

Digital Asset Risk Management Policy

Last updated: 31.05.2024

I. Introduction

Bets Entertainment N.V. (referred to as either "Company", "the Company", "We", "Us", or "Our" in this Policy) having its registered office at Abraham de Veerstraat 9, Curaçao, Company Registration number 155648, has developed a comprehensive risk-based Digital Asset Risk Management Policy ("the Policy") in an effort to maintain the highest possible compliance with applicable laws and regulations relating to anti-money laundering, countering financing of terrorism and combating proliferation financing.

The present Policy shall be regularly reviewed and, if necessary, revised to comply with applicable rules, regulations, policies, and best practices. The present Policy must be adhered to by the Company and Company's staff to mitigate reputational, regulatory, legal and financial loss risks.

The gaming and cryptocurrency markets operate under a stringent framework of rules and regulations created to maintain security and integrity. Most crypto-related services are mandated to implement AML/CFT/CPF procedures to comply with these regulations. At Bets Entertainment N.V., we are committed to safeguarding our clients from any form of scams and fraudulent activities that may arise within the crypto sphere. To achieve this, we adhere strictly to all applicable rules and regulations.

One of the key measures we employ is the AML/CFT/CPF procedure and this Policy. This Policy serves multiple vital functions. Firstly, it ensures that all transactions are entirely legal and transparent in the eyes of regulatory institutions. By monitoring transaction activities, we can effectively prevent illicit activities such as money laundering and fraud.

Moreover, the Policy provides assurance to regulatory authorities that our clients are law-abiding citizens engaged in legitimate transactions. By confirming the legality of each transaction, we create a secure and trustworthy environment for all users.

This policy should be considered in conjunction with the Company's AML/CFT/CPF policy. Together, this policy and the AML/CFT/CPF policy

form a comprehensive framework designed to ensure compliance with applicable laws and regulations. These policies collectively address and mitigate potential risks related to money laundering, terrorism financing, and the proliferation of weapons, thereby reinforcing the Company's commitment to upholding the highest standards of financial integrity and regulatory compliance.

In summary, through the rigorous implementation of the Policy, We demonstrate its commitment to regulatory compliance and client protection. This process helps us ensure that the transactions carry out by our clients are fully legal and transparent.

2. Digital Assets

Digital Assets represent a developing and diverse asset class defined by the use of distributed ledger technology (DLT) or similar technologies. Specifically, Digital Assets are intangible assets that exist solely as entries on a public, permissioned, or private blockchain or other digital, distributed ledgers.

These distributed ledgers and any data stored within them, including the Digital Assets themselves or any references to them, are not managed or controlled by Bets Entertainment N.V. Particularly, Digital Assets may consist of native value units that do not involve or represent any claim against an issuer or another third party. When these units are intended or used for payment purposes and do not qualify as securities or other financial instruments, they are sometimes referred to as payment tokens or pure cryptocurrencies ("Crypto Currencies").

Bets Entertainment N.V. processes any potential Digital Assets transactions through third-party service providers that hold the necessary applicable licenses and are fully compliant with applicable regulatory standards. These third-party service providers are selected based on their adherence to stringent compliance protocols, ensuring that all Digital Assets-related activities are conducted in accordance with legal and regulatory requirements. This provision forms an integral part of the contractual arrangement between the parties involved.

Bets Entertainment N.V. is explicitly excluded from any involvement in the issuance, distribution, trading, or other transactions of similar nature related to Digital Assets. Such activities are not conducted through, nor facilitated by, any domains or platforms licensed under the Company's name. All Digital Asset operations, including but not limited to issuance,

trading, and distribution, are managed exclusively by licensed third parties and are not associated with the Company.

3. Legal and Regulatory Framework

The Legal and Regulatory Framework is set by, without being limited:

EU Legislation:

- Directive (EU) 2015/849 on the prevention of the use of the financial system for the purpose of money laundering or terrorist financing (4th Money Laundering Directive).
- Directive (EU) 2018/843 on the prevention of the use of the financial system for the purpose of money laundering or terrorist financing (5th Money Laundering Directive).
- Commission Delegated Regulation (EU) 2018/1108 on Central Contact Points.
- Commission Delegated Regulation (EU) 2019/758 on Measures for Groups present in Certain Third Countries.
- Commission Delegated Regulation (EU) 2016/1675 on High Risk Third Countries.
- Regulation (EU) 2015/847 - Information accompanying transfers of funds. Regulation (EU) 2023/1113 - Regulation on information accompanying transfers of funds (recast).
- Regulation (EU) 2023/1114- Regulation on markets in crypto-assets.
- EU List of Prominent Public Functions (EUR-Lex - 52023XC00724). Prominent public functions at national level, at the level of International Organizations and at the level of the European Union Institutions and Bodies.
- DIRECTIVE (EU) 2017/541 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL On Combating Terrorism.
- Payment card Industry (PCI) Data Security Standard V1.2 (October 2008).

FATF International Standards:

- FATF Methodology for assessing compliance with the FATF Recommendations and the effectiveness of AML/CFT systems.
- FATF „Combating Proliferation Financing: A Status Report on Policy Development and Consultation“.
- FATF „Guidance on Counter Proliferation Financing“.
- FATF „Guidance on Proliferation Financing Risk Assessment and Mitigation“.
- EU Strategy Against the Proliferation of Weapons of Mass Destruction 15708/03.

Curacao Legislation:

- Sanctions National Ordinance (Sanctielandsverordening, PB 2014, no. 55).
- NOIS: the National Ordinance Identification for Services (Landsverordening identificatie bij dienstverlening, PB 2017, no. 92, GT).
- NOOGH: the National Ordinance on Offshore Games of Hazard (Landsverordening buitengaats hazardspelen, PB 1993, no. 63).
- NORUT: the National Ordinance on the Reporting of Unusual Transactions (Landsverordening melding ongebruikelijke transacties (LMOT), PB 2017, no. 99).
- Appointment of the GCB as the AML/CFT supervisor for the LMOT for the gaming industry (no. 19/0283, Landsbesluit toezichthouder ongebruikelijke transacties kansspelsector).
- National Decree supervisor identification when rendering services gaming sector (Landsbesluit toezichthouder identificatie bij dienstverlening kansspelsector, LB van 28 januari 2019, no. 19/0282).
- Rules for reporting unusual transactions. (PB 2020, 157, Landsbesluit inzake regels voor melding ongebruikelijke transacties (Landsbesluit goAML meldportaal).
- Indicators for recognizing unusual transaction. (PB 2015, 73, Regeling indicatoren ongebruikelijke transacties).
- Gaming Control Board. Regulations for Anti-Money Laundering and Combating the Financing of Terrorism (AML/CFT), August 2016.
- Caribbean Financial Action Task Force (CFATF) International Standards (Round Reports, Public Statements and Notifications).

4. Risk-Based Approach And Risk Assessment

We conduct a risk-based approach and gather relevant information and documentation for each prospective Digital Asset transaction. The Company's employees will exercise appropriate care, due diligence, and sound judgment in evaluating the overall character and nature of it. We operate in accordance with the highest ethical standards and will not engage in business relationships with individuals or entities that could adversely affect the Company's reputation or compromise the integrity of the iGaming, Digital Asset and crypto-related industry.

To effectively identify, assess, and analyze risks related to Digital Asset transactions, the Company prepares a comprehensive Digital Asset Risk Assessment.

Following the mentioned Risk Assessment and classification for a particular transaction, the risk evaluation will be periodically reviewed and updated based on the evolving knowledge of the client and their activities.

5. Managing the risks related to Digital Assets

We acknowledge the potential risks related to Digital Assets and the special characteristics of the cryptocurrency market. These risks include, but are not limited to, security weaknesses within the underlying code or technology, transaction delays, and the irreversibility of transactions. Consequently, We are committed to implementing all possible measures to mitigate these risks and ensure compliance with applicable regulatory requirements.

Risks of Digital Assets relating to the relevant markets, may include:

- Risk of fraudulent transactions. We acknowledge that certain Digital Asset transactions may be linked to fraudulent activity or associated with criminal conduct. In order to mitigate this risk, the Company applies additional software tools, such as amlbot.com, to evaluate and monitor transactions for signs of fraud or suspicious behavior. When a transaction is flagged by these tools, the Company will review it carefully and, if there are reasonable grounds for suspicion, the transaction will be canceled and will not proceed. This proactive approach ensures that transactions are thoroughly vetted to prevent any potential fraud and safeguard the integrity of the Company's operations.

- Digital Assets existing solely on a distributed ledger.

We acknowledge that distributed ledgers on which Digital Assets exist are beyond its control and are susceptible to various events, such as hard or soft forks in a blockchain, which may affect the functionality, convertibility, or transferability of Digital Assets, or result in a loss or reduction in value. To mitigate these risks, the Financial Team of the Company regularly monitors the status and developments of relevant distributed ledgers to identify potential risks early. In addition, special accounting software is used to assess losses resulting from fluctuations in crypto exchange rates and to take any exchange difference rates into account when management reports are prepared.

- Risk of irreversibility of transactions/faulty Instructions. Transactions on a blockchain or other distributed ledger cannot be undone or changed once completed. In other words, sending Digital Assets to a wrong address makes it impossible to retrieve them. To reduce this risk for the players, We

require for third-party providers multiple confirmations from clients before processing transactions and provide clear instructions to ensure the correct address is used. Our customer support team is also available to help clients check their transaction details before sending, which helps prevent mistakes. To reduce this risk for the Company two separate employees within the Treasury department are appointed by CFO to make payments in crypto and fiat currencies.

- Risk of security weaknesses within the underlying code or technology. There is a risk that developers or other third parties might accidentally or intentionally introduce flaws or errors into the underlying code or technology of a Digital Asset. These flaws can be exploited in various types of attacks, which could harm the functionality, convertibility, or transferability of the Digital Assets, or cause a full or partial loss of value. We maintain continuous monitoring to detect and respond to any suspicious activities or potential threats in real-time.

- Risk of evolving markets in Digital Assets. The markets for Digital Assets are constantly changing, leading to higher volatility, limited transparency, reliability issues, and potential execution delays or failures. These factors may result in significant losses or other negative effects for the Client. To reduce these risks, We employ a comprehensive risk management strategy, which includes working with multiple reliable and compliant third-party service providers to ensure timely and efficient execution of potential transactions, providing clients with current information and guidance on market conditions and potential risks, along with dedicated customer support to assist in making informed decisions, and regularly monitoring market conditions and developments to anticipate and respond to potential volatility and market disruptions.

- Risk of delays in execution or settlement of Digital Asset transactions and Mitigation Measures. Execution and settlement of transactions in Digital Assets may depend on specific characteristics of the relevant distributed ledger or the participation of third parties in the network, such as the availability of miners or other processing entities. These dependencies can lead to delays or failures in executing or settling transactions, which may result in significant losses or other adverse effects for the Client. We include provisions in contracts with third parties and partners to address actions in case of delays or disruptions, as well as to provide for compensations or alternative means of fulfilling obligations.

6. Know Your Business (KYB)

In connection with the AML/CFT/CPF policy and in addition to KYC procedures, the Company uses KYB procedures to verify the identity of vendors, suppliers, and contractors ("Business Partners") in the Digital Assets sector. This includes checking the background of the Business Partner, its directors, beneficial owners, and any related individuals or entities. The purposes of KYB are to conduct due diligence during the business relationship and review transactions to ensure they align with the Company's understanding of the Business Partner's business, risk profile, and, if necessary, the source of funds. The Company may apply KYB procedures before entering into contracts with any third parties in the Digital Assets sector to ensure compliance and manage risks. The Company also reserves the right to request additional documentation and information to fully verify the background of suppliers, providers, and contractors.

Our Policy is supported by complex risk measures. If a transaction is flagged as suspicious, the transaction is paused, and the customer involved is required to provide necessary actions or confirmations.