Anti-Money Laundering and Combating Financing of Terrorism Policy
28 February 2019

Anti-Money Laundering and Combating Financing of Terrorism Policy ("CRYPTOWARS OU AML-CFT POLICY")

28 February 2019

1. Introduction

Cryptowars OU, a company registered under the legislation of Estonia, with it's registered number 14616880, having it's legal address at Harju maakond, Tallinn, Kesklinna linnaosa, Narva mnt 7-634, 10117 ("**The Company**") the owner of the website available in the Internet via https://cryptowars-ou.com, places great emphasis on integrity and good governance and is committed to the highest standards of anti-money laundering ("**AML**") and combating the financing of terrorism ("**CFT**" and, together with AML, **"AML-CFT**") in line with the principles and standards of applicable Estonian and EU legislation, best banking practices and applicable market standards including, where relevant, other international financial institutions' standards.

This *"Cryptowars OU Anti-Money Laundering and Combating Financing of Terrorism Policy"* ("**The Company AML-CFT Policy**") establishes the key principles regulating AML-CFT and related integrity aspects in The Company activities is complemented by detailed operational procedures implemented by the Company for its respective daily operations.

Adherence to the Companys' AML-CFT Policy and its implementing procedures is the shared responsibility of all the Company staff and members of governing bodies.

Scope

2.1. Objectives

The Company AML-CFT Policy and its implementing procedures are intended to establish principles designed to prevent The Company, its governing bodies, staff and counterparties from being used for, or connected with, Money Laundering, Financing of Terrorism or other criminal activities.

Adherence to the Company AML-CFT Policy also aims at preventing the Company from being exposed to reputational damage and financial loss in relation to non-compliance with applicable AML-CFT standards. Our Companys' goals require compliance with AML-CFT EU Directives to the extent that these are applicable to The Company activities (Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC).

2.2. Applicability

This AML-CFT Policy is applicable to the Companys' operations and activities, as detailed in the applicable implementing procedures from time to time in force.

2.3. Definition of "Money Laundering"

"**Money Laundering**" is the conversion or transfer of property, knowing that such property is derived from criminal activity or from an act of participation in such activity, for the purpose of concealing or disguising the illicit origin of the

property or of assisting any person who is involved in the commission of such an activity to evade the legal consequences of that person's action;

the concealment or disguise of the true nature, source, location, disposition, movement, rights with respect to, or ownership of, property, knowing that such property is derived from criminal activity or from an act of participation in such an activity;

the acquisition, possession or use of property, knowing, at the time of receipt, that such property was derived from criminal activity or from an act of participation in such an activity;

participation in, association to commit, attempts to commit and aiding, abetting, facilitating and counselling the commission of any of the actions referred to in foregoing points[1].

2.4. Definition of “Financing of Terrorism”

"Financing of Terrorism" is the provision or collection of funds, by any means, directly or indirectly, with the intention that they be used or in the knowledge that they are to be used, in full or in part, to commit, or to contribute to the commission of, any of the offences referred to in Articles 3 to 10 of Directive (EU) 2017/541 of 15 March 2017 on combating terrorism. Where the Financing of Terrorism concerns any of the offences laid down in articles 3, 4 and 9 of Directive (EU) 2017/541, it shall not be necessary that the funds be in fact used, in full or in part, to commit, or to contribute to the commission of, any of those

[1] See definition in Art. 1 (3) Directive (EU) 2015/849, as amended and supplemented from time to time.

offences, nor shall it be required that the offender knows for which specific offence or offences the funds are to be used[2].

3.Counterparty Due Diligence – Risk-Based Approach

The Company applies the following counterparty due diligence measures, as determined on a risk-sensitive basis taking into account where relevant the type of counterparty, business relationship, product or transaction and country of operation[3].

3.1. Identification and Verification of Identity of Counterparty

The Company identifies and verifies the identity of the counterparties with which it enters into business relationships on the basis of documents, data or information obtained from reliable independent sources.

3.2. Identification and Verification of Identity of Beneficial Owner(s)

Whenever the Company is required to identify a counterparty, it identifies and takes reasonable measures to verify the identity of the beneficial owner(s) i.e. the individual(s):

Who (ultimately) own(s) or control(s) the counterparty or its assets;

Or on whose behalf the transaction is carried out or the business relationship with the Company is established.

[2] See definition in Art. 1 (5) Directive (EU) 2015/849, as amended and supplemented from time to time, together with Art. 11 of Directive (EU) 2017/541 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA
[3] See Directive (EU) 2015/849 (Art. 13), as amended and supplemented from time to time

3.3. Establishment of Purpose of Business Relationship

The Company takes reasonable measures to duly assess the purpose, intended nature, economic rationale and overall AML-CFT and related integrity aspects of the business relationship in order to avoid being involved in business relationships structured for the purposes of criminal activities or co-financed through funds of possibly illicit origin.

3.4. On-going Monitoring

On-going monitoring (including monitoring of transactions) is implemented on a risk-sensitive basis to detect possible Money Laundering, Financing of Terrorism or related integrity risks arising throughout the life of the business relationship.

4. Reporting Obligations

Under the Anti-Fraud Policies, any member of the Company staff or governing bodies is required to report any suspected incidents of illegal behaviour in the activities of the Company, serious misconduct or serious infringement of the rules, policies or guidelines, or any action which is, or could be, harmful to the mission or reputation of the Company, immediately after becoming aware of the matter.

Suspicions that funds, regardless of the amount involved, are the proceeds of criminal activities or related to Money Laundering or Financing of Terrorism in the activities of the Company, must be reported for assessment and investigation, as appropriate, to the Compliance Officer.

The Company must ensure confidentiality for members of the Company staff and governing bodies who make bona fide reports of suspicions of Money Laundering or Financing of Terrorism and that such members of staff and governing bodies

will enjoy the assistance and protection of the Company against any acts of retaliation.

5. Sanctions Compliance

The Company is committed to comply with sanctions that apply to the Company operations and activities (EU, UN, and as determined by the Company, Sanctions Authorities outside the EU).

6. Roles and Responsibilities of The Company Governing Bodies and Staff

The Company has designated its Compliance Officer as its Anti-Money Laundering Program Compliance Person (AML Compliance Person), with full responsibility for this AML/CFT Policy. The Copmpliance Officer has a working knowledge of compliance requirements and its implementing regulations and is qualified by experience, knowledge and training. The duties of the AML Compliance Person will include monitoring the firm's compliance with AML obligations, overseeing communication and training for employees. The AML Compliance Person will also ensure that the firm keeps and maintains all of the required AML records. The AML Compliance Person is vested with full responsibility and authority to enforce this Policy, inform the counterparty(ies), or other third parties, that a suspicious transaction is being, will be or has been reported or investigated is prohibited ("no-tipping off").

All members of the Company staff and governing bodies are under an obligation to implement the principles established in this AML-CFT Policy in accordance with the operational terms established in the implementing procedures.

The Company staff with counterparty-facing transaction execution/monitoring responsibilities are the first-line of defence and first-line detectors for i)

identifying suspicions of criminal activities in relation to counterparties, operations or transactions and ii) reporting them immediately in accordance with Article 4.

7. Record Retention

Records must be kept of all transaction data and data obtained for the purposes of identification, as well as of all documents related to AML-CFT[4].

8. Data Protection

Personal data submitted to the Company under this AML-CFT Policy and its implementing procedures are processed under the supervision of The Compliance Officer for the sole purpose of AML-CFT, and in accordance with (EC) Regulation 45/2001 on the protection of individuals with regard to the processing of personal data by the Community Institutions and Bodies and on the free movement of such data ("**Data Protection Regulation**"). The processing of personal data for the purposes of AML-CFT is considered by Directive (EU) 2015/849 to be a matter of public interest and as such, the processing is lawful for the purposes of the Data Protection Regulation[5].

Data subjects are entitled to access, rectify and, for duly justified reasons, block and erase these data ("**Rights of the Data Subject**"), and may exercise their rights by contacting the Company by email contact@cryptowars-ou.com. Data subjects also have the right of recourse to the European Data Protection Supervisor at any time.

[5] Article 5 (a): "processing is necessary for the performance of a task carried out in the public interest (…)".

Detailed provisions relating to the application of the Data Protection Regulation for AML-CFT purposes are available in Annex 1.

9. Training

Adequate AML-CFT training, including on the processing of personal data, is provided as appropriate to the Company governing bodies and staff. Such AML-CFT training is provided to all staff, and in addition specific training, as available from time to time, may be provided to staff responsible for carrying out transactions received or initiated by the Company and/or for initiating and/or establishing business relationships.

10. Review

The Company keeps this AML-CFT Policy under review in cooperation with the Company services concerned and proposes for approval by the relevant management body any appropriate updating in line with Estonia and EU legal and regulatory development and best banking practices or applicable market standards including where relevant other international financial institutions' standards.

Annex 1

Data Protection Statement for AML-CFT Requirements under the Cryptowars OU AML-CFT Policy

Dated: 28 February 2019

All terms defined in this statement have the same meaning as terms defined in the Company AML-CFT Policy.

Personal data submitted to the Company under the Cryptowars OU AML-CFT Policy and / or Privacy Policy and its implementing procedures are processed under the supervision of the Compliance Officer in accordance with (EC) Regulation 45/2001 on the protection of individuals with regard to the processing of personal data by the Community Institutions and Bodies and on the free movement of such data ("**Data Protection Regulation**").

The data categories which may be collected by the Company in this context are mainly limited to identification data, data related to criminal activities and/or other miscellaneous business information, and will be collected exclusively for AML-CFT purposes. The processing of personal data for the purpose of AML-CFT is considered by the 4th AML Directive to be a matter of public interest and as such, the processing is lawful for the purposes of the Data Protection Regulation.

Data subjects include persons who directly or indirectly own counterparties (or potential counterparties) of the Company, as well as persons entrusted with control and management of such legal entities (e.g. beneficial owners, shareholders, chairpersons, chief executive officers, boards of directors,

management committees, supervisory boards, local authority councils or equivalent) or any natural persons-counterparties.

Personal data are collected from the data subject directly or via other publicly available sources ("**Open Sources**") such as newspapers, specialised databases operated by the private sector, specialised external service providers or websites, and all reasonable steps are taken to keep such data accurate and up to date. When data are requested for the purposes of AML-CFT, supply by the data subject is mandatory. Failure to provide the requested data may cause the data subject (and if applicable the counterparty linked to such data subject) to delay the operational processes of the Company or, as the case may be, to become ineligible to enter into a business relationship with the Company.

In accordance with Directive (EU) 2015/849, controls on data subjects include controls relating to due diligence requirements for counterparties (i.e. identity of the beneficial owner(s), ownership and control structure and purpose of the business relationship), as well as for the assessment relating to the Risk Based Approach (i.e. when applicable, qualification of the data subject as a "politically exposed person" or possible administrative and criminal records or proceedings in connection with criminal activities).

Such data subjects are entitled to access, rectify and, for duly justified reasons, to block and erase these data ("**Rights of the Data Subject**"), and may exercise their rights by contacting the Company by email contact@cryptowars-ou.com.

Restrictions to such Rights of the Data Subject may be imposed in accordance with the provisions of the Data Protection Regulation (Article 20 (1)) and more particularly for the prevention, investigation, detection or

prosecution of criminal activities. Such restrictions, if applicable, are dealt with by the GCCO on a case by case basis and will only be applicable for as long as necessary. The data subject, to the extent possible under the Data Protection Regulation, will be informed of the reason why his/her rights are restricted.

Where applicable, the recipients of the data so collected are limited to members of the Company's governing bodies, The Company internal services, EU institutions and bodies, as well as, on the basis of a case by case analysis, national authorities.