compliance Officer responsible for the AML duties typically carried out by MLROs. The Company reserves the right to refuse any new client relationship and/or to review any existing client relationship at its sole and absolute discretion in line with its BRA.

- **Internal risk:**

The Company mitigates risk from human error , and third-party products and/or services through rigorous employee and third-party screening (including background checks, collection of professional references, qualifications and experience, and PEP and sanction screening). It ensures adequate staffing, employee onboarding procedures, training and orientation is carried out, monitors performance and promotes compliance awareness. The Company also evaluates the suitability, enforces technical standards and establishes service level agreements ('SLAs') to ensure reliability and support of third-party service providers. In addition, White Fox N.V. implements access control measures on the proliferation of information within the Company on a strict need-to-know basis, in line with the ISO/IEC 27001:2022 standard.

5.2. Customer Risk Assessment

The Company requires information about each organization and business partner following the laws of prevention of ML/FT prior to establishing legal agreements. The KYC checks performed may vary based on the third-party's nature of

business activities (*e.g. B2C companies vs third-party suppliers*). The Company may decide to extend due diligence questions based on the level of ML/FT risk perceived, according to the information received, publicly available information and other available sources, but overall, the following areas are covered in the Company's due diligence checks:

- Company Information
- Directors, Shareholders and UBOs' Information
- Additional Information (license, certification, etc.)

Please refer to [Annex A: B2B Due Diligence Form & Documentation Request](#) in order to obtain additional information about this specific topic.

5.3. Customer Acceptance Policy

Our approach to customer acceptance is grounded in a principles-based, risk-focused methodology under which every prospective and on-going client relationship is evaluated to determine the appropriate level of customer due diligence ('CDD'). We tailor our CDD measures; ranging from basic identity, incorporation checks and PEP screening for lower-risk entities to EDD such as in depth adverse-media reviews and senior-management oversight for higher-risk relationships - based on jurisdiction, ownership structure, type of services provided and delivery channels.

Any inability to satisfactorily verify identity or ownership, any confirmed match on sanctions/PEP lists, or any unexplained deviation from the customer's known activity profile is escalated immediately to our Compliance function. Where risks cannot be mitigated to an acceptable standard, we reserve the right to refuse or terminate the relationship in line with our internal processes.

5.4. Customer Due Diligence

CDD measures are undertaken prior to establishing a business relationship with a prospective customer and repeated when there is a suspicion of ML/FT, or when there are doubts about the veracity or adequacy of previously obtained customer identification data. Due diligence measures for business customers comprise of the following:

- **Identifying the business customer:** Collecting details such as the legal name, status, registration number, registered address, country of incorporation and jurisdiction of operation.
- **Verifying the identity of the business customer:** Confirming collected details using reliable, independent sources and relevant organizational documents such as; certificates of incorporation, articles of association, and licenses.
- **Identifying and verifying the ultimate beneficial owner/s:** Taking reasonable measures to understand the ownership and control structure of the business customer and verifying the identity of natural persons who ultimately own or control the entity – holding 25% or more of shares or voting rights– or exercise ultimate effective control. This involves obtaining reliable documents such as; share registers, UBO declarations, and conducting checks in commercial registries.
- **Identifying and verifying the identity and authorization of individuals representing the business customer:** Verifying that any individual acting on behalf of the legal entity is authorized and identifying and verifying that individual's identity.
- **Understanding the purpose and intended nature of the business relationship:** Obtaining information on the nature of the customer's

business, the reason for using White Fox N.V.'s services,. This helps in establishing a customer risk profile and detecting unusual activity.

- **Sanctions screening and PEP status screening:** Screening the business customer and its beneficial owners, directors, and any authorized persons (*where applicable*) against UN, EU, and local sanctions lists and conducting PEP screening. This is done at onboarding and regularly thereafter.

Enhanced Due Diligence ('EDD') is conducted for higher risk business customers and situations, including those from higher risk geographic areas, those utilizing products or transactions that might favor anonymity, and when there are new products or technologies. EDD measures for business customers may include obtaining additional information on the entity and associated individuals, the nature of the business relationship, senior management approval, amongst others. For business customers with PEP beneficial owners, directors, or authorized persons, EDD is mandatory and includes obtaining senior management approval and establishing source of wealth ('SoW') and funds ('SoF').

Simplified Due Diligence ('SDD') measures may be applied to business customers in lower risk situations, provided this is consistent with the country's risk assessment. SDD is not permitted when ML/FT is suspected or in specific higher-risk scenarios.

Depending on the risk assessment of the client, the extent of the above mentioned measures may vary.

5.5. Customer Ongoing Monitoring

The Company conducts ongoing due diligence on business relationships and scrutinizes transactions undertaken through the business customer accounts to ensure they are consistent with the business customer's profile and expected activity. This includes maintaining accurate and up-to-date identification data for

the business customer and its associated individuals. Ongoing monitoring is risk-based, with increased frequency and veracity of checks for higher-risk business customers.

Monitoring activities are employed to detect transactions involving high-risk jurisdictions and periodic rescreening of associated individuals against sanctions lists and PEP databases is conducted on an ongoing basis.

5.6. CDD reliance on third-parties

In the carrying out of business, the Company may rely on third parties for performing elements of the CDD measures provided the criteria outlined in the CGA regulations are met. The third party must be subject to CDD and record-keeping requirements, have an existing independent business relationship with the customer, and be regulated or supervised for AML/CFT compliance.

In outsourcing or agency scenarios, where a third party performs or applies CDD measures on behalf of the Company, this is considered an activity carried out by White Fox N.V. The Company is responsible for overseeing the effective implementation of CDD measures by the outsourced entity. Decision-making regarding customer onboarding or continuation of a business relationship based on risk cannot be outsourced. At the time of writing, the Company does not rely on any third-parties to carry out CDD measures on its behalf.

6. External reporting

6.1. Designated Compliance Officer

The Company maintains strict compliance with AML/CFT regulations by appointing a Designated Compliance Officer, who manages all internal disclosures and submits the required reports to the FIU.

Moreover, this Officer acts as the first point of contact for all ML/FT and general compliance issues from staff ,prepares regular reports for the consideration of the Board of Directors and conducts risk assessments of compliance systems. This Official is often consulted with regards to specific scenarios and also carries out periodic reviews and any necessary amendments to the Company's AML policy and other relevant policies and procedures. Together with the wider Legal and Compliance department, responsible stakeholders within the Company conduct the BRA and ensure the implementation of RBA and methodologies in line with regulatory guidance, submitting them for Board of Directors' approval.

6.2. Suspicious Transactions/Activity

Transactions or intended transactions deemed unusual include:

- Transactions which in connection with ML/FT are reported to the FIU of Curaçao.
- Transactions by or on behalf of a natural or legal person, a group or an entity listed under the Sanctions National Ordinance (N.G. 2014 no. 55).
- Transactions in the amount of NAf. 5,000 equivalent or more, regardless whether the transaction is made in cash, by check or other form of payment, or through electronic or other non- physical means. A transaction may consist of a single transaction or a series, combination, or pattern of transactions totaling NAf. 5,000 or more per day.
- Any transaction where there is cause to presume it is related to ML/FT, even if it does not meet the objective thresholds above.

6.3. Tipping Off

The Company, its directors, officers, and employees shall **not** disclose any details or information in connection with a report filed to the FIU or a request for

information made by the FIU to the business customer nor to third parties. This is to avoid "tipping off" and jeopardizing an analysis or investigation.

7. AML Compliance program

The AML program is risk-based and designed to mitigate ML/FT risks in its B2B operations, establishing the corresponding standards to comply with Curaçao laws and regulations. The program includes:

- **Internal policies, procedures, and controls:** Written policies, approved by senior management or the board, expressing commitment to combatting ML/FT/FP and outlining procedures for CDD, unusual transaction reporting, and record keeping specific to business customers. Procedures are maintained to ensure proper identification and verification of business customers and associated individuals, record retention, prompt reporting of suspicions, and cooperation with law enforcement.
- **Designated Compliance Officer:** A senior officer independent from games operations, is formally designated with day-to-day oversight of the AML program for B2B operations. The Compliance Officer has timely access to relevant information and is responsible for designing and implementing the program, verifying adherence to laws, reviewing compliance, reviewing and reporting unusual transactions, and staying informed on ML/FT developments relevant to the B2B sector.

8. Consequences of non-compliance

Violation of AML/CFT laws and regulations are subject to administrative and criminal sanctions. Failure to comply with the obligations to make disclosures to the Compliance Designated Officer or filing the relevant external reports to the FIU

can result in criminal prosecution. Disclosing information about a SAR or an investigation is also an offense. Breaches of this Policy will be taken seriously and will be subject to a disciplinary process, which may include written warnings and/or dismissal.

White Fox N.V. maintains a rigorous A/CFT compliance framework and expects the same level of commitment from its partners. Any instance of non-compliance with applicable AML/CFT laws, regulations, or the requirements outlined in this Policy will not be tolerated and will give rise to any applicable contractual and statutory penalties, subject to immediate and decisive corrective action.

9. Record keeping

White Fox N.V. maintains all necessary records on transactions by business customers for at least **five** years to comply with information requests from competent authorities. Records are sufficient to reconstruct individual transactions. All records obtained through CDD measures are kept for at least five years after the business relationship is ended, or after the date of the occasional transaction. These records are available to domestic competent authorities upon appropriate legal authority.

Records maintained include business customer registration details, identity verification for the entity and associated individuals, enhanced due diligence and relevant correspondence.

10. Policy reviews

To ensure this Policy remains effective, relevant and up-to-date, this Policy shall be reviewed upon any of the following triggers and/or timeframes:

- A. no later than 12 months from the date upon which the Policy was last reviewed;

- B. upon the discovery or recognition by an audit or risk assessment that the Policy requires amendment;
- C. upon the change or enactment of any relevant law or regulation which applies to the Policy;
- D. upon the finding by any regulator that an amendment to the Policy is required;
- E. upon the award of any new gambling licence in any new jurisdiction;
- F. upon the acceptance of customers from a jurisdiction / territory where the Company did not previously accept customers;
- G. upon a change of control or a change of corporate structure of White Fox N.V.

Any amendment of the Policy shall, as soon as is reasonably practicable, be distributed or informed to all persons within the scope of the Policy for information of the amendment. Any change in Policy giving rise to a Procedure review shall be identified and such changes shall be implemented to the relevant Procedure.

11. Contact Information

For any questions regarding this Policy, please contact the Legal and Compliance team via wf@viraemanagement.com.