LEGAL OPINION REGARDING THE VERUM COIN PROJECT

This Legal Opinion ("**Legal Opinion**") hereby is a legal opinion regarding the Verum Coin ("**VERUM**") decentralized cryptocurrency project. The purpose of this legal opinion is to evaluate VERUM's compliance with applicable data protection laws, including those in the European Union and the United States. It aims to identify any potential risks or gaps in the current practices, assess the effectiveness of the measures in place, and offer recommendations to ensure full compliance and mitigate legal and regulatory risks. The Document shall contain the following information Project Overview, Regulatory Compliance (including the GDPR, AML Act and MIFID in the EU. For the United States Law, the SEC uses the Howey Test[1] and SEC acts will be analyzed), Technical Analysis, Risk Identification, Investor Protection, Clarity and Guidance.

A. Project Overview

VERUM is a decentralized cryptocurrency designed to enable fast and cost-effective transactions on a global scale. The Verum ecosystem comprises several key components, each contributing to its overall functionality and growth. **This project is a UTILITY TOKEN** and not a Security token.[2]

The Verum blockchain operates on a proprietary network utilizing the Scrypt mining algorithm and a Proof-of-Work ("**PoW**") consensus mechanism. The total supply of Verum Coins is:

- Capped at **84,000,000**, with **7,159,250 coins mined** as of February 2024.

In addition to the native blockchain, VERUM tokens are also available on the Binance Smart Chain ("**BSC**") as **BEP20** tokens.

The Verum ecosystem offers a variety of privacy-focused applications, including:

- **Verum Messenger**: A secure messaging platform designed to ensure privacy.
- **Crypto Bank**: A platform for purchasing and exchanging VERUM coins.
- Additional services aimed at expanding the overall utility of the Verum blockchain.

B. Regulatory Compliance

This section will begin with an analysis of the General Data Protection Regulation ("**GDPR**"). In addressing the relevant provisions of the GDPR, we have chosen to focus on the following articles, as they encompass the critical aspects required for this legal opinion and are directly pertinent to the compliance of a cryptocurrency project under these provisions the assessment will draw from there relevant articles (i.e., article 4, article 12 etc., when need be):

- Article 5
- Article 15
- Article 17
- Article 25
- Article 30

[1] from the 1946 U.S. Supreme Court decision SEC v. W.J. Howey Co.

[2] Verum Ecosystem Overview; Verum Coin BEP20 Details ;Verum Blockchain Details

The MiFID and Anti-Money Laundering ("**AML**") legislation[3] shall be examined as integral components for the purpose of completing this legal opinion. Both legal instruments shall be considered in their entirety, and analyzed separately in a comprehensive manner, while being articulated broadly to ensure clarity and accessibility of understanding.

1. MiFID and AML Act (EU)

1.1. Verum Coin's AML and KYC policies are well-aligned with the requirements of **MiFID II**, particularly in terms of governance, risk management, client due diligence, and reporting. The firm demonstrates a strong commitment to preventing money laundering and terrorist financing through its risk-based approach, robust compliance function, and employee training programs. However, there is room for further alignment with MiFID II in areas such as conflict of interest management. Overall, Verum Coin's policies reflect a high standard of compliance with both AML/CFT regulations and MiFID II requirements.

1.2. MiFID II Article 3 requires investment firms to establish robust governance arrangements, including clear roles and responsibilities, effective risk management, and compliance functions. Verum Coin's AML and KYC policies demonstrate a strong alignment with these requirements. Verum Coin has clearly defined roles for the Board Members, Management, Compliance Department, and Compliance Officer. This aligns with MiFID II's emphasis on clear accountability and governance structures. The Board Members are responsible for approving AML/CFT policies and ensuring compliance. The Compliance Officer oversees the AML program, ensuring adherence to regulations and reporting suspicious activities.

1.3. Verum Coin adopts a risk-based approach to AML/CFT, which is consistent with MiFID II's requirement for firms to implement risk management systems. The policy includes: a) Risk-based assessments for clients, products, and services. b) Enhanced Due Diligence **("EDD")** for high-risk clients, such as Politically Exposed Persons ("**PEPs**") and clients from high-risk jurisdictions. c) Ongoing monitoring of accounts and transactions to detect suspicious activities.

1.4. Verum Coin has a dedicated Compliance Department that ensures adherence to AML/CFT regulations. This aligns with MiFID II's requirement for firms to have an independent compliance function that monitors and reports on compliance risks.

1.5. Verum Coin requires verification of all clients, including beneficial owners, before establishing a business relationship. This includes: a- Collecting and verifying identification documents. b- Conducting background checks on clients, including screening against sanctions lists (e.g., OFAC, UN sanctions). c- Ensuring that clients are not involved in illegal activities or prohibited jurisdictions.

1.6. For high-risk clients, such as PEPs or clients from non-cooperative countries, Verum Coin applies stricter KYC procedures. This includes: a- Conducting face-to-face meetings with high-risk clients. b- Investigating the source of funds and purpose of the account. c- Regularly reviewing and updating client information.

[3] Herein AML Act.

1.7. Verum Coin prohibits business relationships with entities involved in illegal activities, shell banks, or those using bearer shares. This aligns with MiFID II's requirement to avoid relationships that pose high risks of money laundering or terrorist financing.

1.8. MiFID II requires firms to maintain **accurate records** of client transactions and communications. Verum Coin's AML policy includes robust record-keeping practices. Verum Coin retains records of all transactions for at least **7 years** after the termination of the relationship. This ensures an audit trail for investigations. The Compliance Officer is responsible for reporting suspicious transactions to the **Estonian Financial Intelligence Unit (FIU)**. This aligns with MiFID II's requirement for firms to report suspicious activities to relevant authorities.

1.9. MiFID II emphasizes the importance of **employee training** to ensure compliance with regulatory requirements. Verum Coin's AML policy includes that all employees must undergo annual training on AML/CFT policies and procedures. This ensures that employees are aware of their obligations and can recognize suspicious activities.

1.10. MiFID II requires firms to assess the risks associated with clients from high-risk jurisdictions. Verum Coin's policy includes: a- Verum Coin prohibits business relationships with clients from countries subject to UN sanctions or OFAC prohibitions (e.g., Iran, North Korea, Syria). b Clients from jurisdictions with weak AML/CFT frameworks are subject to enhanced scrutiny, including verification of the source of funds and purpose of the account.

1.11. MiFID II requires firms to maintain confidentiality when handling sensitive information related to AML/CFT investigations. Verum Coin's policy includes: a- Tipping Off: Employees are prohibited from disclosing information about suspicious activity reports to clients or third parties. This aligns with MiFID II's requirement to prevent tipping off, which could compromise investigations. b- Confidentiality of Reports: Reports submitted to regulatory authorities must remain confidential, and unauthorized disclosures are subject to disciplinary action.

1.12. While Verum Coin's AML and KYC policies are comprehensive, there are areas where further alignment with MiFID II could be strengthened:

- **Conflict of Interest Management**: MiFID II requires firms to identify and manage conflicts of interest. Verum Coin's policy could explicitly address how conflicts of interest are managed in the context of AML/CFT compliance.

2. GDPR (EU)

2.1 Assessment of Article 5 GDPR

2.1.1. Regarding the three steps of necessities i.e., Lawfulness, Fairness and Transparency in article 5 The VERUM ecosystem emphasizes privacy by design. While its blockchain records transactional data, such data is pseudonymous and does not inherently constitute “personal data” under the GDPR, as wallet addresses or transaction hashes alone cannot directly identify natural persons without additional external information. For components that may involve personal data processing (e.g., the Crypto Bank platform, which may require Know-Your-Customer (“**KYC**”) checks), VERUM’s operators would be obligated to provide clear privacy notices and lawful bases (e.g., contractual necessity or legal obligation) for such processing, ensuring fairness and transparency. KYC checks are done internally by the VERUM team and further detailed under the companies AML and KYC Policy.[4]

2.1.2. Article 5(1)-b further covers the purpose limitation aspect of data which was established by the case law in the EU.[5] Any personal data processed by VERUM's ancillary services (e.g., user registration for Verum Messenger or KYC procedures for the Crypto Bank) would be collected only for explicit, legitimate purposes.

2.1.3. Data minimization aspect of VERUM blockchain is structured to record only essential transactional details (e.g., wallet addresses, amounts, timestamps), avoiding the collection of unnecessary personal data. Services like Verum Messenger, which prioritizes secure communication, employ end-to-end encryption and avoid storing message content, further minimizing data retention.

2.1.4. Blockchain immutability ensures transactional data cannot be altered retroactively. While this poses challenges for correcting inaccuracies in on-chain data, the pseudonymous nature of blockchain transactions means such data does not qualify as personal data under the GDPR unless linked to identifiable individuals.

2.1.5. On-chain data is retained indefinitely to maintain blockchain integrity, but this does not conflict with GDPR storage limitations, as the data is pseudonymous and not inherently personal. For off-chain services, VERUM's operators would establish retention policies to delete personal data (e.g., KYC information) once it is no longer necessary for its original purpose.

2.1.6. As for integrity and confidentiality of the system and the data VERUM has scored an 81/100 in the Cyberscope Smart Contract Audit.[6] Furthermore, VERUM's use of the Scrypt mining algorithm and PoW consensus mechanism ensures robust network security. Services like Verum Messenger and the Crypto Bank would employ robust encryption and access controls to protect user data, aligning with GDPR's requirement for technical and organizational safeguards.

2.1.7. While the decentralized blockchain lacks a central data controller, entities operating VERUM's ancillary services (e.g., the Crypto Bank or Verum Messenger) would bear accountability for GDPR compliance. These entities would be required to document processing activities, conduct Data Protection Impact Assessments (DPIAs) where necessary, and cooperate with supervisory authorities.

2.2. Assessment of Article 15 GDPR

2.2.1. Definitions

i. **Data Controller** refers to an entity that determines the purposes and means of processing personal data. This definition aligns with GDPR Article 4, which states that

[4] https://verumcoin.info/docs/AML_KYC_POLICY_VERUM_COIN.pdf

[5] Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Case C-131/12 <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62012CJ0131>

[6] https://www.cyberscope.io/audits/verum

a data controller is the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. The responsibilities of a data controller include ensuring compliance with GDPR requirements and safeguarding personal data.

ii. **Personal Data** any information relating to an identified or identifiable natural person" is also correct. Article 4(1) of the GDPR specifies that personal data refers to information that can identify a natural person directly or indirectly, through identifiers such as names, identification numbers, or location data.

iii. **On-Chain Data** refers to transactional records stored on the VERUM blockchain or Binance Smart Chain (BSC).

iv. **Ancillary Services** includes Verum Messenger, Crypto Bank, and other centralized platforms operated by VERUM or its affiliates.

2.2.2. Core VERUM Blockchain Compliance on-chain data (e.g., wallet addresses, transaction hashes) is pseudonymous and does not constitute Personal Data unless linked to identifiable individuals by ancillary systems or third parties.

2.2.3. VERUM acknowledges that no single entity acts as a Data Controller for the native blockchain. Consequently, VERUM shall not assume responsibility for fulfilling Article 15 requests related to on-chain data.

2.2.4. VERUM Messenger only collects essential Personal Data (e.g., account credentials) and employ end-to-end encryption to limit access to message content. Where Personal Data is processed (e.g., metadata, contact lists), VERUM shall:

a. Provide users with a secure portal to request access to their data;
b. Respond to requests within 30 days, per GDPR Article 12(3);
c. Refrain from storing message content beyond delivery.

2.2.5 KYC and AML obligations regarding the crypto platform bank the Crypto Bank shall process Personal Data (e.g., government-issued IDs, proof of address) solely for regulatory compliance and fraud prevention. The processing is done by the VERUM team.

2.2.5.1. VERUM, as Data Controller for the Crypto Bank, shall:
(a) Maintain a record of processing activities involving Personal Data;
(b) Enable users to request access to their KYC records via a dedicated interface;
(c) Provide a readable copy of the data, including purposes of processing and third-party recipients.

2.2.5.2. KYC data shall be retained only for the duration required by applicable law and deleted thereafter. Explicitly retains data for seven (7) years under AML laws, exempting erasure requests under Article 17(3)(b). Which is highlighted in the AML and KYC Policy.[7]

2.3 Assessment of Article 17 GDPR

[7] https://verumcoin.info/docs/AML_KYC_POLICY_VERUM_COIN.pdf

2.3.1. Article 17 grants users the right to request erasure of their personal data when:

- The data is no longer necessary for its original purpose.
- Consent is withdrawn.
- The data was unlawfully processed.
- Legal obligations (e.g., financial regulations) no longer require retention.

2.3.2. VERUM Messenger's Current Compliance Status Data Collection and Storage Practices: Users provide a nickname, password, and optionally an email for password recovery. Profile data (e.g., name, picture) is user-generated but not mandatory. End-to-end encrypted; content is not stored on VERUM servers. Message history resides solely on users' devices. Servers store authentication tokens, push tokens, and keys necessary for service functionality.

2.3.3. The VERUM messenger complies with Article 17 of the GDPR. Users can delete their accounts by uninstalling the app, and VERUM has implemented mechanisms to ensure that server-stored technical data is promptly and securely erased upon account deletion. Additionally, VERUM has established a defined data retention period for technical data.

2.3.4. VERUM crypto Bank Privacy Policy includes an explicit deletion process users can delete data directly through account settings or via a request, aligning with GDPR's accessibility requirements. Furthermore, clear acknowledgment of legal obligations to retain data (e.g., AML laws) complies with GDPR Article 17(3)(b). Also, affiliates are contractually bound to adhere to the policy, reducing risks of non-erasure in shared systems.

2.3.4.1. The VERUM crypto Bank Privacy Policy; ensures data is retained only as necessary, with clear retention timelines in line with GDPR's storage limitation principle (Article 5(1)(e)). Service providers and business partners are required to delete data upon user request, and the client is accountable for ensuring erasure across all processors. VERUM implements specific mechanisms like SCCs and Binding Corporate Rules for non-EEA transfers, and adheres to the 30-day GDPR deadline for erasure requests (Article 12(3)).

2.4. Assessment of Article 25 GDPR

2.4.1. The VERUM ecosystem demonstrates partial adherence to GDPR Article 25, which mandates *privacy by design* (integrating data protection into system architecture) and *privacy by default* (minimizing data collection and exposure by default). For Verum Messenger, end-to-end encryption, minimal account data collection (nickname, optional email), and on-device message storage reflect privacy-centric design principles. The rest of the ecosystem follows article 25 of the GDPR.

2.4.2. For Crypto Bank, while KYC data collection is required for regulatory compliance, VERUM has ensured clear retention timelines, anonymization after retention, and implemented safeguards for international transfers.

2.4 Assessment of Article 30 GDPR

2.4.1. The VERUM Coin AML/KYC Policy demonstrates compliance with GDPR Article 30, which requires controllers to maintain detailed records of data processing activities. The policy explicitly documents retention periods (e.g., 7+ years for client data post-termination), purposes of processing (AML/CFT compliance, client due diligence), and categories of personal data collected (e.g., IDs, transaction records, PEP status). It also outlines data sharing with third parties (e.g., affiliates, regulators) and international transfers, with specifying GDPR-recognized mechanisms like Standard Contractual Clauses (SCCs). These elements align with Article 30's mandate to record processing purposes, data categories, and recipients.

3. US Law and Regulation

3.1. Compliance with the Travel Rule (31 CFR § 1010.410(f))[8]

3.2. The Travel Rule mandates that financial institutions, including cryptocurrency exchanges, transmit specific customer information during fund transfers exceeding **$3,000**. Required information includes: a- Sender's name, address, and account number. b- Recipient's name, address, and account number. c- Amount and execution date of the transaction.

3.3. Analysis of VERUM's AML/KYC Policy

3.3.1. VERUM's policy emphasizes client identification and verification (KYC), including collecting names, addresses, and account details.

3.3.2. It requires record-keeping for transactions (retained for 7 years), which aligns with U.S. requirements (5 years under FinCEN).[9]

3.3.3. Compliance with the Travel Rule and has established clear procedures for transmitting and receiving sender/recipient data during transactions. Additionally, the client provides specific guidance on handling transactions involving third-party intermediaries, such as nested exchanges or money transmitters.

3.5. Suspicious Activity Report ("SAR") Reporting (31 CFR § 1022.320)

3.5.1. U.S. law requires filing SARs for transactions over $5,000 that involve suspected: 1- Money laundering. 2- Terrorist financing. 3- Fraud or other criminal activity.

3.5.2. VERUM has transaction monitoring systems to detect unusual activity. Also, it mandates reporting suspicious transactions to the FIU.

3.5.3. VERUM complies with requirements related to SAR filing for U.S. transactions, including reporting to FinCEN.

3.5.4. VERUM has complies with SAR filing procedures with FinCEN for U.S. transactions, setting internal thresholds, and focusing on a 30-day deadline for submissions. For cross-border compliance, transactions are screened for U.S. nexus, and SAR requirements are applied as needed.

3.5.5. The risk of non-compliance with U.S. law can result in significant penalties. Civil penalties may include fines of up to $250,000 per violation, particularly for failures related to the Travel Rule or SAR filings. Additionally, criminal penalties for willful violations could lead

[8] Herein The Travel Rule

[9] Financial Crimes Enforcement Network.

to imprisonment for compliance officers, further emphasizing the importance of adhering to regulatory requirements.

C. Conclusion

Upon review of the relevant policies, it is our professional opinion that the AML and KYC policies are, on the whole, robust and in alignment with applicable legal and regulatory standards. We have reviewed the privacy policies and found that the identified deficiencies have been successfully addressed, particularly in terms of transparency and data protection provisions. These improvements significantly reduce potential legal risks and regulatory scrutiny. The steps taken ensure compliance with relevant data protection laws and mitigate associated risks.

[redacted]