CRYPTO BLOCKCHAIN INDUSTRIES

CBI Compliance Policy

Version February 09, 2022

1 – INTRODUCTION

Money laundering and the financing of terrorism have been identified as risks to Crypto Blockchain Industries, SA (the "Company"). Legislation derives from the European Union Anti-Money Laundering Directives. Individual guidance is provided by each jurisdiction where the Company operates, hence we are obliged to adhere to this guidance.

CBI activities are in compliance with the French regulation (Sapin Law December 9 2016) the European directive, the 2010 UK anti bribery act.

This legislation, together with regulations, rules and industry guidance/codes, forms the cornerstone of Anti-Money Laundering (AML)/Countering the Financing of Terrorism (CFT) obligations for relevant financial businesses and outlines the offences and penalties for failing to comply. In particular, the Proceeds of Crime Act was amended on 16th March 2018 to bring within scope of AML "undertakings that receive, whether on their own account or on behalf of another person, proceeds in any form from the sale of tokenised digital assets involving the use of distributed ledger technology or a similar means of recording a digital representation of an asset."

The requirements of the different legislations apply to the Company globally. The Company may have additional local policies and procedures designed to comply with their local legislation, regulations and any government approved guidance in the jurisdiction(s) in which they operate.

2 – POLICY STATEMENT

The Company and its directors are committed to full compliance with all applicable laws and regulations regarding money laundering and the financing of terrorism. Every officer, director, employee and associated person of the Company is responsible for assisting in the Company's efforts to detect, deter and prevent money laundering and other activities intended to facilitate the funding of terrorism or criminal activities through its business.

CRYPTO BLOCKCHAIN INDUSTRIES

3 – SCOPE

This Policy applies to all of the Company's customers. This Policy also applies to all staff and any third party the Company might do business with.

4 – LEGAL AND REGULATORY FRAMEWORK

The principal requirements, obligations and penalties, on which the Company's Systems and Controls are based, are contained in the EU Anti Money Laundering Directives and applicable texts and regulations.

5 – WHAT IS MONEY LAUNDERING

Money laundering is the generic term used to describe the process by which criminals disguise the original ownership and control of the proceeds of criminal conduct by making such proceeds appear to have derived from a legitimate source.

6 – MONEY LAUNDERING OFFENCES & PENALTIES

6.1 A person commits an offence if he enters into or becomes concerned in an arrangement which he knows or suspects facilitates (by whatever means) the acquisition, retention, use or control of criminal property by or on behalf of another person. The maximum penalty for this offence on conviction on indictment is fourteen years in prison or a fine or both.

6.2 A person commits an offence if he- (a) acquires criminal property; (b) uses criminal property; or (c) has possession of criminal property. The maximum penalty for this offence on conviction on indictment is fourteen years in prison or a fine or both.

6.3. A person commits an offence if he- (a) conceals criminal property; (b) disguises criminal property; (c) converts criminal property; (d) transfers criminal property;

6.4 A person is guilty of an offence if– (a) he discloses that a money laundering suspicion report has been made or is being contemplated or is being carried out; and (b) the information on which the disclosure is based came to him in the course of a business or activity in the regulated sector The maximum penalty for this offence on conviction on indictment is five years in prison or a fine or both.

6.5 A person is guilty of an offence if– (a) he knows, suspects or has reasonable grounds to suspect that another person is engaged in money laundering, or is attempting to launder money; (b) the information or other matter, on which that

knowledge or suspicion is based came to his attention in the course of his trade, profession, business or employment

7 – WHAT IS TERRORISM FINANCING

Terrorist financing means: (a) the use of funds or other assets, or the making available of funds or assets, by any means, directly or indirectly for the purposes of terrorism; or (b) the acquisition, possession, concealment, conversion or transfer of funds that are (directly or indirectly) to be used or made available for those purposes. Compared with money laundering (which involves the proceeds of all crimes), the amount of money that could be used as terrorism financing is quite small and can also come from legitimate sources. However, the social, political and economic consequences of allowing terrorist organizations to function and prosper are devastating and it is for this reason that Company staff must be on the alert for terrorist financing as well as for the proceeds of crime.

8 – TERRORISM FINANCING OFFENCES & PENALTIES

A person commits an offence if he- (a) Raises funds for terrorism (b) Uses and possesses money or other property for terrorism (c) Arranges funds for terrorism (d) Arranges the retention or control of terrorism property The penalty for these offences is fourteen years in prison or a fine or both.

9 – MONEY LAUNDERING REPORTING OFFICER (MLRO)

The MLRO position is held by Alain Scémama. The activity of the MLRO will start when the AlphaVerse website will start to operate.

It is a requirement for a director of the Company to have overall responsibility and oversight of all compliance matters by the Company and its officers and staff. This position is known as the Compliance Officer. It is a requirement for the Company to appoint an MLRO. The holder of this position, in the Company, would be a member of the Compliance & Regulatory Team (if any, and failing that, an independent officer of the Company nominated by the Company's board of directors). This position is also known as the 'appropriate person' or 'nominated officer'.

The MLRO is responsible for:

- Developing, implementing and overseeing all AML matters within the business;
- Undertaking a risk assessment for the business;
- Creating relevant policies, processes and procedures to prevent the Company from being misused for criminal activity;

- Providing training to staff in order for them to be able to identify red flags;
- Receiving and considering any internal suspicious activity reports;
- Liaising with the relevant Commissioner, the appropriate Financial Intelligence Unit ('FIU') and any other relevant government authority;
- Submitting regulatory reports; and
- Presenting an MLRO report to the Board, at least annually, whereby the operation and effectiveness of the Company's systems and controls is evaluated.

10 – REPORTING: SUSPICIOUS ACTIVITY REPORTS (SAR)

The Company is required to report all circumstances where it has knowledge, suspicion, or reasonable grounds to suspect that money laundering or the financing of terrorism is being or has taken place or attempted through its facilities.

Employees will submit SARs where relevant. The MLRO makes the SARs form available to any employee upon request.

The MLRO is responsible for investigating any internal SAR received and/or any suspicion of money laundering/ terrorist finance.

When considering a SAR, the MLRO determines whether or not it needs to be disclosed to the authorities. In making a decision, the MLRO will consider, amongst others: • the information available regarding the case, i.e.: customer information, documentation, media news; • transactions involved; • account activity inconsistent with the customer's risk profile; • correspondence with the customer; • the reasons for suspicion, etc.

Based on the above consideration, if the MLRO knows or suspect or has reasonable grounds to know or suspect that money laundering or terrorist financing has taken place, then a disclosure will be made accordingly. In the case the MLRO decides not to make a disclosure, this will be thoroughly documented with the reasons why, and shared with the Chief Executive Officer. The MLRO will record all internal SARs received by employees in the SAR's Log. This Log will be kept up to date with any new information that might arise on any given case.

11– CUSTOMER IDENTIFICATION (KNOW YOUR CUSTOMER)

The Company will set up this process when the AphaVerse web site will operate.

Know Your Customer ("KYC") KYC is the process that the company will use to verify the identity of our customers. There are different levels of due diligence we need to perform. This will be determined on a risk-based approach. The Company will apply CDD when: (a) it establishes a business relationship; (b) it suspects money laundering or terrorist financing; (c) it doubts the veracity or adequacy of documents or information previously obtained for the purposes of identification or verification; and (d) it receives

any amounts from the sale of tokens. Moreover, the Company will also apply CDD: (e) in relation to any transaction that amounts to € 1.000 or more, whether the transaction is executed in a single operation or in several operations which appear to be linked; (f) at other appropriate times to existing customers on a risk-based approach; (g) when the Company becomes aware that the circumstances of an existing customer relevant to its risk assessment for that customer have changed; or where there is a legal duty to contact the customer (in the case of a customer that is not an individual) for the purpose of reviewing any information relating to the beneficial owner or beneficial owners

Enhanced Due Diligence (EDD) A 'relevant financial business' must apply EDD measures to appropriately manage and mitigate risks: (a) in the cases referred to in Articles 19 to 24 of the European Union Fourth Anti-Money Laundering Directive (the "Directive"); (b) when dealing with natural persons or legal entities established in third countries identified by the European Commission as high risk third countries; and (c) in other cases of higher risk identified: (i) by the relevant financial business; or (ii) by the Minister by notice in the Gazette. EDD measures need not be invoked automatically with respect to branches or majority-owned subsidiaries of obliged entities established in the European Union which are located in high-risk third countries, where those branches or majority-owned subsidiaries fully comply with the group-wide policies and procedures in accordance with Article 45 of the Directive, and such cases must be handled on a risk sensitive basis. Where the customer is not physically present for identification purposes, the relevant entity must take specific and adequate measures for the higher risk, such as: (a) ensuring that the customer's identity is established by additional documents, data or information; (b) supplementary measures to verify or certify the documents supplied, or requiring confirmatory certification by a credit or financial institution which is subject to the Directive; and (c) ensuring that the first payment is carried out through an account opened in the customer's name with a credit institution.

The Company will apply enhanced customer due diligence measures and enhanced ongoing monitoring in order to manage and mitigate the money laundering or terrorist financing risks arising in the following cases: (a) where there is a high risk of money laundering or terrorist financing; (b) where the customer is situated in a high-risk third country identified by the European Commission (c) where a customer or potential customer is a PEP, or a family member or known close associate of a PEP; (d) in any case where a transaction is complex or unusually large, or there is an unusual pattern of transactions, and the transaction or transactions have no apparent economic or legal purpose;

Where the Company discovers that a customer has provided false or stolen identification documentation or information, and/or where the information held by the Company differs from that of the customer's transaction patterns, the relationship will be terminated. Any customer account closed on these circumstances, will be added to an internal blacklist. The enhanced measures will include, but not be limited to: (a) examining the background and purpose of the transaction, as far as reasonably possible; (b) increasing the degree and nature of monitoring of the business

relationship in which the transaction is made, to determine whether the transaction or the relationship appear to be suspicious; (c) depending on the requirements of the case, may also include, among other things: seeking additional independent, reliable sources to verify information provided or made available to the Company; taking additional measures to understand better the background, ownership and financial situation of the customer, and other parties to the transaction, i.e. payslips, savings, inheritance, bank statements, etc.; (d) taking further steps to be satisfied that the transaction is consistent with the purpose and intended nature of the business relationship; (e) increasing the monitoring of the business relationship, including greater scrutiny of the transactions.

Therefore, applying CDD measures involves several steps:

1. The Company is required to identify customers; (a) identification of a customer means being told or coming to know of the customer's identifying details, such as their name and address. The Company identifies the customer by obtaining a range of information about the customer.
2. The Company must then verify the customers identities, upon registration; Verification means obtaining some evidence which supports this claim of identity. The verification of the identity consists of the Company verifying the information received against documents, data or information obtained from a reliable and independent source.
3. The Company must also verify and whitelist the wallets from which customers remit any cryptocurrencies; verification means obtaining some evidence which confirms the wallet: (i) is not related to terrorist financing; (ii) is not related to the darknet market; (iii) does not belong to mixers; or (iv) does not relate to a sanctioned country. The verification of the wallet consists of the Company verifying the information received against documents, data or information obtained from a reliable and independent source.
4. The company shall also collect IP addresses and to the extent applicable MAC addresses from its customers during the identification and verification process.
5. All purchase of NFT that the customer can use in the company website are made through third party which are independent and outside the company control. Those websites as Opensea or Binance have got their own compliance policy which covered all the compliance risk. Open sea policy is in the address: https://opensea.io/tos; Binance policy is in the address: https://www.binance.com/fr/terms.

12 – ANONYMOUS AND/OR DUPLICATE/MULTIPLE ACCOUNTS

The Company will set up this process when the Alphaverse web site will operate.

The Company does not permit the use of anonymous and/or duplicate/multiple accounts. The Company will have as the necessary systems and controls in place to detect and deter these occurrences. If a customer is found to have opened more than one account, the accounts will be closed. The Company will use a software (or

procure the services of a third-party service provider) to be able to identify this type of accounts. Daily reports will then be analyzed by the Risk and Payment Team, who will then take actions (i.e.: close accounts) accordingly.

13 – ONGOING MONITORING

The Company will perform ongoing monitoring of its customers. The Company will use a software provider who analyses customers' historical information and account profile. This is the way a "whole picture" is produced which analysis customer's profile, risk levels, and predicted future activity. The software also generates reports and create alerts to suspicious activity which are further analyzed by the Company to take actions accordingly. There will also be instances whereby the analysis of transactions, information and/or documentation needs to be done manually. The responsibility for this analysis will depend on various factors, but generally will be performed by fraud, risk and/or compliance.

14 – RECORD KEEPING

The Company keeps records of the procedures applied to establish the identity of its customers, and records of the value of their transactions, for at least 5 years after the relationship ends. This is consistent with data protection legislation.

15 – POLITICALLY EXPOSED PERSONS ("PEPs")

A PEP generally presents a higher risk for potential involvement in bribery and corruption by virtue of their position and the influence that they may hold.

Definition The Directive defines a 'politically exposed person' as a natural person who is or who has been entrusted with prominent public functions and includes the following: (a) heads of State, heads of government, ministers and deputy or assistant ministers; (b) members of parliament or of similar legislative bodies; (c) members of the governing bodies of political parties; (d) members of supreme courts, of constitutional courts or of other high-level judicial bodies, the decisions of which are not subject to further appeal, except in exceptional circumstances; (e) members of courts of auditors or of the boards of central banks; (f) ambassadors, chargés d'affaires and high-ranking officers in the armed forces; (g) members of the administrative, management or supervisory bodies of State-owned enterprises; (h) directors, deputy directors and members of the board or equivalent function of an international organization. No public function referred to in points (a) to (h) shall be understood as covering middle-ranking or more junior officials; 'family members' includes the following: (a) the spouse, or a person considered to be equivalent to a spouse, of a politically exposed person; (b) the children and their spouses, or persons considered

to be equivalent to a spouse, of a politically exposed person; (c) the parents of a politically exposed person; 'persons known to be close associates' means: (a) natural persons who are known to have joint beneficial ownership of legal entities or legal arrangements, or any other close business relations, with a politically exposed person; (b) natural persons who have sole beneficial ownership of a legal entity or legal arrangement which is known to have been set up for the de facto benefit of a politically exposed person. All identified PEPs will be assessed by senior management and a decision will be made on whether to continue with the relationship or terminate it. This will then be recorded in the PEPs Log. PEPs are monitored jn a daily, using a data software, in order to identify any new information which might change their risk profile.

16 – SANCTION LISTS

All new customers are screened against sanction lists. If a potential or current customer is identified as being in a sanction list, the relationship will be terminated immediately. Under no circumstances the Company will, knowingly, engage in a relationship with a person and/or organization appearing in a Sanctions List. Screening of customers against PEPs databases and Sanctions Lists is performed on a daily basis

17– COOPERATION WITH GOVERNMENT BODIES

The Company is committed to the fight against money laundering and the financing of terrorism. As such, the Company will cooperate with any and all law enforcement requests.

External Data Request Any external request received by the Company will be dealt with by the Compliance Department (if any, and failing that, by the board of directors) or other officer and escalated to a director where appropriate. All staff is made aware of this process, both, through this Policy and via internal email communications.

18 – COMMUNICATION

This policy will be placed on the Intranet page and also communicated to staff by email. When the Company engages in business with third parties, this Policy will be provided.
Any changes or amendments to this Policy, will also be communicated to relevant stakeholders (i.e.: employees, third parties, etc.) accordingly.

19 – REVIEW

The Company will review this policy, at least, every year. The review will involve all relevant stakeholders. The Company will make such changes as are reasonably necessary to comply with this Policy and any ongoing license obligations.

20 – NON-COMPLIANCE

All Company's employees are required to read and comply with this policy. Failure to comply with this policy would be considered gross misconduct and might result in termination of employment.

21 – GENERAL DATA PROTECTION REGULATIONS ("GDPR")

This Privacy Notice explains how and why the Company may use personal data, The handling of personal data is treated seriously and the Company respects privacy and rights to control personal data.

How the Company collects data The Company collects personal data when an individual registers their personal details directly with the Company in respect of the proposed token sale.

Lawful basis on which Personal data is relied upon (a) Where an individual has actively registered their interest through the Company's website, the lawful basis for holding and processing personal data would be a "contractual" basis. (b) Personal data collected is subject to third party checks as part of the token sale requirement to combat Money Laundering. In these circumstances where there is a direct contractual relationship between the Company and the individual, the Company is collecting and processing personal data on the basis of legitimate interest. By providing personal data for this purpose individuals accept and agree that the basis upon which the Company is processing personal data is legitimate interest. The Company will only process personal data in accordance with the GDPR. (c) The Company would also retain and process personal data if there is a legal obligation to do so. In order to operate and improve our business, there is also a valid legitimate interest basis for holding and processing of personal data. The Company might also have requested explicit consent in order to use personal data. Where the Company processes personal data based on consent, individuals have a right to withdraw consent at any time.

Principles for collection and processing of personal data The Company has adopted the following general GDPR principles to support and govern its collection and processing of Personal Data: • Personal Data shall be processed lawfully, fairly, and in a transparent manner. • Personal Data shall only be retained for as long as it is required to fulfil contractual requirements. • Personal Data shall be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are collected and/or processed. • Personal Data shall be accurate and, where necessary, kept up to date. • The Data Subject has the right to request from the Company access to and rectification or erasure of their personal data, to object to or request restriction of processing concerning the data, or to the right to data portability.

Disclosure of Personal Data the Company may disclose personal data to certain permitted third parties, such as third-party service providers or cloud service providers,

to comply with contractual obligations. The Company will never sell personal data and will only share it with organizations the Company works with when it's necessary and the privacy and security of personal data is assured.

Personal Data Retention Policy the Company will keep personal information for as long as the Company need it for the purpose it is being processed for, considering any legal obligation the Company may have (e.g. to maintain records for fiscal or reporting purposes), any other legal basis the Company may have for using information The Company will keep the information for a period as set by GDPR.

Data Subject Right Individuals have certain rights over their personal data and data controllers are responsible for fulfilling these rights. The Company are the data controllers, where we decide how and why personal data is processed. Under GDPR, individuals have a right to: (a) know what data is processed, how it is processed and shared and to receive a copy of their personal data (b) erasure, where there are no laws or regulations which mandate the retention of that data (c) rectification of inaccurate personal data (d) withdraw their consent (e) data portability (f) restriction of processing of specific personal data items (g) object to processing performed in the legitimate interests of the Company subject with the objection evaluated in the context of the risk to the data subject (h) object to direct marketing and have the direct marketing ceased immediately (i) be subject to a decision based solely on automated processing (j) claim compensation for damages caused by a breach of the Act.

Access to Personal Data An individual's right to access can be exercised in accordance with the EU General Data Protection Regulation 2016. Any requests from data subjects about the information held on them must be documented and include the nature of the request and the response given. To progress your request two forms of identification (ID) will also be required before any data is compiled, these must be dated within the last three months. The Company, upon being satisfied that an individual meets the criteria for disclosure of data under GDPR, will provide a response to the individual within 28 days from that date.

* * *