

Elfy Interactive B.V. Anti-Money Laundering, Counter-Terrorist Financing and Sanctions Policy

Policy Summary

- Approving Officer: Chief Compliance Officer
- Responsible Office: Elfy Compliance Department
- Effective Date: June 28, 2025
- Next Review Date: June 28, 2026

1. Policy Statement

Elfy Interactive B.V. is committed to upholding the highest standards of integrity and regulatory compliance in its operations. This policy sets forth our framework to prevent, detect, and report activities related to money laundering (ML), terrorist financing (TF), and sanctions violations, in line with Curaçao law and international best practices. Elfy maintains a zero-tolerance approach to financial crime and is dedicated to fulfilling its obligations under the National Ordinance on the Identification of Clients (NOIS), the Reporting of Unusual Transactions (NORUT), the Sanctions National Ordinance, and the requirements of the Curaçao Gaming Control Board (CGA).

Elfy Interactive B.V. is committed to maintaining the highest standards of regulatory compliance and financial crime prevention. This policy integrates the company's operational complexity—including multiple brands, cross-border business, and use of fiat and cryptocurrency—into a unified AML/CFT compliance framework. As a Curaçao-licensed gaming operator, Elfy's AML policy is fully aligned with the National Ordinance on Offshore Games of Hazard (NOOGH), the Sanctions National Ordinance, and CGA requirements, and is tailored to our remote gaming footprint.

2. Purpose

The purpose of this policy is to provide clear guidelines for Elfy's internal AML/CFT processes. It ensures compliance with legal and regulatory requirements, protects the company's operations, reputation, and partners, and establishes a robust governance framework to manage and mitigate ML/TF risks.

This policy is intended to unify Elfy's approach across multiple brands and operational domains, ensuring compliance with both local and international standards. It addresses the dynamic risks associated with online gaming, cryptocurrency adoption, and cross-border services. The policy provides operational clarity for staff, legal protection for the business, and reassurance for regulators and financial partners.

The purpose of this Policy is to establish a framework for detecting and preventing money laundering (ML), terrorist financing (TF), and proliferation financing (PF), and to comply with applicable legislation, including the NOIS, NORUT, Sanctions National Ordinance, and the requirements of the CGA. (CGA AML Policy Jan 2025, p. 6)

3. Scope

This policy applies to all directors, officers, employees, contractors, and partners of Elfy Interactive B.V., across all jurisdictions in which the company operates. It governs business conducted using both fiat and cryptocurrency and includes all customer relationships, B2B counterparties, and delivery channels.

This policy applies to all directors, officers, employees, contractors, and business partners of Elfy Interactive B.V., across all licensed domains including: winover.com, otobet.com, betewin.com, rigobet.com, casinoda.com, betpin.com, beinbet.com, betle.com, jackpotz.com, jokeras.com, slotin.com, sortebet.com, azerbet.com, multiwin.com, casimo.com, winspin.com, and spartans.com. It covers operations conducted through both fiat and crypto payment rails and extends to affiliated partners operating under Elfy's gaming framework.

4. Definitions

- ML: Money Laundering
- TF: Terrorist Financing
- CDD: Customer Due Diligence
- EDD: Enhanced Due Diligence
- PEP: Politically Exposed Person
- MLRO: Money Laundering Reporting Officer
- UTR: Unusual Transaction Report
- FIU: Financial Intelligence Unit Curaçao
- BRA: Business Risk Assessment
- CRA: Customer Risk Assessment

5. Policy Implementation

5.1 Business Risk Assessment

Elfy performs an annual Business Risk Assessment (BRA) to evaluate ML/TF risks across its operations. This includes geographic exposure, transaction types, client profiles, and payment methods (including crypto). The BRA is reviewed and updated following material business changes.

Elfy's BRA includes qualitative and quantitative metrics, internal audit findings, and threat

typologies derived from law enforcement trends. Crypto-specific vectors such as mixing services, peer-to-peer wallets, and privacy coins are reviewed regularly.

In addition to standard BRA criteria, Elfy evaluates ML/TF risks stemming from DeFi exposure, anonymous wallet access, and unusual blockchain behaviors. A dedicated crypto risk matrix is maintained and reviewed biannually. The BRA is adjusted when onboarding new products, verticals, or high-risk clients.

5.2 Customer Risk Assessment

Each client undergoes a Customer Risk Assessment (CRA) during onboarding. This includes reviewing jurisdiction of incorporation, ownership structure, regulatory licenses, sanctions exposure, and AML history. Risk levels guide onboarding decisions and monitoring intensity.

Customers operating in or connected to decentralized finance (DeFi), gambling affiliates, or NFT-based platforms are flagged for enhanced analysis. Reputation risk scoring is supported by automated screening and manual reviews.

5.3 Customer Acceptance Policy

Elfy only accepts customers that meet strict onboarding standards. This includes verified identity, documented beneficial ownership, clear business justification, and favorable compliance history. Clients with links to high-risk jurisdictions or PEPs are escalated for review by the MLRO.

Elfy's policy includes a dynamic approval matrix for onboarding clients. For corporate applicants, legal opinions may be requested to validate their business legitimacy. Customers must pass initial automated screening and provide documentation on ownership, purpose of business, and financial standing.

5.4 Customer Due Diligence

CDD is required for all clients and includes identity verification, ownership tracing, and sanctions screening. For high-risk entities, Enhanced Due Diligence (EDD) is conducted, including source of funds analysis and management-level approvals.

CDD is tiered by risk level, ranging from simplified onboarding for low-risk corporates to detailed UBO validation, source of funds, and transactional purpose documentation for high-risk cases. Video KYC and blockchain wallet analytics tools are employed when appropriate.

In addition to standard CDD, Elfy uses blockchain forensics to assess wallet behavior. Clients must pass KYC screening, and their wallet addresses are checked for association with high-risk activities. EDD is applied to clients using mixers, high-velocity wallets, or obscure coins.

5.5 Ongoing Monitoring

Customer relationships are reviewed periodically and monitored continuously. Elfy uses both manual review and automated alerts to detect suspicious behavior, unusual transaction patterns, and risk profile changes. Monitoring intensity is proportional to risk level.

Monitoring triggers include spikes in deposit volume, IP anomalies, third-party media alerts, and regulatory blacklists. Machine learning tools support detection of pattern deviations while human review ensures case validation.

Ongoing monitoring systems are connected to both fiat PSPs and blockchain nodes. Threshold triggers are in place to detect unexpected behavior, and high-risk activity prompts real-time intervention. Data analytics tools are also used to detect connections between clients.

5.6 Reliance on Third Parties

Where permitted, Elfy may rely on regulated third parties to perform certain CDD elements. In such cases, Elfy ensures that the third party is subject to equivalent AML/CFT obligations, and retains full responsibility for compliance outcomes.

Reliance may only occur if the third party is regulated, supervised, and located in a jurisdiction that applies FATF standards. Elfy remains ultimately responsible for the CDD process and must obtain all identification data without delay. (CGA AML Policy Jan 2025, p. 16)

5.7 Reporting of Unusual Transactions

Suspicious or Unusual Transactions are reported to FIU Curaçao via the UTR portal (https://portal.fiucuracao.cw/goAMLWeb_PRD/Home). Employees must escalate concerns to the MLRO immediately. Tipping-off is strictly prohibited, and all reporting obligations are reinforced through regular training.

5.8 AML Compliance Program

Elfy has established an AML program that includes appointment of an MLRO, documented policies and procedures, regular training, internal audits, and board-level oversight. The program is reviewed annually and adjusted based on regulatory changes and audit feedback.

Elfy shall implement and maintain appropriate internal controls, policies, and procedures to prevent and detect ML/TF, and to ensure compliance with the NOIS, NORUT, and related CGA Guidelines. These controls shall be reviewed and approved by senior management and be made available to competent authorities upon request. (CGA AML Policy Jan 2025, p. 19)

Elfy will deliver ongoing AML/CFT training to relevant employees. Training shall be tailored

to the function, and updated in line with evolving risks, red flags, and typologies relevant to Elfy's services. (CGA AML Policy Jan 2025, p. 20)

6. Sanctions and Freezing of Assets

Elfy monitors sanctions lists from the UN, EU, OFAC, and local authorities. If a customer is identified as sanctioned, all assets are immediately frozen, access is blocked, and the case is reported to FIU Curaçao. Internal procedures support full legal compliance under the Sanctions National Ordinance.

Elfy shall have procedures to promptly identify and freeze property of individuals or entities designated under national and international sanctions. These procedures shall be documented and form part of the institution's compliance program. (CGA AML Policy Jan 2025, p. 20)

7. Technology and Product Risk

Before launching new products, services, or technologies, Elfy conducts a documented risk assessment to evaluate ML/TF risks. This includes AI tools, crypto wallets, smart contracts, and third-party platforms. Reviews are conducted by Compliance and signed off by the MLRO.

All crypto integrations undergo smart contract code risk reviews. New platforms are penetration-tested and onboarding tools must meet AML interface standards. AI systems are stress-tested for bias and false positives in monitoring behavior.

8. Governance and Oversight

The MLRO is responsible for overseeing the AML program and reporting directly to executive management. The Risk and Compliance Committee meets quarterly to review risk metrics, audit results, and escalate issues to the Board. An independent audit is conducted every 24 months to assess AML/CFT effectiveness.

An independent audit function must be in place to test the AML/CFT system, policies, procedures, and internal controls. The frequency and scope shall be determined by the institution's ML/TF risk profile and must be sufficient to ensure effectiveness. (CGA AML Policy Jan 2025, p. 19)

9. Recordkeeping

All CDD records, risk assessments, and reports are retained for a minimum of 5 years. This includes transaction logs, onboarding files, and audit trails. Electronic systems are used to securely store and retrieve documentation when needed for audits or regulatory inquiries.

Elfy shall maintain records on transactions and CDD for at least five years after the business relationship has ended or the date of the occasional transaction. Records must be readily available to the FIU and other competent authorities. (CGA AML Policy Jan 2025, p. 21)

10. Policy Review and Updates

This policy is reviewed annually and whenever there is a change in law, regulation, business operations, or AML/CFT risk exposure. All revisions are approved by the MLRO and the Compliance Department, and communicated to relevant stakeholders.

11. Policy History

- Original approval: September 13, 2024
- Current version: 1.2 (June 28, 2025)
- Last review date: June 28, 2025

12. Contact and URL

Compliance Department – Elfy Interactive B.V.

Email: compliance@elfyinteractive.com