

SONNE N.V.

**CRYPTOASSETS
COMPLIANCE POLICY**

Version 1.0

Table of Contents

KEY INFORMATION	3
1. INTRODUCTION.....	4
2. GENERAL REGULATION	6
3. POLICY INTEGRATION	8
4. ONGOING MONITORING	9
5. TRAVEL RULE COMPLIANCE	11
6. SANCTIONS AND GEO-RISK MANAGEMENT	12
7. ANONYMOUS TRANSACTIONS PROHIBITION.....	13
8. RISK FACTORS.....	14
9. PREVENTIVE MEASURES	15
10. STAFF TRAINING	17
11. CONTACT INFORMATION	18
12. POLICY HISTORY	19

KEY INFORMATION

Approving Official(s):

- Morganite Corporate Services B.V, Director SONNE N.V.

Responsible Office:

- Compliance Department, SONNE N.V.

Effective Date:

- March 19, 2025

Next Review Date:

- March 19, 2026 (initial review within one year, subsequent reviews every three years. Additional revisions and updates are also possible upon significant regulatory, technological, or operational changes.)

1. INTRODUCTION

The gambling markets (online casinos) are evolving rapidly to accept cryptocurrency payments, but regulators are struggling to keep pace with the technology changes and put adequate safeguards in place to guard against potential money laundering risks. The information provided in this policy aims to clearly reflect the procedures, methods and approaches for accepting cryptocurrencies in the gambling sector and to provide the gambling regulator with an insight into the implementation of cryptocurrencies by operators and platform providers, the ways in which cryptocurrencies are used and the related regulatory measures already implemented in the company, as well as the possibility of further improving such measures.

Cryptocurrency is defined as a form of virtual asset that uses cryptography to secure financial transactions and is intended to be used as a new and alternative payment method. Cryptocurrencies run on a distributed public ledger called blockchain which provides a publicly available record of all transactions through the use of public keys. The driving force behind the development of these alternative payment systems was to remove a single point of failure (i.e.: the banks) by using peer-to-peer networks to verify and authenticate transactions on a publicly available blockchain. A transaction is considered verified once a miner solves a cryptographic (mathematical) puzzle. This peer-to-peer verification network enhances the transparency of transactions and theoretically eliminates the need for a central approving authority. Cryptocurrency transactions are supported by wallets (hot or cold) and accompanied by a public and private key. Hot wallets indicate that the user's private key is stored online and cold wallets indicate the private key is stored offline.

Nevertheless, there is a high probability that cryptocurrency and other virtual assets may be used for the purposes of money laundering and terrorist financing.

The primary purpose of this Cryptoassets Compliance Policy (hereinafter – the "**Policy**") is to ensure that the Company is in compliance with the FATF Recommendations and Guidance, including FATF Guidance for a Risk Based Approach to Virtual Assets and Virtual Asset Service Providers ("FATF Guidance") as applicable to the remote gaming sector.

The present Policy is implemented as part of the Company's wider AML/CTF obligations. The Company is committed to implementing a risk-based approaches to assessing, managing and mitigating the risk factors related to the use of Virtual Assets.

This Policy does not replace the existing Anti-Money Laundering and Counter-Terrorism Financing (AML/CTF) Policy implemented by SONNE N.V., but is intended only to expand and supplement it for the comprehensive protection of the Company and the counteraction to money laundering and terrorist financing.

2. GENERAL REGULATION

Cryptoassets encompass Virtual Assets that function as a medium of exchange, unit of account, or store of value within the SONNE N.V. (hereinafter referred to as the "**Company**") remote gaming operations or related financial activities. Virtual Assets are characterized by their fungibility and transferability in digital form. Non-fungible tokens (NFTs), such as digital collectibles or unique in-game assets, are excluded from the definition of Virtual Assets under this Policy unless they are used as a financial instrument. NFTs may be integrated into the gaming environment as rewards, collectibles, or other closed-loop benefits without constituting Virtual Assets.

The Company shall ensure full compliance with all applicable laws and regulations of Curaçao and other relevant jurisdictions governing the use of Virtual Assets in remote gaming and financial transactions. This includes adherence to anti-money laundering (AML), counter-terrorism financing (CTF), and know-your-customer (KYC) requirements. The Company shall implement robust monitoring and reporting mechanisms to ensure that Virtual Assets are used in accordance with regulatory standards.

Company") authorizes deposits and withdrawals using Virtual Assets. All withdrawal requests must utilize the same Virtual Asset and be directed to the Wallet address from which the customer's deposit originated, except in cases where:

- a) Security concerns necessitate the use of an alternative Wallet address;
- b) Other justifiable and documented reasons require a change, provided the alternative Wallet address is operated by a regulated Virtual Asset Service Provider (VASP).

The Company shall maintain detailed records of the rationale for using any alternative Wallet address to ensure transparency and compliance.

In order to properly regulate and enable the use of Cryptoassets in its activities, the Company is guided by both internal policies, including the Anti-Money Laundering and Counter-Terrorism Financing (AML/CTF) Policy, as well as applicable laws and regulations of the Government of Curacao, international laws and recommendations regarding the use of cryptoassets, including but not limited to: **National Ordinance on Money Laundering and Terrorist Financing (NOMLTF)**: Governs anti-money laundering (AML) and counter-terrorism financing (CTF) obligations, including customer due diligence, transaction monitoring, and reporting of suspicious activities involving Virtual Assets; **National Ordinance on the Supervision of Trust Service Providers**: Regulates entities providing services related to Virtual Assets, including Virtual Asset Service Providers (VASPs), ensuring

compliance with financial oversight requirements. FATF Recommendations: **Recommendation 15 (New Technologies)**: Requires jurisdictions and entities to assess and mitigate risks associated with Virtual Assets and VASPs, ensuring adequate AML/CTF measures are in place; **Recommendation 16 (Wire Transfers)**: Mandates the inclusion of originator and beneficiary information in Virtual Asset transactions to enhance traceability, commonly referred to as the "Travel Rule."; **FATF Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers (Updated October 2021)**: Provides detailed guidance on identifying, assessing, and managing risks related to Virtual Assets, including KYC procedures, sanctions screening, and suspicious transaction reporting; **5th Anti-Money Laundering Directive (AMLD5) (Directive (EU) 2018/843)**; **Central Bank of Curaçao and Sint Maarten (CBCS) Guidelines**.

3. POLICY INTEGRATION

This Cryptoassets Compliance Policy is fully integrated with the SONNE N.V. Anti-Money Laundering and Counter-Terrorism Financing (AML/CTF) Policy. All Virtual Asset transactions shall adhere to:

- ✓ **Customer Risk Assessment (CRA):** Virtual Asset users are subject to the AML/CTF Policy's risk scoring framework, with cryptocurrencies automatically classified as high-risk payment methods (AML/CTF Policy, Section 5.5).
- ✓ **Customer Due Diligence (CDD):** Identification, verification, and SoF/SoW checks for Virtual Asset transactions align with AML/CTF Policy thresholds ($\geq$ Naf. 4,000 or EUR 2,000) and EDD requirements for high-risk customers (AML/CTF Policy).

4. ONGOING MONITORING

The Company implements robust monitoring mechanisms to track transactions involving Virtual Assets including those conducted via VASPs and Self-hosted Wallets. Any suspicious activities or transactions that raise concerns regarding the SOF or destination of funds shall be promptly reported to the competent authorities.

The Company is planning to resort to specialized screening third-party providers and software for the purposes of:

- ✓ Monitoring incoming Virtual Asset deposits for potential links to sources associated with illicit activities.

Monitoring procedures include:

- Blockchain Analytics (з цією метою Компанія може співпрацювати third-party providers (e.g., Chainalysis, Elliptic)):
 - Screen incoming Virtual Asset deposits for links to illicit sources (e.g., dark pool wallets, sanctioned entities).
 - Trace transaction histories to identify mixing/tumbling services or anonymity-enhanced Virtual Assets.
 - Flag high-risk patterns, such as rapid fund movements across jurisdictions or disproportionate transaction volumes.
 - Behavioral anomalies (e.g., large deposits with minimal play, smurfing, or VPN usage).
- ✓ Detecting illicit sources of Virtual Asset funds and transactions associated with criminal activities;
- ✓ Flagging suspicious patterns or behaviors indicative of involvement in illicit activities.
- ✓ **Periodic Audits:** The Compliance Department conducts quarterly reviews of Virtual Asset transactions, with findings reported to the MLRO and documented for regulatory inspection.

The MLRO maintains a register of disclosures Suspicious Activity Reports (SARs) and ensures collaboration with law enforcement and regulatory bodies. The MLRO shall have full access to information and records of the company that the Director considers necessary to evaluate internal reports received.

If the MLRO considers that there is knowledge of, suspicion or reasonable grounds to suspect money laundering or terrorist financing the MLRO is responsible for:

- ✓ Submitting the necessary information to the FIU via the goAML portal within 7 days of detection, in English, with all relevant documentation;
- ✓ Recording the disclosure in the register of disclosures.
- ✓ Dealing with subsequent production or account monitoring orders if there are any.

Furthermore, the Company takes responsibility to collaborate with law enforcement agencies and regulatory bodies in investigations related to illicit activities and transactions with the use of virtual assets.

5. TRAVEL RULE COMPLIANCE

The Company complies with FATF Recommendation 16 (Travel Rule) for Virtual Asset transactions, ensuring traceability of originator and beneficiary information. Procedures include:

- ✓ **Data Collection:** Collection and verify originator and beneficiary details (e.g., name, wallet address, account number) for all Virtual Asset transactions.
- ✓ **Data Sharing:** Sharing Travel Rule data with counterparty VASPs via secure, standardized protocols (e.g., TRISA, OpenVASP), ensuring compliance with Curaçao's NOMLTF and EU AMLD5.
- ✓ **Counterparty VASP Verification:** Confirm that recipient VASPs are regulated and compliant with AML/CTF standards, per CBCS Guidelines. Transactions to non-compliant VASPs are flagged for EDD.
- ✓ **Record-Keeping:** Maintain records of Travel Rule data for ≥ 5 years, accessible to the FIU Curaçao upon request, per FATF Recommendation 11.

6. SANCTIONS AND GEO-RISK MANAGEMENT

The Company implements robust sanctions screening and geo-risk management for Virtual Asset transactions to mitigate ML/TF/FP risks:

- ✓ **Sanctions Screening:** All Virtual Asset transactions are screened against:
 - UN Sanctions List, EU Sanctions Map, FATF list and Curaçao sanctions lists (e.g., N.G. 2015, no. 27–30, 65).
 - Known illicit wallet databases via blockchain analytics tools.
 - Screening occurs at onboarding, during transactions, and every 6 months for existing customers, per Company AML/CTF Policy.

- ✓ **Geo-Risk Mitigation:** Virtual Asset transactions involving high-risk jurisdictions (as listed in AML/CTF Policy Appendix 1, e.g., Iran, North Korea) are subject to:
 - Enhanced Due Diligence, including SoF/SoW verification and senior management approval.
 - Geo-blocking of wallet addresses associated with prohibited jurisdictions, enforced via IP and blockchain analytics.

- ✓ **Tainted Asset Handling:** If a Virtual Asset is identified as tainted (e.g., linked to sanctioned entities or illicit activities), the transaction is frozen, and a SAR is filed with the FIU via goAML within 7 days. Funds are held until regulatory clearance, per AML/CTF Policy.

7. ANONYMOUS TRANSACTIONS PROHIBITION

Virtual Assets, Wallets and VASPs that are known to be used for the concealment or obfuscation of identity or the SOF (including so called mixing and tumbling services) are prohibited within the gaming ecosystem. The Company actively prevents the use of such identity and source concealment tools for remote gaming transactions and takes all the necessary measures to identify and address any attempts to circumvent transparency measures. First of all, Customers will not be able to register with fictitious names or anonymous accounts. When registering with a website owned by the Company, the account will not be opened unless the requested identity details (shown above) are completed in full. Duplicate accounts will not be allowed, and checks will be made at the time of registration.

Fictitious names will not be allowed. Obvious fictitious names will be identified at the time funds are deposited to the account and the account will be terminated.

A participant whose account is terminated shall be advised by email unless it is in relation to a matter reported to the FIU via the goAML.

8. RISK FACTORS

Generally, according to the cybersecurity and virtual asset guidelines, the following factors might be considered red indicators for the risk of money laundering and terrorist financing:

8.1. Anonymiser software, IP mixers, coin mixers and anonymity enhanced Virtual Assets:

these tools are designed to obfuscate the origin and destination of virtual assets, making it difficult to trace transactions. Their use may indicate an attempt to conceal illicit activities such as money laundering or terrorist financing.

8.2. IP does not match registration details provided: If the IP address used for transactions or account access is from a different geographical location than the one provided in the customer's registration details, it may suggest an attempt to hide the true location of the user, raising suspicion of fraudulent activity.

8.3. Significant transactions in Virtual Assets where the frequency or value is unusual:

Large or frequent transactions that deviate from the customer's typical transaction behavior or profile may indicate suspicious activity. This could include sudden large purchases or sales of VAs that are inconsistent with the customer's known financial situation or history.

8.4. Transactions involving Virtual Assets that are not plausible given the information known about the customer: Transactions that do not align with the customer's known business activities, income level, or stated purpose for using VAs can be a red flag. For example, a customer with a modest income making large Virtual Asset transactions without a clear source of funds.

8.5. Source of wealth is unclear or cannot be verified: If the origin of the customer's funds is unknown or cannot be reasonably verified, it increases the risk of those funds being derived from illegal activities. This includes situations where the customer is unable or unwilling to provide sufficient information about how they acquired their wealth.

8.6. Transactions involving jurisdictions with weak AML/CFT controls: Engaging in transactions with countries known for weak regulatory oversight or high levels of corruption can increase the risk of money laundering and terrorist financing.

8.7. Rapid movement of Value: Quick successive transfers between different VASPs and Wallets especially across different jurisdictions, may indicate layering which is a common money laundering technique used to obscure the origin of funds.

8.8. Use of anonymous payment methods for funding Virtual Asset transactions: The use of payment methods that offer anonymity can be a red flag, as they make it difficult to trace the source of funds.

9. PREVENTIVE MEASURES

The Company shall implement risk mitigation strategies to address the threat posed by illicit transactions and sources of funding, including:

- o Enhanced due diligence measures for Virtual Asset deposits that are deemed to be higher risk.
- o Regular training for staff on identifying and responding to illicit activity risks.
- o Collaboration with cybersecurity experts to strengthen platform defenses against criminal infiltration.

Some of the key safeguards in terms of AML/CTF with the use of virtual assets include:

- ✓ **Customer Verification.** Customers must be registered and have completed the customer identification processes and the wallet address must be verified as part of the customer identification procedures;
- ✓ **Payments:** Fiat and crypto payments shall be maintained separately and cannot be interchanged, the deposit method must be the same as the withdrawal method and the Company must also maintain logs of failed deposits and withdrawals. Crypto payments would only be allowable on approved online betting platforms, no live events or phone bets;
- ✓ **Responsible gambling limits** are applicable in fiat regardless of if the payment is made in crypto. Initial guidance would suggest limits of NAf. 4,000 or EUR 2,000 (single or linked), per EU Directive 2018/843.
- ✓ **Company shall hold wallets in the cryptocurrencies** traded with sufficient funds on hand to pay out any winnings and record the exchange rate at the time of the transaction;
- ✓ **Transaction monitoring** shall be conducted on a regular or real-time basis;
- ✓ **Conversion rates** must be up-to-date for value-based thresholds/alerts;
- ✓ **Consideration** shall be given to setting lower thresholds for CVC/VC than for fiat transactions;
- ✓ Monitoring shall include **in-game play, deposit frequencies and transaction patterns** rather than focusing only on value in, value out.

In certain cases, highlighted by the risk assessment, the Company may consider that a participant poses a higher risk. In these circumstances, enhanced due diligence will be requested and collected by the Company. Participants who pose an additional risk will be

recorded as high risk within the administrative system and a report of their transactions and any other relevant information made available to the MLRO.

The Company also recognizes the risks associated with the misuse of technological developments for the purpose of money laundering or the financing of terrorism.

Consequently:

- The management shall retain a close eye on technological developments that are taking place particularly in relation to phishing activity, identity fraud, money laundering etc.
- In addition, the Company shall engage with technology partners who are at the forefront of software and IT security and are engaged to maintain the on-going integrity of the website, servers and backup.
- The Company is committed to the continuous upgrading of its software and seeks to counter potentially adverse or threatening technological advancements through the implementation of best of breed software and security solutions.

10. STAFF TRAINING

It is key to effective AML/CFT arrangements that:

- Staff have sufficient knowledge or awareness to detect money laundering.
- Staff have sufficient training to know how to deal with cases once they know of or suspect money laundering.
- Staff are aware of their personal legal obligations.

The steps adopted by the group to ensure staff have appropriate awareness and training are as follows:

- ✓ All new staff will receive AML/CFT induction training, to include:
 - o The provisions of the AML/CFT including recognition of predicate offenses (EU Directive 2018/1673) and the appropriate internal procedures and policies including registration and identification procedures, record keeping etc.
 - o Their personal obligations under the AML/CFT and associated personal liabilities for non-compliance.
 - o The internal reporting procedures detailed in the AML/CFT Manual.
- ✓ AML/CFT refresher training shall be delivered for all staff and key persons
- ✓ The MLRO shall provide ad hoc information about news and developments. This will be targeted as appropriate.
- ✓ The MLRO shall send periodic reminders of the need to report certain matters.

11. CONTACT INFORMATION

For questions, contact:

- Compliance Department, SONNE N.V.
- Email: legal@sonne-it.org

12. POLICY HISTORY

Version	Date	Approved By
1.0	March 19, 2025	Morganite Corporate Services B.V., Director

Signed This 19th day of March 2025

A handwritten signature in black ink is written over a horizontal line. To the right of the signature is a circular corporate seal. The seal features the Morganite logo (a stylized 'M' inside a square) and the text 'MORGANITE' above 'CORPORATE SERVICES B.V.'. The outer ring of the seal contains the text 'CHAMBER OF COMMERCE NO. 2006' at the top and 'KONINKRIJK DER NEDERLANDEN' at the bottom.

Director: Morganite Corporate Services B.V.
Norine Clifton
Managing Director