

ANTI-MONEY LAUNDERING & COMPLIANCE PROGRAM

COMPANY OVERVIEW

NewAge N.V. (“Dixy”; “Company”; “Us”; “We”; “Our”) is a company registered and established under the laws of Curaçao, with registration number 161385 and registered address at Abraham Mendez Chumaceiro Blvd. 03 , Willemstad, Curaçao. NewAge N.V. is licensed and regulated by the Curacao Gaming Authority (CGA) with License Number: OGL/2024/1409/0649. The Company provides licensed online games of chance in compliance with the applicable regulatory framework.

In line with relevant domestic and international compliance standards, Dixy has implemented a robust compliance framework commensurate with its products and services with the aim of detecting and deterring illicit activities on the Dixy platform. We undertake a Risk Based Approach (“RBA”) in Our assessment of players using Our Dixy platform at every stage of the customer lifecycle.

Regulatory Compliance Framework

While Dixy is not classified as a financial institution under Curaçao law, it adheres to the core principles outlined in the 2016 Regulations on the Prevention of Money Laundering and Terrorist Financing. Dixy has adopted a comprehensive AML/CFT program that aligns with guidance issued by the CGA and international standards set by the Financial Action Task Force (FATF).

Dixy's internal compliance team is responsible for monitoring legal and regulatory developments and ensuring alignment with best practices.

Measures include:

Maintenance of updated internal AML/CFT policies, procedures, and operational controls; Appointment of a dedicated AML/KYC compliance function responsible for implementation and enforcement; Regular AML/CFT training programs for staff with access to client data or transactional workflows; Independent audits, system monitoring, and remediation protocols to ensure continuous compliance.

GLOSSARY OF TERMS & DEFINITIONS

Money Laundering

The process of making illegally-gained proceeds appear legal. This process is generally broken down into three steps: placement, layering and integration.

Placement

The process of placing unlawful proceeds into traditional financial institutions, through deposits or other avenues.

Layering

The process of separating proceeds of criminal activity from their origin through the use of layers of complex financial transactions, such as converting cash into traveller's checks, money orders, wire transfers, letters of credit, stocks, bonds or purchasing assets.

Integration

Using apparently legitimate transactions to disguise the illicit proceeds, allowing the laundered funds to be distributed back to the criminal; integrating the now clean money back into normal use.

Suspicious Activity

Activity conducted by a user or non-user using the institution where there are indications that the persons engaging in the transaction may be doing so for fraudulent or illegal purposes.

Sanctions

Sanctions are activities conducted by the international community to prohibit or constrain activities of the target of the sanctions.

Dixy has appointed a Chief Compliance Officer responsible for coordinating the implementation of Our AML Policy. The Chief Compliance Officer's duties also include developing AML initiatives, working with management to revise the AML/KYC policy, assessing new regulatory requirements and investigate potentially suspicious or unusual activity and reporting them where necessary.

CLIENT DUE DILIGENCE (“CDD”)

Dixy will apply appropriate user due diligence and ongoing monitoring measures by using a combination of software products which are enforced through internal operational features to ensure compliance with applicable laws.

KNOW YOUR CUSTOMER (“KYC”)

Dixy adopted a RBA CDD approach to enable Us to better understand the nature and purpose of player’s relationship to Dixy in order to develop a customer risk profile. In doing so, Dixy collects certain documentary and non-documentary information upon registration and account-opening. Dixy maintains different CDD for different accounts and services.

For instance, the CDD require users to go through Our customer identification program (“CIP”). Our CIP consists of procedures for:

Collecting baseline (e.g., wallet address, email address) information at account creation through Dixy’s user onboarding portal; Monitoring the risk profile associated with the underlying cryptocurrency wallet used to fund the user’s account; Maintaining records of the information used to identify the user; and Determining if a user appears on any list of known or suspected terrorists or terrorist organizations provided to the financial institutions based on the above information.

The above steps are operationalized using the following measures:

Identity and Age Verification

A third-party service provider will support’s Dixy’s ability to determine the legitimacy of the identification information other KYC materials or information provided and will confirm that the user is permissible.

The service provider also will confirm that the user does not appear to be located in a comprehensively-sanctioned or otherwise prohibited jurisdiction and will search global sanctions lists to confirm that the user does not appear thereon using onboarding information such as wallet addresses.

Customer Information

Dixy will collect details on each user to form a reasonable belief that Dixy knows the identity of its users commensurate with the user’s risk profile. For instance, Dixy may collect such details as the wallet address, name, address, country, date of birth, or postal code (collectively, “KYC Information”).

Dixy will collect any of the above KYC Information prior to issuing a Dixy funding addresses to users, such as address for depositing funds or QR codes. Dixy does

not allow corporate entities or non-natural persons to register. Dixy may, at its Own description, rely on the performance by another institution of some or all of the elements of our CIP.

Geo-blocking for Prohibited Jurisdictions

Dixy will require contractual client certifications that, through IP address-based geo-blocking, no gaming services will be offered in countries where such activity is not permitted.

Geo-blocking for Sanctioned Jurisdictions

Dixy also will require contractual client certifications that such users are not subject to United States, European Union, or other global sanctions or watch lists, including individuals or entities associated with the United States' comprehensively sanctioned jurisdictions, Iran, Cuba, North Korea, Syria and the Crimean region of Ukraine.

Dixy will rely on various RBAs to verify these representations including as in the below-described KYC measures and through IP address-based geo-blocking.

Contractual Prohibitions on Users Onboarding from Prohibited Jurisdictions

Users are notified at onboarding that Dixy does not offer services in restricted jurisdictions. Dixy's policy on restricting user activity stems from a combination of its risk, fraud prevention, and AML standards, as well as any assessments associated with the permissibility of its services in certain jurisdictions.

Approval and Adoption

This Anti-Money Laundering and Counter-Terrorism Financing (AML/CTF) Policy has been reviewed and approved by the Board of Directors and is hereby adopted as the official AML/CTF Policy of the Company. This Policy shall take effect on the date of execution below and shall remain in force until amended or replaced.

For and on behalf of the Company:



Zhou Linjian
Director

Date: 6/23/2026