

ZOZO TECHNOLOGY B.V.

ANTI-MONEY LAUNDERING POLICY

Approval	Board of Directors
Responsible Office	Compliance Officer
Review	Annually
Audience	All Employees, Contractors, and Third Parties
Effective Date	April 10, 2025
Version	2.1 — 24 March 2026 (supersedes v1.0)
Next Review Date	May 30, 2026

Policy History

Date	Ver.	Summary of Changes	Management Approval
6 October 2025	1.0	Initial policy implementation	Gouloud Hammoud, obo Guardian Corporation Curaçao B.V.
10 February 2026	2.0	Minor formatting updates to policy document. No changes to policy content, procedures, or compliance requirements.	Compliance Officer, Zozo Technology B.V.
24 March 2026	2.1	Following CGA Notice ADMIN-20565, the following changes were made from v1.0: 1. §5.1 — Four-stage onboarding model introduced: Stage 1 (account creation — email, username, password only); Stage 2 (email OTP verification + full KYC form + ID upload combined, triggered before first deposit); Stage 3 (jurisdiction check); Stage 4 (deposit activation). 2. §5.1 — Mandatory KYC fields at registration updated to NOIS/CGA minimum requirements only: full name, date of birth, place of birth, residential address, nationality, ID number, and government-issued ID document upload. Occupation fields collected during CDD/EDD process where applicable. 3. §4.2 — Restricted Jurisdictions framework added with definitive Restricted Jurisdictions List (Appendix I) enforced via onboarding drop-down and IP geo-blocking. 4. Appendix I — New: Restricted Jurisdictions List (27 entries, 7 regional groups).	Compliance Officer, Zozo Technology B.V.

TABLE OF CONTENTS

- 1. Introduction
 - 1.1 Policy Statement
 - 1.2 Purpose of this AML Policy
 - 1.3 Definitions
- 2. Policy Implementation
- 3. The Risk-Based Approach
- 4. Customer Acceptance Policy
 - 4.1 Customer Risk Assessment
 - 4.2 Prohibited Accounts & Restricted Jurisdictions ← UPDATED v2.0
 - 4.3 Politically Exposed Persons (PEPs)
 - 4.4 Sanctions Screening
- 5. Customer Due Diligence (CDD) Measures
 - 5.1 Customer Onboarding and Identification ← UPDATED v2.0
 - 5.2 Verification of Beneficial Ownership
 - 5.3 Customer Risk Assessment and Purpose of Relationship
 - 5.4 Simplified Due Diligence (SDD)
 - 5.5 Customer Due Diligence (CDD)
 - 5.6 Timeline for Compliance and Non-Compliant Documents
 - 5.7 Enhanced Due Diligence (EDD)
 - 5.8 Ongoing Monitoring
 - 5.9 Reliance on Third Parties
- 6. Reporting of Unusual Transactions
- 7. Anti-Money Laundering Compliance Program
- 8. Compliance and Consequences of Non-Compliance
- Appendix I — Restricted Jurisdictions List ← NEW v2.0

1. INTRODUCTION

1.1. POLICY STATEMENT

Zozo Technology B.V. (the "Company") is licensed and regulated by the Curaçao Gaming Authority (CGA) to offer remote (online) games on the internet, under License No. OGL/2024/1519/0809. The Company has developed this comprehensive Anti-Money Laundering, Counter Terrorism Financing and Counter Proliferation Financing ("AML, CTF and CPF") policy in accordance with its license conditions.

As a responsible gaming enterprise, the Company acknowledges the paramount importance of upholding the integrity of its financial systems and preventing the exploitation of its operations for unlawful activities.

1.2. PURPOSE OF THIS AML POLICY

This Policy ensures the Company's compliance with applicable AML, CTF and CPF legal and regulatory requirements supervised by the CGA and the Curaçao Financial Intelligence Unit (FIU). Applicable legislation includes:

- Code of Criminal Law (Penal Code) (N.G. 2011, no. 48)
- National Ordinance on Identification of Customers when Rendering Services (NOIS) (N.G. 2017, no. 92), last update June 2024
- National Ordinance on the Reporting of Unusual Transactions (NORUT) (N.G. 2017, no. 99), last update June 2024
- National Decree on penalties and fines for reporting unusual transactions (N.G. 2021, no. 69) as amended by PB 2023, no. 6
- Ministerial Decree — Regulation Indicators Unusual Transactions (N.G. 2015, no. 73)
- Sanctions National Ordinance (N.G. 2014, no. 55); Kingdom Sanction Act (N.G. 2016, no. 54)
- National Ordinance on Games of Chance (PB 2024, no. 157)
- CGA Regulations for combating Money Laundering, Terrorism Financing and Proliferation Financing, last update January 2025

1.3. DEFINITIONS

All defined terms from Policy v1.0 are retained and incorporated herein by reference. New terms introduced in v2.0 are defined in context within the relevant section.

2. POLICY IMPLEMENTATION

Sections 2.1 (Responsibility of Senior Management), 2.2 (AML&TF Compliance Officer), and 2.3 (Employees) are unchanged from v1.0 and incorporated by reference.

3. THE RISK-BASED APPROACH

Sections 3.1 and 3.2 are unchanged from v1.0 and incorporated by reference.

4. CUSTOMER ACCEPTANCE POLICY

4.1. CUSTOMER RISK ASSESSMENT

Section 4.1 is unchanged from v1.0.

4.2. PROHIBITED ACCOUNTS & RESTRICTED JURISDICTIONS [UPDATED — v2.0]

4.2.1 Prohibited Accounts

The following categories of individuals are prohibited from being accepted as customers:

- Individuals under the age of 18
- Individuals listed on sanctions imposed by the UN, EU, or OFAC
- Individuals for whom there are reasonable grounds to suspect involvement in ML/TF/PF or any other form of criminal activity
- Self-excluded customers barred from our websites or included in any national self-exclusion register as stipulated by licensing conditions
- Individuals who have submitted documents or information reasonably suspected to be fraudulent or falsified

4.2.2 Restricted Jurisdictions [NEW — v2.0]

The Company maintains a Restricted Jurisdictions List (set out in full in Appendix I) comprising all countries and territories from which the Company does not hold the necessary regulatory authorisation, or where online gaming is otherwise prohibited under applicable local law.

The Restricted Jurisdictions List is enforced through two complementary technical controls:

- Primary control — Onboarding drop-down gate: At Stage 2 of the onboarding process (see §5.1), customers must select their country of residence. Countries appearing on the Restricted Jurisdictions List are excluded from the selectable options or, where technically necessary, trigger a 'service not available' notification that prevents the customer from proceeding.
- Secondary control — IP-based geo-blocking: The Company operates IP-level geo-blocking as a secondary layer to prevent access from restricted jurisdictions, including for customers who may attempt to circumvent the onboarding drop-down control.

The Restricted Jurisdictions List shall be:

- Reviewed and formally approved by the Compliance Officer at least annually, or following any material change in the Company's licensing position, applicable CGA guidance, or relevant FATF designations
- Cross-referenced against the FATF list of high-risk and other monitored jurisdictions, the U.S. Department of State's International Narcotics Control Strategy Report (INCSR), and the Company's CGA licence conditions
- Maintained as Appendix I to this Policy, updated at each annual review, and made available to CGA examiners upon request in accordance with §7.4

4.3. POLITICALLY EXPOSED PERSONS (PEPs)

Section 4.3 is unchanged from v1.0.

4.4. SANCTIONS SCREENING

Section 4.4 is unchanged from v1.0.

5. CUSTOMER DUE DILIGENCE (CDD) MEASURES

5.1. CUSTOMER ONBOARDING AND IDENTIFICATION [UPDATED — v2.0]

The Company operates a staged onboarding model designed to ensure full AML/KYC compliance under NOIS and CGA licensing conditions, while providing a clear and structured customer journey. No financial activity — including deposits, withdrawals, or wagering with real funds — is permitted until all applicable onboarding stages have been successfully completed.

5.1.1 The Four-Stage Onboarding Gate

Stage	Gate	Requirements
1	Account creation	Email address, username, and password only. Account is created but all financial activity is disabled. No KYC data is collected at this stage. This mirrors industry standard practice.
2	Email OTP verification & KYC data collection	When the customer initiates their first deposit, they are prompted to verify their email address via a one-time passcode (OTP) and complete the full KYC form in the same step. The following must be provided before deposit functionality is enabled: • Full legal name (first and last) • Country of residence • Place of birth • Date of birth • Permanent residential address (street, city, postal code) • Nationality • Identification number • Upload of a valid government-issued ID document (passport, national ID card, or driver's license — must include photograph and be legible) Deposit functionality remains locked until all of the above are successfully submitted.
3	Jurisdiction check	The system validates the customer's country of residence against the Restricted Jurisdictions List (Appendix I). Customers from restricted jurisdictions receive a 'service not available' notification and cannot proceed.
4	Deposit & financial activity enabled	Only after successful completion of Stages 1–3 is the customer's wallet and deposit functionality activated. No financial transactions are permitted prior to completion of all preceding stages.

5.1.2 Mandatory KYC Data Fields (Stage 2)

The following fields are the minimum mandatory requirements under NOIS and CGA licensing conditions and must be submitted — together with email OTP verification — before deposit functionality is enabled:

- Full legal name (first name and last name)
- Country of residence — validated against the Restricted Jurisdictions List (Appendix I)
- Place of birth
- Date of birth
- Permanent residential address (street address, city, and postal code)
- Nationality
- Identification number

- Upload of a valid government-issued identification document (passport, national ID card, or driver's license) — must include a photograph and be legible

Where an identity document is not in a language understood by the Company, a certified translation may be required. Proof of permanent residential address dated within the last 6 months (e.g., utility bill or bank statement) must also be provided. The Company prohibits anonymous and fictitious accounts and applies robust technical controls to prevent their creation.

5.1.3 Non-Compliant Documents

Where a document submitted at Stage 3 does not meet verification standards, the designated compliance staff member must immediately flag it, inform the customer of the specific reason for non-compliance, and provide a reasonable opportunity to resubmit. All actions, communications, escalations, and outcomes must be recorded in the customer's file to ensure a complete audit trail.

5.2. VERIFICATION OF BENEFICIAL OWNERSHIP

Section 5.2 is unchanged from v1.0.

5.3. CUSTOMER RISK ASSESSMENT AND PURPOSE OF RELATIONSHIP

Section 5.3 is unchanged from v1.0. Occupation information is collected as part of the CDD/EDD process when required by the customer's risk profile or upon reaching the Cg. 4,000 threshold, in line with the risk-based approach.

5.4. SIMPLIFIED DUE DILIGENCE (SDD)

Section 5.4 is unchanged from v1.0.

5.5. CUSTOMER DUE DILIGENCE (CDD)

Section 5.5 is unchanged from v1.0.

5.6. TIMELINE FOR COMPLIANCE AND NON-COMPLIANT DOCUMENTS

Section 5.6 is unchanged from v1.0.

5.7. ENHANCED DUE DILIGENCE (EDD)

Section 5.7 is unchanged from v1.0.

5.8. ONGOING MONITORING

Section 5.8 is unchanged from v1.0.

5.9. RELIANCE ON THIRD PARTIES TO PERFORM DUE DILIGENCE

Section 5.9 is unchanged from v1.0.

6. REPORTING OF UNUSUAL TRANSACTIONS

Sections 6.1–6.4 are unchanged from v1.0 and incorporated by reference.

7. ANTI-MONEY LAUNDERING COMPLIANCE PROGRAM

Sections 7.1–7.4 are unchanged from v1.0 and incorporated by reference.

8. COMPLIANCE AND CONSEQUENCES OF NON-COMPLIANCE

Section 8 is unchanged from v1.0 and incorporated by reference.

APPENDIX I — RESTRICTED JURISDICTIONS LIST

Effective: 24 March 2026 | Approved by: Emmanuel [Legal], Compliance Officer | Next review: May 2027

The following jurisdictions are restricted. Customers residing in or connecting from these countries or territories are not permitted to register or access financial services on the Company's platform. This list is enforced at onboarding via the country-of-residence drop-down and via IP-based geo-blocking.

Restricted Jurisdiction	Region/Group	Basis for Restriction
NL ANTILLES		
Aruba	NL Antilles	No authorisation / Kingdom territory restriction
Bonaire	NL Antilles	No authorisation / Kingdom territory restriction
Curaçao	NL Antilles	Domestic jurisdiction — operator jurisdiction, not a serviceable market
Saba	NL Antilles	No authorisation / Kingdom territory restriction
Sint Eustatius (Statia)	NL Antilles	No authorisation / Kingdom territory restriction
Sint Maarten	NL Antilles	No authorisation / Kingdom territory restriction
EUROPEAN UNION		
Austria	European Union	No CGA authorisation / regulated market
France	European Union	No CGA authorisation / regulated market
Germany	European Union	No CGA authorisation / regulated market
Greece	European Union	No CGA authorisation / regulated market
Malta	European Union	No CGA authorisation / regulated market
Netherlands	European Union	No CGA authorisation / regulated market
Spain	European Union	No CGA authorisation / regulated market
EUROPE		
United Kingdom	Europe	No CGA authorisation / regulated market
ASIA/PACIFIC		
Australia	Asia/Pacific	No CGA authorisation / local prohibition
NORTH AMERICA		

United States of America	North America	No CGA authorisation / local prohibition
United States Minor Outlying Islands	North America	U.S. territory — same restriction as USA
FRANCE/OVERSEAS		
French Guiana	France/Overseas	French overseas territory — same restriction as France
French Polynesia	France/Overseas	French overseas territory — same restriction as France
French Southern Territories	France/Overseas	French overseas territory — same restriction as France
BRITISH CROWN DEPENDENCY		
Isle of Man	British Crown Dependency	No CGA authorisation / own regulatory regime
FRANCE/OVERSEAS		
Saint Barthélemy	France/Overseas	French overseas collectivity — same restriction as France
Saint Martin (French part)	France/Overseas	French overseas collectivity — same restriction as France
NL ANTILLES		
Sint Maarten (Dutch part)	NL Antilles	Kingdom territory restriction — duplicate entry for drop-down
EUROPE		
United Kingdom (excl. Northern Ireland)	Europe	Sub-designation of UK restriction
United Kingdom of Great Britain and Northern Ireland	Europe	Full designation of UK restriction
BRITISH OVERSEAS TERRITORY		
Virgin Islands (British)	British Overseas Territory	No CGA authorisation
NORTH AMERICA		
Virgin Islands (U.S.)	North America	U.S. territory — same restriction as USA

This list comprises 28 restricted jurisdictions across NL Antilles, European Union/Europe, Asia/Pacific, North America, and French/British overseas territories. It will be reviewed annually by the Compliance Officer and updated to reflect any changes in the Company's licensing position or applicable regulatory guidance.