Internal AML (Anti Money Laundering) policies

Created on: 15.12.2023

Last updated on: 01.12.2024

Name of the company: CryptoEngine s.r.o.

ID number: 195 68 258

Legal address: Cimburkova 916/8, Žižkov, 130 00, Praha 3

Phone number: +44 7429548578

Email address: support@cryptos-engine.com

I. Definitions

I.1. Introduction

§ 1. Meaning of the document

(1) . For the purpose of preventing the risk related to legalization of funds from criminal activities and financing of terrorism, the company CryptoEngine s.r.o. applies the system of internal rules and measures.

(2) In a simplified way: legalization of revenues from criminal activities (in laic terms: „money laundering“) means an activity when a customer uses the services of the company CryptoEngine s.r.o. for covering illegal origin of his property or to make its back tracking difficult. Similar rules as those applied in CryptoEngine s.r.o. are binding for similar types of business in the Czech Republic as well as in other countries, because money laundering and terrorism financing is nearly always performed on international level.

(3) The company CryptoEngine s.r.o. regularly checks whether a customer is subject to international sanctions or not, respectively fulfilment of other procedures as described here below.

I.2. General Terms

§ 2. AML Act

(1) For the purposes of this document, the AML act means Act No. 253/2008 Coll. on some measures against legalization of revenues from criminal activities and terrorism financing, as amended.

§ 3. Legalization of revenues from criminal activities

(1) According to the AML act, legalization of revenues from criminal activities means activities that are to cover illegal origin of any economic benefit emerging from criminal activities with the aim of establishing an appearance that the property benefits were obtained in compliance with law; the above stated activities include for example:

(a) change or transfer of property while knowing that it originates from criminal activities for the purpose of its secrecy or hiding its origin or with the purpose of helping a person participating in such illegal activities to avoid legal consequences of his behaviour,

(b) keeping secret or hiding the real character, source, movement of property or its handling or change of rights related to property while knowing that it originates from criminal activities,

(c) obtaining, keeping, using the property or its handling while knowing that it originates from criminal activities, or

(d) criminal conspiracy of persons or any other form of unification with the purpose of activities specified in previous points.

§ 4. **Terrorism Financing**

(1) According to the AML act, terrorism financing includes:

(a) collection or provision of financial means or other property while knowing that it will be used – even partially – for committing a crime of terror, terrorist attack or a criminal act that should allow or assist in committing of such a criminal act or that should support a person or a group of persons preparing for committing such a criminal act, or

(b) behaviour leading to provision of remuneration or compensation of an offender of a criminal act of terror, terrorist attack or a criminal act that should allow or help in such a criminal act commitment, or persons close to the offender according to penal law, or collection of means for such a remuneration or compensation.

(1) Terrorism financing also means financing of mass destruction weapons distribution, i.e., collection or provision of financial means or any other property while knowing that it will be used – even partially – by the distributor of mass destruction weapons or for such weapons distribution in contradiction with international law requirements.

§ 5. **Obliged person**

(1) According to the AML Act, an obliged person means the company CryptoEngine s.r.o., with its registered seat in Cimburkova 916/8, Žižkov, 130 00 Praha, company ID: 195 68 258 for activities of providing of services related to a Virtual assets.

§ 6. **Customer**

(1) For the purposes of this document, a customer means any natural person or legal entity:

(a) which the company CryptoEngine s.r.o. established business relation with, or

(b) which started negotiations with CryptoEngine s.r.o. on business relation establishment (i.e., it showed interest in a business relation establishment), or

(c) which the company CryptoEngine s.r.o. already finished business relations with

(d) which becomes a virtual assets service user of the company CryptoEngine s.r.o.

(e) a person being an agent of services of another customer (e.g., it is entitled – on the basis of a power of attorney that the company must keep – to issue Virtual assets).

(2) It is not decisive whether it is a natural person or a legal entity carrying business or not. In case of a legal entity, it is supposed that one concrete natural person always acts on behalf of it (e.g., a member of the statutory authority, an employee, etc.).

§ 7. **Virtual Assets Service**

(1) For the purpose of this document, the virtual assets service means any handling of customer's property or provision of a service to a customer as mentioned in §4(8) of AML Act, and contain next services:

(a) Virtual assets wallet service:

(i) means a service in the framework of which keys are generated for customers or customers' encrypted keys are kept, which can be used for the purpose of keeping, storing and transferring virtual assets;

(b) Virtual assets exchange service

(i) means a service with the help of which a person exchanges virtual assets against a fiat currency or a fiat currency against virtual assets or virtual assets against another virtual assets;

(c) which is not contained in previous point, but it is directly connected with such an activity.

According to §4(9) of AML Act, virtual asset means an electronically storable or transferable unit that is:

capable of performing a payment, exchange or investment function, whether or not it has an issuer, unless it is

a security, an investment instrument, or a monetary instrument under the Act on Payments,

an entity referred to in Section 3(3)(c)(4) to (7) of the Act on Payments, or

a unit by which a payment is made pursuant to Section 3(3)(e) of the Act on Payments, or

a unit referred to in point (a)(ii) and which can ultimately be used to pay only for a narrowly defined range of goods or services which includes an electronically storable or transferable unit referred to in point (a).

(2) A virtual assets service also means any service provided without appropriate authorization, registration or license, even though it would be in contradiction with law.

§ 8. **Business relation**

(1) A business relation means a contractual relation by and between the customer and the company CryptoEngine s.r.o., by frame contract, based on which the customer is provided with virtual assets service. Customer's instruction

(1) Customer's instruction means any instruction issued by the customer or by a person authorized to act in this matter on customer's account, requiring for the company CryptoEngine s.r.o. to provide a virtual assets service or to make another act within the scope of the virtual assets service provided, e.g., a Virtual asset order. The instruction can be given electronically, by phone, personally or in any other way.

§ 9. **Staff setting**

(1) The obligations set out in this document apply to certain groups of employees - in particular the employees, the AML officer and the responsible person. They also apply to any person who may encounter a suspicious transaction (Chapters IV1. – IV.3) or perform any of the activities described in this document, as well as other persons. All of these people may potentially encounter trade suspected of attempting ML-FT.

(2) It is irrelevant whether it is a direct employee or a work performed on the basis of

another relationship or without any relationship (even as a free aid).

(3) Unless the company CryptoEngine s.r.o. is capable of ensuring the full and error-free performance of its obligations under this document and the Risk Assessment, it must reduce or even suspend virtual assets service activity until such a defect ceases, unless this is in conflict with the obligations under the legal regulations. This is the case, for example, in the event of a sudden failure of employees and replacement by temporary under-experienced assistance. Thus, ML-FT prevention activities must at all times be adequately staffed (both qualitatively and quantitatively). Responsibility for meeting this obligation lies with the responsible person.

(4) Furthermore, the responsible person is responsible for selecting the persons who are bound by this document. The responsible person shall always verify that the employee is able to fulfil the obligations laid down in this document before recruiting a new employee for the position concerned by this document or before transferring an existing employee to that position. These abilities / skills include:

(a) sufficient language and professional communication skills of the employee to handle communication with a typical customer

(b) sufficient employee awareness of the management and ownership structures of the customer, which is a legal entity, so that he / she can perform his / her duties perfectly for this type of customer

(c) sufficient computer skills and software that is used to enable the employee to make full use of these resources to fulfil their duties

(d) sufficient knowledge of all procedures set out in this document and the Employee Risk Assessment achieved by the training under Chapter V.3, which must be carried out no later than the first act mentioned in this document or the Risk Assessment.

§ 10. **Employee**

(1) For the purposes of this document, an employee means any person who is – in the course of fulfilment of its work tasks – in the name of the company CryptoEngine s.r.o.:

(a) authorized to negotiate regarding establishment of a business relation with a potential customer, or

(b) authorized to establish business relation with a customer, or

(c) negotiates with the customer on provision of virtual assets service or receives customer's instructions, or

(d) performs individual acts in provision of virtual assets service to a customer (even partial ones), or

(e) participates in any way in negotiations with a customer or in activities connected with provision of virtual assets service.

(2) An employee is a direct employee as well as a person performing such activities on the basis of another relation than the employment contract, including a negotiator.

(3) An employee is also a person who is not an employee at the present moment, but he/she

was authorised (even though just temporarily) to perform an activity, the realisation of which is set to an employee by this document.

§ 11. **Personal related to the Customer**

(1) For the purposes of this document, persons related to customers mean all and any of the following persons (natural persons or legal entities):

(a) statutory authority of the customer or a member of it

(b) beneficial owner or controlling person of the customer

(c) a person authorised to negotiate with the company CryptoEngine s.r.o. on behalf of the customer

(d) a person authorised by the customer to make business (to enter virtual asset orders).

§ 12. **AML officer**

(1) A person identified in this document as an AML officer means a person authorised to arrange compliance of business activities of the company CryptoEngine s.r.o. with legal regulations in the field of avoidance of proceeds from criminal activities, terrorism financing and application of international sanctions. It concerns mainly arrangement of compliance with the following regulations:

(a) AML Act

(b) Act No. 69/2006 Coll. on realisation of international sanctions

(c) Regulation No. 67/2018 Coll. on selected requirements towards system of internal regulations, procedures and control measures against legalization of proceeds from crime and financing of terrorism

(d) approved AML standards communicated by the Czech National Bank.

(2) Generally, it is supposed that the AML officer is a person directly governing an employee, authorized to establish business relation or negotiations in the matter of virtual assets service provision.

(3) The person appointed in the company CryptoEngine s.r.o. and authorised to execute the position of an AML officer is specified in Annex No. 2.

§ 13. **Responsible person**

(1) The responsible person of the obliged person means – for the purposes of this document – any member of the statutory authority of the obliged person.

§ 14. **Virtual assets service value**

(1) For the purposes of this document the virtual assets service value value means the general value of property being a subject of the virtual assets service.

§ 15. **Conversion of sums**

(1) For the purposes of this document, the sum which is set in Euro (EUR) means an equal

value in any currency converted based on the exchange rate announced by the Czech National Bank and valid for the day. If the exchange rate is not available that day yet, the exchange rate for the previous day applies. For current Exchange rates list of the Czech National Bank see https://www.cnb.cz/cs/financni-trhy/devizovy-trh/kurzy-devizoveho-trhu/kurzy-devizoveho-trhu/.

§ 16. **Binding force for third persons**

I.3. The procedures set forth in this document are also binding on persons acting in the performance of virtual assets service or in establishing business relationships on behalf of or for the account of the company CryptoEngine s.r.o. mainly for authorized representatives (hereinafter referred to as "representative"). Definition of a Politically Exposed Person

§ 17. **Politically Exposed Person – definition**

(1) According to the AML Act, a Politically Exposed Person („PEP") means a natural person who is or was in an important public function with regional, national or even higher importance, for example:

(a) chief representative of municipal authorities – major of a town or village, chief magistrate, region commissioner,

(b) chief representative of municipal authorities for a foreign country with federative organization – chief representative of country authorities, members of country government and parliament, etc.,

(c) head of state, prime minister, head of central authority of state administration (e.g., a minister) and his/her representative (deputy minister or secretary of state),

(d) member of the Parliament, member of the control authority of a political party,

(e) judge of the supreme court, constitution court or another supreme judicial authority,

(f) member of the banking council of a central bank,

(g) high officer of armed forces,

(h) member of the statutory authority or representative of a member (in case of a legal person to be a member of the statutory authority) of a business corporation controlled by state,

(i) ambassador or head of a diplomatic mission,

(j) or a natural person performing or having performed any similar function in another country, EU authority or in an international organization.

(2) A PEP is also considered to be a person close to the above stated person, mainly:

(a) relatives in direct line – parents, grandparents, etc., children, grandchildren, grand grandchildren, etc.

(b) siblings, wife, husband, partner

(c) relatives of wife, husband, partner – son in law, daughter in law, father in law,

mother in law

(d) a person who lives with him/her on permanent basis

(e) a person in family relation or similar relation to him/her, in case of any detriment suffered by one person to be justifiably considered as own detriment by the other person.

(3) A PEP is also considered to be a person from the "business surroundings", being

(a) a partner or beneficial owner of the same legal entity or trust fund as the person in the first paragraph,

(b) known by the obligated person to be in close business relation with the person as per the first paragraph; that means material inter-relations within the scope of business activities, when the success or detriment of one person could be justifiably considered to be own benefit or detriment by the other person,

(c) a beneficial owner of a legal entity or trust fund, which is the obligated person aware of the fact that they were developed in favor of the person specified in the first paragraph.

I.4. Definition of a Beneficial Owner

§ 18. **Beneficial owner of a legal entity**

(1) According to the AML Act, a beneficial owner means a natural person with factual or legal possibility of direct or indirect application of decisive influence in a legal entity, in a fiduciary fund or in any other legal organisation without legal personality. It is supposed that in case of fulfilment of conditions contained in previous sentence, the following person is a beneficial owner:

(a) In case of a business corporation (usually a limited liability company, a joint stock company, etc.), the beneficial owner is a natural person who:

(i) independently or together with persons acting in compliance manages more than 25 % of voting rights of the business corporation or has a share in basic capital above 25 %, or

(ii) independently or together with persons acting in compliance controls the person specified in previous point, or

(iii) is a recipient of at least 25 % of profits of the business corporation, or

(iv) is a member of the statutory authority, representative of a legal person in the authority or in the position similar to the position of a statutory authority member, if he is not a beneficial owner or if it is not possible to set him according to previous points.

(b) In case of an association, a non-profit organization, association of unit owners, church, religious association or any other legal entity according to the act dealing with position of churches and religious associations, the beneficial owner is a natural person:

(i) who manages more than 25 % of its voting rights, or

(ii) who is recipient of at least 25 % of the means distributed by it, or

(iii) who is a member of the statutory authority, representative of a legal person in the authority or in the position similar to the position of a statutory authority member, if he is not a beneficial owner or if it is not possible to set him according to previous points.

(c) In case of foundation, institution, endowment fund, trust fund or any other legal organization without legal personality a natural person or a beneficial owner of a legal entity, the beneficial owner is a person being in position of:

(i) a founder, and then

(ii) trustee, and then

(iii) beneficiary, and then

(iv) a person, in the interest of whom there was established or works the foundation, institution, endowment fund, trust fund or any other legal organization without legal personality, unless the fiduciary is appointed, and then

(v) persons entitled to perform supervision over the administration of the foundation, institution, endowment fund, trust fund or any other legal organization without legal personality.

I.5. Definition of a Controlling Person

§ 19. **Controlling person**

(1) According to Section 74 et conseq. Act No. 90/2012 Coll., on Commercial Companies and Cooperatives (Business Corporations Act), a controlling person means a natural person or legal entity who may directly or indirectly apply decisive influence in a business corporation. The indirect corporation means the influence executed through another person or other persons.

(2) The controlling person(s) is/are:

(a) always a person who is a majority owner, unless specified otherwise in the points below, and then

(b) always a person who is a controlling person of the concern (Section 79 Act No. 90/2012 Coll.), and then

(c) a person who may appoint or remove most of the persons being members of the statutory authorities of the business corporation or persons in similar position or members of a control authority of the business corporation, which he/she is a partner of, or he/she may push such an appointment, or

(d) the person who manages the share in voting rights representing at least 40 % of all the votes in the business corporation, unless the same or higher share is managed by another person or persons, acting in conformity, or

(e) persons acting in conformity, who jointly manage a share in voting rights representing at least 40 % of all the votes in the business corporation unless the

same or higher share is managed by another person or persons, acting in conformity, or

(f) a person who independently or together with other persons, acting in conformity, obtains a share in voting rights representing at least 30 % of all the votes in the business corporation and the share represented more than one half of voting rights of present persons during 3 recent consequent meetings of the supreme authority of the person.

II. Business relation establishment

II.1. Procedure during business relation establishment

§ 20. Procedure before business relation establishment

(1) The employee authorized to negotiate the business relation establishment with the customer:

(a) establishes a file (as a physical and virtual space) to keep all necessary information

(b) performs the initial identification of the customer

(c) performs the first check of the customer

(d) sets up the risk profile of the customer

(e) provides this information to the AML officer, who assesses customer's risk profile, in particular if it is of type B, C, D or even E.

(2) If it is proved that the customer is a PEP, the establishment of the business relation must be approved by the statutory authority of the company CryptoEngine s.r.o. (including the case when the customer is a legal entity, towards which obligations are applied as well as towards the PEP).

§ 21. Persons authorised to act on customer's behalf in the matter of business relation establishment

(1) Only a customer is entitled to act in the matter of a business relation establishment (i.e., the customer himself or his statutory authority or member of the statutory authority) or a person authorised by the customer to do so, customer's statutory representative or guardian.

(2) The authorization is proved by a power of attorney with legalised signature of the donor or by its legalised copy, containing identification data of the donor of power and the deputy and also the extent in which the deputy may act on behalf of the donor of the power. Original copies of the power of attorney or its legalised copy must be maintained.

(3) Statutory representation is proved by a deed indicating it – for example a certificate of birth of a child, represented by a parent. In case of a different statutory representative or guardian the right to represent a customer is proved by a court resolution. The company does not have to keep such documents – in case of a court resolution it must only record the file number.

§ 22. When the customer conceals acting on behalf of a third person

(1) In case of an employee to suspect for the customer not to act on his own behalf while negotiating on business relation establishment (i.e., that the purpose of the business relation is to provide services to a different person but the customer) or that he conceals that he acts on behalf of a third person, the employee refuses to establish the business

relation.

§ 23. **Simplified identification and check of the customer**

(1) The AML act sets a group of persons generally considered to be of a low risk due to supervision executed over them. In relation to such persons, the company CryptoEngine s.r.o. does not have to perform identification and checks using the procedures specified in Chapters II.2 and II.5.

(1) It concerns the following persons:

(a) Clients without the national risk factors, and

(b) Clients who are not showing the factors for EDD.

(2) National risk factors are as following

(a) Client risk factors:

(i) The business relationship is conducted under unusual circumstances,

(ii) the client is located in a geographic area of heightened risk as set out in point 3,

(iii) the legal entity or trust is a personal asset holding vehicle,

(iv) the client is a business corporation in which there may be authorized shareholders or partners or which issues shares in bearer form,

(v) the client uses cash extensively in its business activities,

(vi) the ownership structure of the client appears unusual or overly complex given the nature of its business,

(vii) the client is a beneficiary of a life insurance policy,

(viii) the client's business involves increased risk.

(b) Factors relating to products, services, transactions or distribution channels:

(i) use of private banking services,

(ii) the use of products or transactions that could facilitate anonymity,

(iii) business relationships or transactions without the personal presence of the customer or the natural person acting on his behalf and without certain security measures such as electronic signatures,

(iv) incoming payments from unknown or unrelated third parties; or

(v) new products and new business practices, including new distribution systems, and the use of new or emerging technologies for new or existing products.

(c) Geographic risk factors:

(i) Countries that have been identified by European Union authorities or international institutions dealing with measures against money laundering, terrorist financing or proliferation of weapons of mass destruction as lacking effective systems to combat money laundering and terrorist financing or engaging in illicit proliferation of weapons of mass destruction,

(ii) countries that have been identified by credible sources as having significant levels of corruption or other criminal activity,

(iii) countries subject to sanctions, embargoes or similar restrictive measures

imposed, for example, by the European Union or the United Nations; or

(iv) countries that provide funding or support for terrorist activities or in which identified terrorist organisations operate.

(3) It is necessary to write a record about the whole checking procedure, clearly indicating also who, when and on the basis of what performed the checks. The record is maintained and kept as a part of documentation related to the customer or to the business relation.

(4) Moreover, in the course of the business relation duration, the employee must periodically check whether there persist all the conditions for use of simplified verification and check of the customer. In case of any of the conditions to be broken, the customer is considered to be not allowed to be applied the simplified identification and check of customer and the procedures must be immediately performed before provision of any other services to the customer.

(5) Application of the procedure of simplified identification and control / check does not affect other obligations set in this document, mainly the obligation of assessment whether the service provided to the customer does not indicate features of a suspect trade according to Chapter IV.1 List of features and suspect trades and their assessment.

§ 24. **Enhanced identification and check of the customer**

(1) The AML act sets a group of factors that can mean a high risk of a client. In relation to such persons, the company CryptoEngine s.r.o. has to perform stronger identification and checks.

(6) Enhanced identification and check should happen in the following cases:

(a) During establishment and during the course of a business relationship with a person established in a high-risk third country (as per FATF and EU lists that can be found in the Annex 5),

(b) prior to the execution of a transaction relating to a high-risk third country (as per FATF and EU lists that can be found in the Annex 5),

(c) prior to or when entering into a business relationship with a politically exposed person.

(7) In enhanced identification and control, CryptoEngine s.r.o. shall, to the extent necessary to effectively manage the identified risk, go beyond the measures applied in client identification and control:

(a) obtain additional documents or information about:

(i) the beneficial owner,

(ii) the intended nature of the business relationship and

(iii) the source of the client's and beneficial owner's funds and other assets,

(b) verify the documents or information obtained from multiple credible sources,

(c) regularly and intensively monitor the business relationship and the transactions within the business relationship,

(d) obtain the consent of a member of its statutory body or the person authorised by it to manage the measures against money laundering and terrorist financing to

enter into or continue the business relationship,

(e) requires the first payment under the business relationship or a trade outside the business relationship to be made from an account held in the name of the client with a credit institution or a foreign credit institution which is subject to customer identification and control requirements at least equivalent to those of European Union law, or

(f) implement other measures taking into account the nature of the obliged person, its activities and its own risk assessment.

II.2. Initial Identification of a Customer

§ 25. **Initial identification procedure**

(1) The initial customer identification means the procedure, when the identity card (as specified here below) is used for check and recording of identification and other data of the customer (for specification see below).

(2) The initial identification of a customer is performed by one of the following ways:

(a) so called „face to face“ – a personal meeting with the customer or with a person representing him/her

(b) so called „remote“ – the customer sends the documents and the customer is checked by the first payment without necessity of a personal meeting with the customer.

(c) so called “technical” – the customer sends the documents and is checked by video verification.

(3) More, the initial identification of a customer always includes:

(a) establishment whether the customer is a PEP or not using the procedure according to Chapter II.3 and also

(b) establishment whether the Czech Republic applies international sanctions towards the customer according to Chapter II.4.

(4) In case of the customer’s initial identification to be performed just earlier, it is not necessary to repeat the process. **Identification of a natural person „face to face“**

(1) The „face to face“ identification is performed in physical presence of the customer or a person that represents the customer in the course of the business relation establishment (in case of a customer – a legal entity). On the basis of the identity card presented, the employee checks „face to face“ the compliance of customer’s appearance (or the person representing the customer) with the image in the identity card and more, he/she checks and records identification data from the identity card.

(2) More, in case of a legal entity to be the customer, it is also necessary to perform identification of the legal entity and to find out whether the „face to face“ identified natural person is entitled to act on behalf of the customer, respectively let him/her prove it by a power of attorney.

§ 26. **„Remote“ identification of a customer**

(1) An employee may perform identification even without physical presence of the customer who is a natural person or a natural person acting on behalf of the customer when establishing the business relation in case of the customer to be a legal entity (i.e.,, without presence of the person signing the contract). The procedure replaces identification of only the specific acting natural person and that is why it is necessary to make other steps in identification as usual (to establish PEP, to check sanctions, respectively to identify a legal entity, to check the right to act on behalf of the customer, etc.).

(1) If it is not possible to apply the complete procedure as specified here above or there are any doubts regarding real identity of the customer, the employee will not use the identification procedure and he will use some other method.

(2) The identified natural person will send (by e-mail or by post) to the company CryptoEngine s.r.o. a copy or a scan or photo of two different types of IDs (belonging to the identified person; he follows the list of accepted identity cards), while:

(a) if it is an ID of the identification card type, the customer sends copies, scans or photos of the front and rear side of the card;

(b) if it is an ID of a plate type (i.e.,, a „booklet“), the customer will send a copy, scan or a photo of the identification spread respectively also of the page with require data (for example address of stay inside of the residence permit);

(c) the customer may hide the data that are not require for the identification performance (e.g., wife’s name, etc.);

(d) both of the IDs must clearly indicate not only the identification data, but also the type and number of the identity card, country and possibly the authority issuing it and the term of validity;

(e) the copy and the scan may be black-and-white, but there must not emerge any doubts regarding genuineness of the identity cards or the person’s identity.

(3) More, the customer will send to the company CryptoEngine s.r.o. a proof, confirming existence of an account kept at the customer’s name in a bank or in a savings and loan co-operative or in a foreign bank or in a savings and loan co-operative operating in the territory of a member state of the European Economic Area, while:

(a) there is accepted a copy, scan, PDF file or a photograph containing the agreement on account keeping or customer’s account statement (that also means a common account of a married couple in case of the customer being a natural person)

(b) we do not accept images from Internet banking (so called „Print Screens“)

(c) the customer may hide the data that we do not require, but it must be always seen that the account is kept to customer’s name (i.e., in case of a legal person not to the name of the acting natural person, but beneficiary person in the name of the legal entity).

(4) More, there must be arranged that the first payment from the contract concluded will be

performed through the customer's account from the previous point:

(a) the first payment means a payment from the customer of the company CryptoEngine s.r.o.; in such a case the sum of the payment is not significant

(b) a payment to the account is not supposed to be a cash deposit to the account or payment by a postal order

(c) the employee is obliged to supervise for the first payment to be done in compliance with the condition; if it is not done so or if the payment is not successfully performed (e.g., it returns back), it is necessary to immediately terminate services provision and perform the identification in a different way.

(5) Except for the above stated conditions, the employee will assess – based on information available to CryptoEngine s.r.o. whether the customer, product or concrete business relation does not represent an elevated risk of abuse for legalization of proceeds from crimes or terrorism financing – otherwise he will not use this way of identification. He will also use risk assessment.

§ 27. **„Technical" identification of a customer**

(1) An employee may perform identification even without physical presence of the customer who is a natural person or a natural person acting on behalf of the customer when establishing the business relation in case of the customer to be a legal entity (i.e., without presence of the person signing the contract). The procedure replaces identification of only the specific acting natural person and that is why it is necessary to make other steps in identification as usual (to establish PEP, to check sanctions, respectively to identify a legal entity, to check the right to act on behalf of the customer, etc.).

(2) If it is not possible to apply the complete procedure as specified here above or there are any doubts regarding real identity of the customer, the employee will not use the identification procedure and he will use some other method.

(3) The identified natural person must use the following:

(a) a document according to the §33 is used for identification of a person and verification of data with the help of information technology means;

(b) an information technology tool with a working camera, microphone and necessary hardware and software for digital identification, as well as internet connection with adequate speed.

(2) Tools provided for in section 3 (b) must meet the technical specifications, standards and procedures for a high level of assurance laid down by a directly applicable regulation of the European Union governing minimum technical specifications, standards and procedures for levels of assurance for electronic identification devices and which is issued and used within a qualified system under the Electronic Identification Act.

(3) The client sends the KYC questionnaire and any other required papers to the CryptoEngine s.r.o..

(4) A third-party firm that provides video identification of clients can be used by the CryptoEngine s.r.o..

§ 28. **Accepted identity cards (certificates of identity)**

(1) The employee of CryptoEngine s.r.o. will accept for identification purposes mainly the following type of identity cards (certificates of identity):

(a) passport issued by any country

(b) identity card issued by a member state of the European Union and Iceland, Norway, Switzerland and Liechtenstein;

(c) driving license issued by a member state of the European Union and Iceland, Norway, Switzerland and Liechtenstein;

(d) residence permit proof issued by a member state of the European Union and Iceland, Norway, Switzerland and Liechtenstein.

(2) In addition to the types of identity cards listed here, an employee may also use another identity card issued by a public authority for identification, is valid at the moment of identification, includes images and at least some of the authorized holder's identification data.

§ 29. **Features of an identity card not suitable for identification**

(1) In case that the customer presents an identity card that shows any of the below stated features, the employee will refuse to make the identification on its basis and he will ask the customer for a different identity card:

(a) identity card not showing any marks of credibility (mainly in case of identity cards issued abroad)

(b) identity card, which the employee does not believe to be issued by a public administration authority (mainly in case of identity cards issued abroad)

(c) identity card after its validity term expiration (if specified)

(d) identity card which is excessively damaged (i.e., unreadable, overwritten, glued, without pages to be fixed, with missing pages or additionally glued)

(e) identity card without photograph or with a photograph that was adjusted or changed or that cannot be used for sufficient check of compliance of the photograph and the customer’s appearance

(f) identity card in which the appearance on the photograph does not correspond with the customer’s appearance

(g) identity card from which it is not possible to clearly set the authority and the state of the card issue

(h) identity card which is just a black-and-white or colour copy of the original identity card.

(2) In case of the employee not to be sure whether the identity card presented is valid or authentic, it is possible to check authenticity and protective elements against forgery using the on-line system „PRADO – public registry of valid identity cards and passports“. The system is available for free at http://prado.consilium.europa.eu/. More, the system provides references to national sites of document issuers, where it is possible to check whether the document has not been marked as stolen, missing or otherwise

excluded from the evidence.

§ 30. **Identification data of a natural person**

(1) On the basis of the identity card presented or delivered, the employee checks and records all of the below stated identification data:

(a) all the names and surnames of the customer (if there may appear any doubts – in case of foreigners – which is the name and which is the surname, the surname is written in capital letters)

(b) personal number; if it was not assigned, then the date of birth

(c) place of birth (including the country in case of the place of birth to be outside the Czech Republic)

(d) sex

(e) permanent or other residence

(f) citizenship

(g) type and number of identity card

(h) country, respectively authority issuing the identity card

(i) term of validity of the identity card.

§ 31. **Absence of identification data of a natural person**

(1) In practice there may occur a situation when some required data are not apparent from the identity card presented or sent, because they are not contained there. In such a situation the employee directly asks the identified person about the missing data and asks the person to communicate the data in written or oral form (unless it has already done so e.g., in an application for use of services) and to supported by a supporting document. In case of the person not to have the supporting document, there is no other possibility but to rely on the statement.

(2) Regarding the individual identification data established only on the basis of oral communication (and possibly verified from some supporting document only) it is necessary to note that they were verified on the basis of an identity card.

§ 32. **Initial identification of a natural person - entrepreneur**

(1) In case of the customer to conduct in the business relation as a natural person – entrepreneur, it is necessary – together with the above stated process of identification of a natural person – to record and check even all of the below stated data:

trade name, differing amendment or other marking

place of business

identification number of the person.

(2) The employee will verify the above stated data on the basis of a document presented by the customer regarding registration of the natural person in the evidence of natural persons – entrepreneurs or the employee may arrange such a document by himself. The document is most frequently an original or a legalised copy of an extract from the trade

registry or commercial registry or some similar evidence. The document must contain currently valid data.

(3) Even those identification data are recorded in the contractual documentation.

§ 33. **Procedure for the initial identification of a legal entity**

(1) In case of the customer to be a legal entity, the identification of each person acting on its behalf in business relation establishment must be performed, while the employee also identifies the legal person (i.e., the customer himself). More, it is also necessary to identify every person to act on behalf of the customer in the course of the business relation duration (so called agent / managing clerk).

(2) The employee proceeds as follows: the customer presents a proof on existence of a legal entity or the employee obtains it by himself. The document includes mainly:

- (a) original or certified copy of an extract from the trade register in case of legal entities registered in such a registry (mainly business corporations)
- (b) record from initial session of the municipal council in case of a municipality
- (c) extract from the registry of churches and religious organizations as issued by the Ministry of Culture of the Czech Republic
- (d) similar evidences in abroad
- (e) in case that there is not any such evidence in the country of headquarters of a foreign entity, then an officially legalised Articles of incorporation or some other document establishing the foreign entity and containing all the changes.

(3) The employee must always have available an original copy or certified copy of the proof of existence of the foreign entity.

(4) The document on existence of a legal entity must contain the currently valid data and the document may not be older than 6 months.

(5) In case of the customer to present a proof of existence of the legal entity issued in another country, it is necessary to pay extra attention to the fact whether it was issued by an entitled authority. It is not possible to consider a private subject to be an entitled authority – just the public administration authority of the foreign country.

§ 34. **Identification data of a legal entity**

(1) Identification data of a legal entity are all of the below stated data:

- (a) trade name or name, including the differing amendment or other marking
- (b) headquarters of the company (address and country)
- (c) identification number of the company or similar number assigned abroad
- (d) data of each natural person being a statutory authority or its member and allowing its clear identification; it concerns the following data as a minimum: all the names and surnames, dates of birth, permanent or other residence and citizenship.

(2) In case of another legal entity to be the statutory authority, its member or controlling person (see the definition in Chapter I.5), there will be recorded event its identification

data as specified above.

(3) In case of the customer to be a trust fund or some other legal organisation without legal personality, the identification data include its marking and identification data of its administrator, manager or person in similar position according to this chapter (these may be natural persons or legal entities).

(4) The document Risk Assessment may (so as to eliminate ML-FT risks) set even other identification data that must be obtained, recorded and possibly also checked. The treasurer must respect the extended list.

§ 35. **Initial identification of a customer on the basis of a power of attorney**

(1) In case of the customer (a natural person or a legal entity) to be represented on the basis of a power of attorney, the employee proceeds as follows:

(a) The attorney must present or deliver to the employee the power of attorney he acts upon and he must do so always before the business relation establishment. There is accepted only the original of the power of attorney or its legalised copy, not a standard scan or plain copy. The signature of the donor of powers need not be legalised, but it is recommended in consideration of higher business safety. The employee will keep the document on permanent basis.

(b) More, the employee performs identification of the attorney using the procedure as described in this chapter. The attorney and the donor of powers may be a natural person or a legal entity and identification may be performed „face to face“ or on „remote“ basis.

(c) More, the attorney will prove the identification data of the donor of powers. It is not necessary to identify the donor of powers „face to face“, his clear identification should emerge from the power of attorney.

(d) More, the employee states in the record of identification data of the attorney and the donor of powers that it is representation based on the power of attorney. Only then the identification is finished in full.

§ 36. **Initial identification of the represented customer**

(1) In case of the customer to be represented by a legal representative or a custodian, the employee proceeds as follows:

(a) The statutory representative must prove to the employee an appropriate legal relation on the basis of which he acts, always before the deal realization. The statutory representative is responsible for correct identification of the represented person. There is accepted only an original or certified copy of the document, not a standard scan or ordinary copy. The employee need not keep the document, it is sufficient to make a plain copy or – in case of a court resolution – he just records the file number.

(b) Then, the employee performs identification of the statutory representative. It may be a natural person or a legal entity and the identification may be performed „face to face“ or on „remote“ basis.

(c) Then, the statutory representative proves the identification data of the donor of powers. It is not necessary to identify the represented person „face to face“. A suitable form of proving is supposed to be e.g., the fact that identification data of the customer emerge from the document on representation or it is also possible to accept a written declaration of the statutory representative on such data.

(d) More, the employee states in the record with identification data of the statutory representative and the represented person that the customer is represented by a statutory representative. Only then the identification is finished in full.

§ 37. **Initial identification of the customer on the basis of the deed of identification**

(1) The initial identification of the customer (including a customer represented on the basis of the power of attorney or by a legal representative) may also be performed by the notary public or contact point of public administration (so called CZECH point) by writing so called deed on identification. The deed contains – in the form of non-detachable appendix – the documents on the basis of which the identification was performed and that clearly depict the customer.

(2) In such a case the employee checks the presented original of the identification deed and its appendices, then he checks completeness and readability of data. Then the employee performs the initial identification without physical presence of the customer in such a way as if the original document is presented. The original of the identification deed must be permanently kept. Only then, the initial customer's identification is performed in full.

II.3. Procedure for Establishment of a Politically Exposed Person

§ 38. **Establishment of a politically exposed person**

(1) In case of the customer to be a natural person, the fact whether it is a PEP or not is established only at the customer himself (i.e., the natural persons) and not at possible attorney, statutory representative or a guardian.

(2) If the customer is a legal entity, the fact whether it is a PEP or not is established for the following persons:

(a) any person acting on behalf of the customer in the matter of trade or business relationship (acting person) and then

(b) each statutory representative of the customer - including those who do not act in the matter of business (members of the statutory body and further, if the member of the statutory body of the customer is a legal entity and its representative)

(c) any beneficial owner of the customer.

(3) The PEP definition is contained in Chapter I.3.

(4) The customer that has PEP in its structure is subject of EDD.

§ 39. **Establishment procedure**

(1) PEP establishment is performed by declaration of the customer or a person acting on customer's behalf (statutory representative, proxy, attorney, legal representative, guardian, etc.) or by searching of the fact in the commercially distributed system for control and search for „risk" customers, based on information from public resources and provided in the form of a paid service by some specialised business subjects. It is also allowed for the employee to perform own investigations, e.g., while using open sources of information (Internet, etc.). The employee uses websites such as Facebook, LinkedIn, Instagram, Twitter, Forbes, Google, and others, as well as the national list of PEP functions, to collect information, analyze it, and make a decision. The employee always uses a combination of at least two methods of PEP research.

(2) In case of the customer to state to be a PEP or in case of the employee to know that from another source, the employee must establish (from the customer or in a different way) the following information:

   (a) identification of function respectively even other details about it

   (b) respectively description of relation to a person in leading position (if it is a person from his/her „family" or „business" environment, who is not in any leading position

   (c) respectively at least approximately date of finishing the function (if the function has been terminated).

II.4. Verification of International Sanctions

§ 40. **International Sanctions**

(1) International sanctions are a set of restrictive measures that the international communities (UN, EU) use as a tool to maintain or restore international peace and security, protect fundamental human rights, and fight terrorism. They are accepted by the competent authorities (UN Security Council, EU Council or European Commission) in the form of resolutions or decisions and regulations. In addition, the Czech Republic has a local individual list of 'intra-European terrorist groups'.

(2) The Czech Republic applies two types of sanctions:

   (a) sanctions, which it applies towards specific natural and legal persons, listed on the sanction lists (so called sanctioned persons)

   (b) sanctions, which it applies towards certain types of goods (so called sector sanctions).

(3) The following types of sanction regulations are legally binding (directly applicable) in the Czech Republic:

   (a) resolutions of the United Nations Security Council

   (b) resolutions of the EU Council or Commission (see https://sanctionsmap.eu)

   (c) resolution of the Czech Republic government (see http://www.amlsystems.cz/AML-dokumenty).

(4) Carrying out of international sanctions in the Czech Republic is partially regulated by

the AML Act and also by Act No. 69/2006 Coll., on Carrying out of International Sanctions.

(5) For more information on the application of international sanctions, please consult the Financial Analytical Office website at: http://www.financnianalytickyurad.cz/mezinarodni-sankce.html.

(6) The obligation to enforce international sanctions also applies to any other activities of CryptoEngine s.r.o., not only to those covered by this document.

§ 41. **Sanction lists**

(1) Two groups of sanction lists are legally binding for the Czech Republic:

(a) sanction regulations coming out from EU law accessible through EUR-Lex - access to European Union law at http://eur-lex.europa.eu.

(b) Government Decree No. 210/2008 Coll., On Implementation of Special Measures to Combat Terrorism, as amended, located eg at http://www.amlsystems.cz/AML-documents.

(2) The responsible person shall give employees access to these lists.

§ 42. **Screened persons**

(1) Prior to establishing each business relationship and then with the specified periodicity, the employee must verify whether the Czech Republic does not apply international sanctions against the customer or the persons associated with the customer. The verification periodicity of international sanctions should be set so that no service is ever provided to a customer that is subject to international sanctions - i.e., ideally prior to the provision of each virtual assets service or at least once a day, or possibly whenever the sanction lists are updated.

(2) If the customer is a natural person, the screening includes the customer himself / herself and, if applicable, also all the persons acting on behalf of the customer (proxy, legal representative, guardian).

(3) If the customer is a legal person, this screening includes the following persons (both natural and legal):

(a) the customer itself (a legal person in this case); and also

(b) all members of the statutory body (these may be natural or legal persons); and

(c) all controlling persons (see the definition in the Chapter I.5); and

(d) all persons that are the beneficial owners of the legal person (which is identified during the initial check of the customer, according to the Chapter II.5, these may be natural persons only); and

(e) possibly also an agent, proxy, legal representative, and guardian

(f) with all the persons the identity of which the company established within the scope of identification or control (mainly all the persons from the management and control structure of the customer).

(4) Furthermore, in the duration of the business relationship, it is always necessary to verify

the international sanctions against the counterparty of the customer's transaction (if the counterparty of the company is known), especially if CryptoEngine s.r.o. ensures the execution of payments, taking into account all the information accompanying these transactions (e.g., the requisites of SWIFT messages, SEPA payments and letters of credit etc.)

§ 43. **Search for a person in sanction lists**

(1) The employee looks for all the aforementioned persons (both natural and legal) up in the currently valid and available sanction lists.

(2) The employee has the obligation to create a record about the screening and the result, which corresponds to the requirement of reconstructability according to Chapter V.6, i.e., it contains at least the following information:

(a) date of verification and name of the person who performed the verification (if performed by a specific employee and not automated)

(b) a list of natural and legal persons that have been reviewed in the sanction lists

(c) information on the sanction lists under which the verification was carried out

(d) result of verification (negative or positive finding).

§ 44. **Sanction programs**

(1) In addition to verification of the persons' presence on the sanction lists, the AML officer and the employee must be familiar with the currently effective EU sanction programs. The Czech Republic, as a member country of the EU, does not only apply sanctions to certain persons only, but also to certain types of goods or services. It may happen (even during a business relationship) that the inspection of the customer indicates, based on the customer's communication or based on the submitted documents, that the customer uses the services of the company to trade or transfer (on the customer's own behalf or on another person's behalf) goods or services subject to international sanctions, e.g., the customer states that the payment relates to the movement of the goods and it turns out that it concerns so called dual-use goods that can also be used for military purposes and the expedition of such goods to some countries is forbidden).

The list of currently applicable sanctions is included in the "Consolidated list of sanctions" section: https://eeas.europa.eu/topics/sanctions-policy/8442/consolidated-list-of-sanctions_en.

§ 45. **Procedure in case of a person to which the international sanctions apply**

(1) In case the Czech Republic applies international sanctions against the customer or the persons associated with the customer or if the virtual assets service are in any way related to international sanctions, such negotiation regarding establishment of a business relationship or provision of virtual assets service is inevitably a suspicious transaction, and it is necessary to take all the steps listed in the Chapter IV.2.

(2) It is also necessary for the employee to ensure that the company proceeds in accordance with the specific sanction and in accordance with Act No. 69/2006 Coll., on Carrying

out of International Sanctions. For this purpose, contact both the AML officer and the statutory body of CryptoEngine s.r.o. and coordinate the next step with it.

II.5. Procedure during the Initial Customer Check

§ 46. **Initial customer check**

(1) The purpose of the initial customer check is to obtain information about the customer, necessary for the assessment, in particular:

(a) whether the customer does not represent any risk for CryptoEngine s.r.o. from the point of view of money laundering and financing of terrorism and in the preparation of its risk profile and whether fulfils the criteria of acceptability.

§ 47. **Procedure during the initial customer check**

(1) The initial customer check is performed by the employee, who will:

(a) find out and record what is the purpose of the intended business relationship (the purpose for which the customer will use the services); and

(b) find out, verify, and record the source of funds or other assets that will be the subject of the business relationship; and

(c) if the customer is a natural person, find out and record the list of all countries where the customer has a nationality and also a permanent or other stay; and

(d) if the customer is a legal entity, find out and record the list of all countries where the customer has its registered office, branches; and

(e) if the customer is a legal entity, find out and record information about the customer's ownership and management structure and further identify and record its beneficial owner so that it can be identified and always record the method and source of the findings of the beneficial owner, unless this is clear from the documents or records kept

(f) if the customer is a legal entity or a natural person doing business, it also detects and records a detailed description of all the customer's activities (not only those related to virtual assets service) - in order to fully understand his / her activities

(2) In addition, the employee will also find out whether the customer will act or act solely on his / her own behalf or whether he / she represents or will represent another person (especially the so-called Agency Agreement). If this is the case, the employee will perform a review to identify, understand and document the activities of the represented person, their ownership and management structure, and the beneficial owner as if they were the customer himself. In addition, the employee obtains representation documents.

§ 48. **Procedure for finding and verification of data**

(1) The employee finds out the data necessary for the check primarily by the means of his / her own investigation and from the available documents and also from the customer's statement.

(2) The purpose of the business relationship is often understood from the interview with the customer, or the customer declares it.

(3) The source of funds is often implied by the accounting documents entered into the collection of documents of the customer registered in the Commercial Register in the Czech Republic, by the published annual reports, and by the trade licenses that the customer has and through which the customer generates funds. The employee must always obtain sufficient information in order to verify the source of funds, In the case of one-time sums, the employee must find out more details (such as from whom the inheritance was inherited and in what amount, which property and for what amount was sold, the amount of the winnings and by which game operator it was paid). In the case of repeated income, its source, i.e., denomination of the business or the employer, and the approximate amount of such regular income.

(4) The list of all countries where the customer (natural person) has a nationality and a permanent or other residence, as well as the list of all countries where the customer (legal person) has its registered office, branches, organizational units, or premises, from the customer's website, or from the customer's statement.

(5) Information about the ownership and management structure and about the beneficial owner of the customer, legal persons will be found by the employee, in particular, by his / her own research of publicly available information (information contained in the extract from the Commercial Register, documents from the of the General Meetings based on the collection of documents kept by the registry court, etc.). If this information cannot be found, the employee will ask the customer for his statement and possibly a proof. The method of obtaining the ownership and management structure data and the beneficial owner will also be recorded by the employee (i.e., the source and the procedure by which the employee obtained the information). The management structure is determined by the employee to the second level: the first level is the management structure of the customer itself; the second level is the management structure of the controlling person (the parent company). Identification of the management structure does not apply to "sister" companies, unless it is necessary from the risk assessment point of view.

§ 49. **Verification of the data obtained during the check**

(1) If the employee assesses that there are doubts about the truthfulness or completeness of the data that the customer has stated during the check, he / she will ask the customer to prove the data obtained during the check by the relevant documents:

   (a) The source of funds and the purpose of the business relationship can usually be verified from accounting documents, statements from the person managing the customer's accounts, statements from the statutory body (in case of a legal person), confirmation issued by a bank or other third party, etc.

   (b) The beneficial owner of the legal person can be verified, in particular, from the last minutes of the general meeting. Only originals or certified copies of the submitted documents are accepted.

(2) Only originals or certified copies of the submitted documents are accepted. The

employees will make regular copies of these documents and he / she will keep them permanently.

II.6. Creation of Customer's Risk Profile

§ 50. **Creation of the Customer's risk profile**

(1) Prior to establishing the business relationship, the employee will create a risk profile of the customer. This is a characteristic of the particular customer.

(2) If a business relationship has been established in the past and it lasts (the customer uses other company services), the risk profile will be updated when establishing any further business relationship.

§ 51. **Risk profile**

(1) The customer's risk profile means the assessment of the customer that represents a potential risk that the services of CryptoEngine s.r.o. may be misused by the customer for the purpose of legalizing proceeds of crime or for financing of terrorism. As part of the risk profile, the customers are classified into the following groups according to the risk factor that has occurred in their case:

   (a) a customer with the type A risk profile – i.e., a customer without an identified risk factor

   (b) a customer with the type B risk profile – i.e., a customer with a low identified risk factor

   (c) a customer with the type C risk profile – i.e., a customer with an identified risk factor

   (d) a customer with the type D risk profile – i.e., a customer with a high identified risk factor

   (e) a customer with the type E risk profile C – i.e., an unacceptable customer.

(2) The risk profile is crucial in two respects:

   (a) influences the periodicity and intensity of the actions performed under this document

   (b) serves as an essential piece of information when assessing suspicious transactions.

§ 52. **Risk factors**

(1) The risk factor means the characteristic of the customer, the product provided to the customer, or the way it is provided to the customer, which increases the risk that the services of CryptoEngine s.r.o. may be misused by the customer for the purpose of legalizing proceeds of crime or for financing of terrorism. Based on the existence of specific factors, the client is given a risk profile of A,B,C,D, or E.

§ 53. **Risk profile - type A**

(1) A customer with a risk profile of type A does not represent for the company CryptoEngine s.r.o. no, or only very small (negligible) risk in terms of money laundering and terrorism financing, in case of:

(a) The jurisdiction of the client is low risk (as per Annex 5),

(b) The country of origin of the beneficial owner and representative is low risk (as per Annex 5),

(c) The monthly turnover of the client is less than 5 000 EUR,

(d) The client's business activity is low or medium risk (as per Annex 6).

(e) Where there are no known risk factors to assign a risk profile of type B, C, D or E.

§ 54. **Risk profile - type B, C, D**

(1) The customer is assigned the risk profile of the type B, C or D if there are no known risk factors which would assign the customer the risk profile of type E and at the same time, any of the risk factors listed in the Risk Assessment document as risk factors of the type B, C or D are found.

(2) A client with a Type B risk profile poses a low risk to the CryptoEngine s.r.o. in terms of money laundering and terrorist financing. To obtain this risk profile, the client must meet the following conditions:

(a) The client's jurisdiction is low risk (as defined in Annex 5),

(b) The customer's monthly turnover is less than 10 000 EUR,

(c) The client's business is low or medium risk (as set out in Annex 6),

(d) Where there are no known risk factors to assign a C or D risk profile.

(3) A client with a Type C risk profile poses a money laundering and terrorist financing risk to the Company. To obtain this risk profile, the client must meet the following conditions:

(a) The customer's monthly turnover is less than 15 000 EUR,

(b) There are no known risk factors to be assigned a Type D risk profile.

(4) A customer with a Type D risk profile poses a high risk to the Company in terms of money laundering and terrorist financing. He is always an EDD subject.

(5) A customer with the risk profile of the type B, C or D represents for CryptoEngine s.r.o. the potential risk from the point of view of legalization of proceeds from crime and financing of terrorism and therefore all employees, including the AML officer, must:

pay high attention when assessing any suspicious behaviour of this customer according to Chapter IV.1,

to place increased demands on the accuracy of information provided by the customer within the framework of the initial or continuous check, or possibly to substantiate the declared information by means of a specific document;

to carry out a continuous check of the customer at least once in a certain time period specified in the Risk Assessment

check for each transaction that exceeds the amount specified in the Risk Assessment

carry out a continuous check of a certain number of transactions selected at random over a certain amount of time; the time interval, the number of transactions selected at random and the minimum amount are set by the Risk Assessment

obtain AML, KYC and other similar regulations from the Customer if the Customer's activity requires them to be processed and to assess whether they are sufficient.

§ 55. **Risk profile - type E**

(1) The customer is assigned the risk profile of the E type in the event that any of the risk factors listed in the Risk Assessment document is found with the customer, making the customer unacceptable.

(2) A customer with the risk profile of the type E represents for CryptoEngine s.r.o. extremely high risk from the point of view of the legalization of proceeds from crime and the financing of terrorism. In the event that the customer is assigned the type E risk profile, the business relationship will not be established with the customer, or the business relationship with the customer will be terminated.

II.7. Establishing a Business Relation

§ 56. **Establishing a business relationship**

(1) A business relationship can only be established with the customer if all three of the following conditions are met:

(a) the operations preceding the establishment of the business relationship under the Chapter II.1 have been fully performed; and

(b) the AML officer has approved the establishment of the business relationship if required by it in the Risk Assessment; and

(c) if the customer is a PEP, a consent to the establishment of the business relationship must be issued by the statutory body of CryptoEngine s.r.o. or a person appointed by it; there must be a record written about the consent issued; and

(d) none of the facts mentioned in the Chapter II.8 has occurred.

(2) The business relationship is established by signing the documents on the basis of which the business relationship is established, or when the services are made available for the customer, whichever comes first.

§ 57. **Instructing the customer about the need to report changes of the data**

(1) In addition, when establishing the business relationship, the customer will be obliged to notify all changes to the data the customer has provided during the establishment of the business relationship. These include in particular:

(a) the data provided at initial customer identification

(b) changes in the fact that the customer or the customer's beneficial owner is or is

not a PEP

(c) changes in the list of people who are considered to be the beneficial owner of the customer

(d) the data provided during the customer control, etc.

(2) The Customer must make the notification of the change of the data or of its completion without any delay, but not later than prior to being provided with the next virtual assets service. The customer will also be informed that failure to notify a change may be a reason for termination of the business relationship.

II.8. Ban to Enter a Business Relationship

§ 58. **Ban to establish a business relationship**

(1) The company CryptoEngine s.r.o. rejects to enter into a business relationship with a customer if:

(a) the customer does not provide us with required cooperation within the performance of the verification and initial identification – i.e., does not provide with the information and data required or does not support these with relevant documents (if required), or

(b) if there have emerged any doubts related to the correctness and completeness of the information provided to us by a customer within the initial identification or initial verification, or

(c) if there was established any suspicion that a customer has provided us with untrue, distorted or incomplete information or in the event when a customer submitted false, altered or untrustworthy documents

(d) due to any other reason is not possible to perform the initial identification or initial verification of a customer, or

(e) it is clear at the customer that the intended business relationship is intended to provide services to a person other than himself (i.e., he acts solely as an intermediary or identity provider) and the customer does not present a power of attorney; or

(f) the customer is subject to EDD and the statutory body CryptoEngine s.r.o. or the person authorized by it has not consented to the establishment of a business relationship

(g) the customer is PEP and CryptoEngine s.r.o. does not know the origin of the property that the customer will use for each service

(h) the customer has been, pursuant to its risk rate, ranked within a group of customers with which the company shall not establish any business relationship.

(2) In the event when the establishment of business relationship is refused, a closer attention of employees shall be focused on the facts, whether the behaviour of a customer, due to which such a situation emerged, is typical of suspicious business characteristics, pursuant to the Chapter IV.1.

III.Business Relation with client

III.1. Obligations in the Course of the Business Relation Duration

§ 59. **List of obligations**

(1) Within the duration of the business relationship entered into with a customer, the company CryptoEngine s.r.o. is obliged to perform, in particular, the following:

(a) if the customer appoints a new joint holder, i.e., a person who will newly execute trades on behalf of the customer (e.g., enter virtual asset orders for transfers), he / she will also identify him / her; the joint holder may act on behalf of the customer only after the company receives the power of attorney to represent the customer in the execution of transactions or has the right to represent the customer as a statutory body or its member or is the legal representative of the customer

(b) check the validity and completeness of the data obtained in the framework of the customer's identification (when establishing a business relationship, also continuous, including the status of PEP) and record their changes and additions

(c) continuously verify whether the Czech Republic is applying international sanctions against the customer or a related person, including those who are a counterparty to the trade, if the company becomes aware of them

(d) carry out a continuous check of the customer

(e) continuously update the customer's risk profile (categorize the customer according to risk factors) - if there is a change, the AML officer must be informed and the customer must assess whether the business relationship is terminated; The AML officer shall take into account, in particular, the obligations under Chapter III.2 and the customer's risk profile, in particular if it is of type B, C, D or even E; this must be done by the AML officer no later than before the next transaction (especially before the next virtual assets service is provided)

(f) to continually assess whether the behaviour of the customer or of the persons acting on his / her behalf shows any signs of suspicious trade or whether the services provided to the customer indicate this

(g) refuse to provide a service in certain situations and possibly terminate the business relationship

(h) if the customer is a PEP, all substantial changes to the framework virtual assets service contract that have been triggered by the customer's request (egg request to increase limits, new joint holder, etc.) must be approved by the statutory body of CryptoEngine s.r.o. and the approval to create an alert; The risk assessment may be determined by other groups of risk customers for whom the AML officer approves these significant changes in the business relationship.

(2) The Risk Assessment document may determine, for each customer risk group, the

frequency or circumstances that trigger the need to meet individual obligations during the business relationship, as well as the intensity with which those ongoing obligations need to be met. It is the fulfilment of a risk-oriented approach to monitoring and managing the business relationship.

§ 60. Check of information in case of doubts

(1) Whenever doubts arise as to the information or data (obtained as part of customer identification or control), the employee shall verify this information without undue delay. This is done by verifying the information either from publicly available sources or by contacting the customer to provide appropriate explanations and possibly documents.

§ 61. Updates of customer's risk profile

(1) Throughout the business relationship, all employees continually update the customer's risk profile. This means that if there is a circumstance that causes a worsening of the customer's risk profile, there will be a change, or vice versa - if circumstances worsening the customer's risk profile disappear, it will change in the opposite direction, if permissible. The rules and factors set out in Chapter II.6 and in the Risk Assessment will be used to update the risk profile.

(2) The frequency of updating the customer's risk profile is determined by the Risk Assessment.

(3) The employee always keeps a record of changes in the customer's risk profile, which enables the situation to be reconstructed - i.e., it includes information on the reason for the change, the method of finding, source and eventual verification of the circumstances, date and information on the currently valid risk profile data. The history of changes in the risk profile must show all its changes, i.e., previous information is not deleted, only new one is added.

III.2. Data Updates

§ 62. Customer's data changes and information added

(1) In the course of the business relation duration, the employee must check the validity and completeness of the customer's data, which is stored in the customer's file. In particular the following ones:

(a) Validity and completeness of the identification data, including changes in the personal composition of Customer's statutory body – a legal person

(b) Information whether any facts have not been changed, whether any of persons is a PEP person or not

(c) Information whether the Czech Republic has not applied international sanctions towards a customer

(d) Validity and completeness of the data sourced within the verification of a customer, in particular the information whether the intended purpose of business

relationship still persists, whether the source of financial funds used by a customer is still up to date, whether in case of that customer – a legal person – has not been changed the ownership and management structure or beneficial owners, a list of all countries in which the company has its registered office, branches, business divisions or establishments, and if that customer is a natural person, then information on a list of countries in which that customer is having a citizenship, as well as permanent or other kind of residence

(e) Reasoning why the simplified identification and verification was applied to a customer (where applicable).

(2) In the event, when customer's identity card validity has expired, i.e., the identity card, on the basis of which a customer, a natural person, was verified, there is no need to have the data on new identity card. However, if customer's identification data has been changed, there is necessary to verify the new data from his/her identity card and record even the information on his/her identity card in which the new data is stated. The data on original identity card shall not be deleted.

(3) Every change or data added shall be recorded by the employee. The record shall be entered by the employee who found out such a data change or who found out the information which shall be necessarily added, or who was given such information on change from a customer.

(4) A change or completion shall be performed as follows: the originally recorded information shall be supplemented with the new one. It is necessary to proceed in such a way which allows us to distinguish whether this is the case of a data change or just a data completion (i.e., whether the originally recorded data stays valid or not). Moreover, it shall be apparent who from our employees and when (date) has entered the data change or data completion, or the source of data verification shall be identified.

(5) If this is the case of data change, the originally recorded data cannot be deleted, in spite of the fact such data is not valid anymore; it is necessary to keep it stored as the data which was valid in the past (including the documents which supported the data – if required).

(6) Furthermore, if it is required during the procedure of changed or supplemented data sourcing to support such a new information with any document or verification upon any kind of declaration, power of attorney or other document, then it is necessary to submit such a document or perform its verification within its full scope.

III.3. Verification of a Customer in the Course of the Business Relation Duration

§ 63. **Continuous verification of a customer**

(1) The continuous verification of a customer is aimed to trace the services provided to a customer during the business relationship in order to be able to verify whether the transactions and acts were in compliance with the facts known to the company CryptoEngine s.r.o. about the customer.

(a) the services used are consistent with the client's financial circumstances and economic activity

(b) the services used are consistent with the originally intended purpose of the business relationship (product used)

(c) the services are not used by a person other than the client, i.e. in particular whether they serve as an instrument for the transfer or storage of funds to a person other than the client.

(1) This monitoring is essential to assess whether the services provided to the client do not exhibit the characteristics of suspicious business under Chapter IV.1. In particular, the automated system assesses the following information:

(a) the volumes of funds that the client transfers using the services of the company or accumulates with the company

(b) the type of payments made, destinations, recipients, volumes, etc.

(2) Customer's risk profile shall be understood also as the key factor during the procedure of continuous verification. If a customer was ranked with a type B, C, D risk profile, then this kind of assessment increases:

(a) The frequency of continuous verification performance, and also

(b) The intensity under which is the continuous verification performed, and also

(c) The requirement for information reliability, i.e. the information which is submitted by a customer – his/her statements or declaration are not sufficient any more, but other documents shall be required having in view that the documents of highest possible reliability are these which were verified by a third party, nor just by a customer, ideally such a person shall be acting independently and shall be a recognised authority (state administration bodies, an auditor, etc.).

(3) Special attention shall be focused on a PEP person active beyond the EU or on a PEP person active within the territory of EU, i.e. the persons in case of which was found out a risk factor. Such persons are considered risky, having in view the fact they may dispose of property of corruption origins or other similar behaviour, or from subsidy frauds. As for this person, the alert (generated by automatic data-processing system) limits shall be for the purposes of its generation pre-set (at the level of regularly received income of a person in certain position performed currently within the PEP person, including some reserve from gathered savings).

§ 64. **Records of continuous and business control**

(1) A record must be made and kept of each continuous check, from which all events can be reconstructed (i.e., in particular that a periodic scan has been carried out, that a warning has been issued, who handled it and how, data from it, any other documents obtained, etc.).

§ 65. **Customer's obligation to provide us with cooperation**

(1) A customer is obliged to undergo the continuous verification, i.e., submit all the required information and present the documents to support declared facts (if required

by the employee). In the event when a customer did not provide us with sufficient cooperation in the course of continuous verification, then he/she cannot be provided with the service (i.e., financial funds kept with the company CryptoEngine s.r.o. will not be transferred to any payee unless a customer undergoes the verification procedure), the business relationship will be terminated (according to Chapter III.2), and simultaneously this is a feature of suspicious business according to Chapter IV.1, and it is necessary to follow the procedure shown in Chapter IV.2, and this kind of suspicious business shall be reported.

III.4. Ban to Provide Service and the Obligation to Terminate a Business Relation

§ 66. **Ban to provide service**

(1) A customer will not be provided with the service and business relationship with a customer will be terminated if any of the following facts would emerge:

(a) A customer rejects to undergo the identification, if its performance becomes obligatory (e.g., if identification data has been changes or should be completed)

(b) A customer rejects to submit a power of attorney if there has emerged a reason to submit this kind of document (e.g., when the executive ceases to hold its office, but a customer – a legal person – still requires he/she should act on customer's behalf, or in the event when the employee suspects a customer does not act in its own name, i.e., the funds that are subject to respective service does not belong to a customer, but is owned by any other person, and a customer acts in this case only as intermediary or identity provider)

(c) A customer rejects the cooperation in the course of verification, i.e., rejects to submit or complete the data for which he/she was asked by the company CryptoEngine s.r.o. during the initial or continuous verification, or eventually rejects to submit relevant documents when he/she was asked for them

(d) A customer who was not a PEP person has become in the course of business relationship duration a PEP that is active beyond the EU or a PEP active within the territory of EU, and in case of such person was identified a risk factor, and the company CryptoEngine s.r.o. is not aware of the origin of customer's financial funds or the statutory body of CryptoEngine s.r.o. has not granted its consent with the continuation of such business relationship, or such a consent has not been granted by a person authorised by the statutory body

(e) A person performing the identification or verification has doubts whether the information stated by a customer is true (and such doubts were not refuted by a customer)

(f) Risk assessment of a customer became worse and a customer moved to the group of E risk profile, i.e., to the group of customers that are not allowed to enter into a business relationship with the company, i.e., the existing business relationship is terminated

(g) Identification of a customer was performed via a distance identification, and the first payment resulting from the business relationship was not successfully made to the account stated on a customer's name – in this event the business relationship is not terminated, however, the customer is not provided with any further services up to the moment when a „face to face“ identification is made

(h) during risk assessment it was discovered that sanctions were imposed against customer and there is no permission from FAÚ and statutory authority

(2) When any of the stated situations arises, the employee shall report it to an AML officer without delay, and also is obliged to ensure that a customer is not provided with the required service by the company CryptoEngine s.r.o. An AML officer shall ensure the business relationship with a customer will be terminated (de facto and de jure). Furthermore, the employee shall pay increased attention when assessing whether the behaviour of a customer does not show some features of suspicious business, pursuant to Chapter IV.1 hereof.

IV. Suspicious Business

IV.1. List of Suspicious Business Features and Their Assessment

§ 67. **Suspicious business in general**

(1) A suspicious business shall be understood as the service provided in circumstances which give rise to a suspicion to perform a legalization of proceeds of crime, or a suspicion that the assets which are subject to certain service are determined for the terrorism financing purposes.

(2) A suspicious business may be also understood as the customer's behaviour which is not directly intended to be provided with a service, but is giving rise to a substantiated suspicion that a customer is aimed to act illegally, i.e., within the scope of mentioned unfair activity. A suspicious business or transaction may be also a service which has not been provided by the employee (in circumstances stated in Chapter II.5), or if the case was recognised only as a customer's attempt to establish the business relationship.

§ 68. **Features and circumstances of a suspicious business**

(1) Features and circumstances which might indicate the case of a suspicious business:

(a) the payment was credited from other account then usually in particular customer's case, or the payments are credited from the account or even various accounts which are not owned by the customer, and there is no apparent connection between the owner of that account and the customer

(b) the customer is from the country in which the company usually does not offer its services – for the list of the countries see Annex No. 5

(c) the customer is using services (Enters the virtual asset orders, etc.) from more countries

(d) the customer uses funds to purchase such type goods, and eventually also such volume of goods which does not correspond to usual behavior of a customer or to its financial means

(e) the customer asks for the virtual assets service and makes or requests the payment in cash and vice versa

(f) the customer resells goods or services purchased for funds for no apparent economic reason

(g) the customer uses funds as a deposit instrument (stores and holds assets there for no apparent reason) and then requests a redemption

(h) the customer requests external transfer to an account that does not belong to him / her - belonging to a person with no apparent relationship with the customer

(i) the customer's business or place where funds can be used is fictitious or difficult to verify or otherwise non-standard

(j) a "sleeping" customer - the customer with whom the business relationship was established does not use the services and the view will change without any

justification, or the frequency and volume of the services used will suddenly cease again

(k) the purpose for which the customer uses the services is contrary to the declared purpose

(l) the volume of services used by the customer does not correspond to the customer's property and economic conditions (and it is contrary to what the company CryptoEngine s.r.o. knows about the customer)

(m) the virtual assets service of the company are probably used by a person other than the customer himself

(n) the customer makes multiple transfers and the volume of these transfers is just below 1 000 EUR or below15 000 EUR as they consider that they are not subject to monitoring

(o) the customer offers the employee money or other remuneration for performing a non-standard service or potentially suspicious transaction or for establishing a business relationship where the employee does not require all the particulars (identification, control, etc.)

(p) the customer mentions that the funds which are the subject of the service are of illegal origin or intended to finance terrorism

(q) the customer unreasonably assures the employee that the funds which are the subject of the service have been acquired in accordance with the law or that the money is not of illegal origin or that it is not intended to finance terrorism

(r) the customer shows an unusual interest in the policies, procedures and measures which the company CryptoEngine s.r.o. follows within the System of Internal Rules and Risk Assessment

(s) the customer has extensive knowledge of legalization of proceeds of crime or terrorism financing

(t) the customer is unreasonably nervous during the negotiations and gives the impression that he has been instructed by another person

(u) the customer is unusually trying to converse with an employee on the topic of money laundering or terrorism financing

(v) the customer deliberately seeks to establish a friendly relationship with the employee

(w) the person acting on behalf of the customer is accompanied by another person and is monitored

(x) the customer uses the services of multiple companies for no apparent reason

(y) the customer uses services that are normally provided by banks and is willing to use the services of the company without justification even if it is significantly more expensive for him

(z) the customer uses the services of the company without any links to the Czech Republic and without it, i.e., it tries to introduce another country into the transfers in order to make it difficult to trace the financial flows

(aa) the customer carries out activities that may help to conceal his identity or to conceal the identity of his beneficial owner

(bb) the customer submits an identity document that shows any of the features listed in Chapter II.2 under points Features of an ID Unsuitable for Identification

(cc) the customer presents only copies of identity cards or unverified copies of other documents

(dd) the customer requests identification on the basis of a document other than that required by the employee

(ee) there are reasons to refuse to provide a service or the obligation to terminate a business relationship under Chapter III.4

(ff) the customer tries to persuade the employee not to request some data that is necessary for identification or control purposes

(gg) the customer asks questions that lead to suspicion that he is trying to avoid identification and control

(hh) the customer provides confusing, deceptive or contradictory information

(ii) the customer knows little details about the purpose of the business relationship or the origin of the funds

(jj) the customer over-explains the origin of the funds or the purpose of the transaction

(kk) the customer carries out high-volume transactions using funds obviously used for business purposes, but the customer does not wish to associate them with the business (i.e., to tell the business person which funds belong to and for whom he is acting)

(ll) the counterparty of the service is a person whose activity is linked to a country where measures against money laundering or terrorism financing are applied insufficiently or not at all; a list of these countries is given in Annex 5

(mm) the employee knows from a reliable source (e.g., television, newspapers, etc.) that the customer or business counterparty is involved in illegal activities or has a criminal history

(nn) in the course of one day or in the days immediately following, the customer will carry out noticeably more deals than is usual for his activity

(oo) the customer indicates the purpose of the transaction, which is hardly compatible with his activity

(pp) the customer is a non-profit or charitable organization and the purpose of the business that he or she communicates is contrary to the activity that he or she states or publicly declares.

(2) The present list is only a non-exhaustive. Practical experience can include also other circumstances not stated here, these indicate that the service might be used to legalize the proceeds of crime and financing terrorism, therefore this could the case of a suspicious business.

(3) On the other hand, if the business shows any of the stated features, this is not necessarily

the case of a suspicious business.

§ 69. **Assessment of the features and circumstances**

(1) Assessment of these circumstances shall be performed by the employee, as follows:

(a) Individually for each the situation and business relationship,

(b) Prior and in the course of business relationship duration, eventually also after its termination

(c) Having in view all the other services that are provided to a customer by the company or that are or were subject to negotiations with a customer

(d) Considering all the customer-related facts that are known to the company CryptoEngine s.r.o.

(e) Having in view the customer's risk rate and risk profile.

(2) In the course of assessment are taken into account not only the circumstances, in which the service is performed, but also the information submitted by a customer during the initial or continuous verification (check). An AML officer and the employee may take into consideration also other relevant circumstances and facts that are not stated herein directly.

(3) The employee cannot express towards a customer that the employee is performing the assessment whether this is or is not a suspicious business.

§ 70. **Point of view of Customer's risk profile**

(1) When identifying and evaluating a suspicious transaction, the employee also takes into account the customer's risk profile, which has been assigned or updated according to Chapter II.6.

(2) For customers with a risk profile of type B, great care must be taken when assessing the potential suspicion of a transaction. Customers with an assigned risk profile of type E will not be provided with services and the business relationship with them will be terminated.

(3) Furthermore, it is necessary to impose higher demands on customers with a risk profile of type B to prove the claimed facts with credible documents.

§ 71. **Business that is always suspicious**

(1) The always suspicious business is that one which shows at least one of the following features:

(a) A customer refuses to undergo the verification or does not support us with sufficient cooperation during the verification and check (typical customer reaction: I am not going to discuss something like this with you… „ or „This is not your business…" or a customer suddenly stops the dialog).

(b) A customer refuses to submit identification data of a person, on behalf of which he/she is acting.

(c) A customer of its beneficial owner (in case of a legal person) is a person, towards

which the Czech Republic applies the international sanctions in accordance with applicable law on international sanctions application.

(d) Subject matter of the business is or should be the goods or services towards which the Czech Republic applies the sanctions in accordance with applicable law on international sanctions application

§ 72. **Procedure in case of suspicious business**

(1) In the event when the employee has assessed the customer's behaviour shows the features of suspicious business, the steps shall be as follows:

(a) If the initial identification of a customer has not been performed yet, the employee shall follow the steps stated in Chapter III.4

(b) If the initial verification (check) of a customer has not been performed yet, the employee shall follow the steps stated in Chapter IV.1

(c) If the continuous verification (check) of a customer has not been performed yet, the employee shall follow the steps stated in Chapter III.3

(d) follow the procedure shown in Chapter IV.2.

(2) In practice, there could occur even the situation when the employee has assessed that this is the case of a suspicious business and the identification or verification of a customer could not be successfully finished or was not performed at all (as the customer e.g., refuses to cooperate). Also, in this case, it is necessary to report a suspicious business following Chapter IV.2 - if there exist at least some information on a customer.

IV.2. Suspicious Business Reporting

§ 73. **Procedure in case of suspicious business reporting**

(1) If the case has been assessed by the employee as a suspicious business, immediately after the performance the employee contacts an AML officer (see the Annex 2), and

(a) Shall report he/she found out a suspicious business,

(b) Shall submit all the data and all the printed documents related to a suspicious business (in particular the data and documents obtained during the customer's identification and verification procedure),

(c) Shall state the reasons why the business was assessed as suspicious one,

(d) Shall inform an AML officer on other facts which the employee considers essential in relation to this business,

(e) Next, the employee shall cooperate with an AML officer upon officer's requirements

§ 74. **Activity of an AML officer**

(1) An AML officer shall start to be focused immediately on the case when it was reported by the employee, and shall perform all the steps in order to assess the business. In the event when an AML officer has assessed the business as suspicious one, an officer shall

decide whether there have arisen the grounds for the postponement of customer's order, in accordance with Chapter IV.3. Next, the suspicious business shall be reported to FAU without undue delay, however, not later than within 5 days from the moment when the suspicious business was found out.

§ 75. **Notification of a suspicious business**

(1) A notification on a suspicious business to the FAU may be filed by one of the following ways:

(a) On the basis of the information obtained, an AML officer shall draw up a notification on suspicious business. A form titled „OPO“ should be filled in for these purposes, i.e., to announce a suspicious business, the form is stated in the Annex 4 hereto. To notify this kind of business also other form may be used, but all the required legal particulars shall be included (for more information see the Annex 4). This document should include the copies of all the documents there are available in relation to the suspicious business. Such well documented business is to be announced by an AML officer in writing, using a registered letter with a form and shall be sent to the address: Finanční analytický úřad, Poštovní přihrádka 675, Jindřišská 14, 111 21 Praha 1.

(b) The notification on a suspicious business may be submitted also orally, which shall be recorded in the protocol in the place determined after previous agreement speaking to a phone number operator: +420 257 044 501.

(2) An AML officer shall complete the notification (if available):

(a) Further information found out about a customer,

(b) Information whether a customer was in the past provided also with other services and the details should be added,

(c) Visual, audio or audio-visual record of a customer, if any of these exists.

(3) If any such document exists, an AML officer shall keep a receipt on filed notification on a suspicious business (advice of delivery of a registered letter, etc.).

§ 76. **Evidence of filed notifications**

(1) In addition, the AML officer keeps a record of all reports of suspicious transactions submitted for CryptoEngine s.r.o. filed, it is necessary to respect the obligation of confidentiality according to Chapter V.2. This documentation also includes copies of all reports of suspicious transactions submitted.

§ 77. **Obligation to provide the AML officer with co- operation**

(1) In the event when an AML officer requires so, all the employees are obliged to provide him/her with a cooperation in the course of fulfilment of the obligations resulting from the present document, as well as from the law. The employees and an AML officer shall act in the matter of filed notification on a suspicious business without unreasonable delays.

IV.3. Postponement of the Customer’s Order Fulfilment

§ 78. **Decision making on postponed of the customer’s order fulfilment**

(1) AML officer shall, without delay, when he/she receives a notification on a suspicious business from the employee, and when he makes its own decision whether this is the case of suspicious business or not, decide, whether the customer's order should be postponed or not, i.e., regarding that customer who has been stated in respective notification. In particular, this shall be understood as a blocking of Virtual asset order performance.

(2) AML officer is obliged to make a decision on the postponement of the customer's virtual asset order if, due to its immediate performance could result in a frustration or significant complications in the field of securing of the proceeds of crime or funds designated for the terrorism financing.

(3) An AML officer shall decide whether the customer's order shall be fulfilled in such a case when both the following conditions are met:

(a) There is no threat that the immediate fulfilment of the customer's order could result in a frustration or significant complication in the field of securing of the proceeds of crime or funds designated for the terrorism financing

(b) An AML officer is not aware of the fact that such a postponement could result in a frustration or otherwise jeopardise the investigation of suspicious business.

§ 79. **Procedure in case of order fulfilment postponement**

(1) Next, an AML officer shall instruct all the employees, who are authorised to receive and perform the customers' orders, not to fulfil any other orders of that customer. All the employees are obliged to adhere to such an instruction. If the performance of the order is provided by an automatic data-processing system, then it is necessary to implement changes into the system which ensures the customer's order will be postponed.

(2) Furthermore, an AML office shall keep with care:

(a) the information on postponed fulfilment of customer's order

(b) precise information on the date and time, when the FAU has received the notification on a suspicious business, in accordance with Chapter IV.2.

(3) If the funds, to which is the postponed customer's order related, is being kept by the company CryptoEngine s.r.o., then an AML officer shall ensure such funds against any possible transactions.

§ 80. **Postponement period of customer’s order fulfilment**

(1) A fulfilment of the order shall be postponed for the period of 24 hours, since the moment when the FAU (the Financial Analytical Office) has received the notification on a suspicious business.

(2) The FAU may then adopt a decision to extend this period even by up the next three working days. The FAU shall inform the company CryptoEngine s.r.o. on such

extended period in its notice, which may be performed orally, by phone, via a fax message or electronically. Once the notice is received, an AML officer shall inform the FAU by return, that the company CryptoEngine s.r.o. will extend the period for which is the customer's order postponed, and confirms the time when such a notice was received. The period of three working days starts to be counted from the moment, when the extended period was noticed by the FAU.

(3) If the FAU notifies the company CryptoEngine s.r.o., within the period, for which the customer's order is postponed, on the fact that the FAU has filed a notification to the competent law enforcement authority, then CryptoEngine s.r.o. may fulfil the customer's order at the earliest after three working days from the date on which the criminal complaint was lodged, unless up to the end of this period the competent law enforcement authority adopts decision on the withdrawal or confiscation of the subject matter of that suspicious business.

§ 81. **Customer's order fulfilment**

(1) If the company CryptoEngine s.r.o. has not received from the FAU, within the period for which is the customer's order postponed, any notice that the FAU has filed a notification to the competent law enforcement authority, then the company shall fulfil the customer's order. The same procedure is applied by the company CryptoEngine s.r.o. in the event, when a criminal complaint was lodged and no decision was made up to the end of the period extended by three working days, i.e., in case of the withdrawal or confiscation of the subject matter of that suspicious business.

(2) In this case, an AML officer shall promptly ensure that the customer's order will be fulfilled.

§ 82. **Confidentiality obligation**

(1) All the employees (including an AML officer) are obliged, in the event when the customer's order fulfilment was postponed, follow the confidentiality obligation, i.e., under no circumstances a customer cannot be informed, nor any other unauthorised person, on the fact, the notification on a suspicious business was filed, nor on any detailed information, even not after the moment, when the FAU adopts decision not to lodge a criminal complaint.

(2) For more information on the confidentiality obligation see Chapter V.2.

V. Other obligations

V.1. Information Obligation

§ 83. **Procedure for providing the FAU with information**

(1) The company CryptoEngine s.r.o. communicate, at the FAU's request, information on the services or trade relations for which the FAU is investigating within a specified period. The responsible person shall ensure the submission of documents on these transactions or give them access to authorized employees of the FAU.

(2) In case of personal contact, the authorized employees of the FAU shall produce a service card issued pursuant to the Act on Implementation of International Sanctions. The model of this card is a part of Decree No. 53/2017 Coll. FAU employees are not obliged to give their name.

(3) If requested by the AML officer or responsible person, each employee is obliged to provide assistance to him in the performance of this duty.

V.2. Confidentiality Obligation

§ 84. **Confidentiality Obligation**

(1) The employees, a person responsible, and an AML officer are obliged to follow the confidentiality obligation on the facts related to:

   (a) Notifications and investigation of a suspicious business

   (b) acts performed by the FAU

   (c) Performance of information obligation (see Chapter V.1).

(2) Next, everybody how becomes aware of these facts is obliged to keep them confidential.

(3) If these persons were transferred to another job position, by the fact when their employment relationship was terminated or due to other contractual relationship with CryptoEngine s.r.o., nor by the fact that the company CryptoEngine s.r.o. ceases to provide its services, the confidentiality obligation shall not be extinguished

§ 85. **Exceptions form confidentiality obligation and related procedure**

(1) The AML Act allows exemptions from confidentiality obligation in such cases that are stated in Section 39 of the AML Act. Thus, in the event, when any person requires to be provided with the information which is subject to the confidentiality obligation, shall notify a person responsible that shall review whether the Section 39 of the AML Act might by applied, i.e., the exemption from the confidentiality obligation towards a specific person. After the investigation findings a person responsible shall make a decision, whether and within which scope the information can be submitted. In the event when the information is requested by the FAU, the procedure of Chapter V.1 shall be applied.

V.3. Obligation to Train Employees

§ 86. **Training obligation**

(1) The responsible person is obliged to ensure all the employees undergo the training, i.e., the employees that may, during the performance of their working tasks, encounter a suspicious business, including a person responsible and an AML officer. The training shall include the rules and procedures stated herein, risk assessment, the AML Act, eventually the other legal regulations. The employees must be trained in such a way to be able to perform their work without mistakes and apply all the provisions stated herein, i.e., the provisions which are related to such employees. A person responsible shall amend and update the content of training.

§ 87. **Training frequency**

(1) The training must be performed at least once within the period of 12 months. There is also necessary to train all the not yet trained employees before they enter respective work positions (i.e., new or transferred employees).

§ 88. **Training report**

(1) The responsible person keeps and archives, in accordance with Chapter V.5 the attendance list and training content list. For these purposes may be used a sample of employees training report which forms a part of the Annex No. 3.

V.4. Obligation to Draw Up the Assessment Report

§ 89. **Assessment report**

(1) The responsible person shall prepare a report evaluating the activity of CryptoEngine s.r.o. at least once every 12 consecutive calendar months. in the area of preventing money laundering and terrorism financing. The evaluation report shall be drawn up not later than the end of the fourth calendar month following the end of the evaluation period.

(2) This report contains the following:

(a) assessing whether the procedures and measures it applies to prevent money laundering and terrorism financing are sufficiently effective; and

(b) an assessment of whether weaknesses were identified in the system of internal policies, procedures and control measures during the reporting period and what risks might arise therefrom; and

(c) statistics on suspicious transactions notifications for the past period, broken down by branches or activities regulated by AML by law; this information will be provided by the AML officer, who keeps a record of the suspicious transactions reported and beyond

(d) if shortcomings in the prevention of money laundering and terrorism financing are identified, the evaluation report shall include a proposal to remedy them.

(3) All the conclusions and assessment views shall be properly justified, a simple statement is not sufficient.

(4) If the assessment report is drawn up by other person than the AML officer, then the report must include also the view of the AML officer regarding the completeness and correctness of the data included in this report.

(5) The assessment report shall be discussed by the company statutory body within the period of 4 months after the last day of the assessed period. Company statutory body shall state its review to the report which reflects the shortcomings and proposals stated in the report.

(6) Evaluation of the assessment report performed by the above-named persons must be traceable, i.e., it shall be always obvious, who and when performed the assessment and upon which grounds. This information forms a part of the assessment report.

(7) The assessment report shall not be sent anywhere, it shall be archived for the period of 5 years.

V.5. Information and Documents Keeping and Archiving

§ 90. **Way of data recording**

(1) All the data and documents related to the business relationship shall be archived. In particular, this is the case of filled in forms, original documents or copies of documents submitted by a customer, and other company internal records. All the data and documents related to a specific service shall be archived analogically.

(2) A part of these documents may be also in a digital form. Any other way of data and documents archiving may be decided by a person responsible.

§ 91. **Making copies**

(1) The employee shall, pursuant to the AML Act, be authorised to make and keep the copies or identity cards or other documents records, upon which the identification is performed.

(2) In the event when from a copy made and archive is apparent the data which shall be otherwise obligatory recorded applying the way described herein, then it is not necessary to enter the data into the form. It is sufficient when the data is clear from the copy which was made.

§ 92. **Way of data and documents keeping**

(1) From each recorded information and archived documents shall be apparent:

(a) To which business relationship they are linked

(b) The employee who entered the data, amended the data or verified the data, and archived the documents

(c) The date on which was the data entered, amended or verified or when the documents were archived.

(2) Next, an AML office shall ensure safe archiving of the copies of filed notifications on a suspicious business, a document on their lodging, eventually an advice on their delivery.

§ 93. **Digital data**

(1) If the data or documents are recorded in a digital form, then the back-up shall be performed by a person responsible or by a person authorised to do so.

(2) Archiving some documents in a digital form is not allowed, which results from the provisions of the AML Act that prescribes some documents to be archived only as the original documents or certified copy – this is, in particular, the case of the powers of attorney and identification documents.

§ 94. **Period for which the information and documents shall be archived**

(1) Pursuant to the AML Act the company CryptoEngine s.r.o. is obliged to archive the data and documents for the following period:

(a) All the information and documents related to the business relationships and services defined herein shall be archived for the period of 10 years. This period starts to be counted by the first day of a calendar year which follows the year in which specific relationship was terminated.

(b) The employee training report (see Chapter V.3) shall be archived at least for the period of 5 years after the date when the training was performed.

(c) The assessment report (see Chapter V.4) shall be archived for the period of 5 years as a minimum.

V.6. Requirement for Traceability

§ 95. **Traceability**

(1) The term of traceability stated herein shall be understood as the state when it is possible, in case of certain procedure, determine retrospectively, why a specific action was performed (what was the reason), in what circumstances, what precede that action, and eventually what followed that action, what exactly was done, and who and when performed the steps.

(2) What shall be also traceable retrospectively:

(a) All the approval and decision-making procedures (incl. the evaluation procedure of customer's risk profile), in accordance with the present document, and also

(b) All the control and verification activities, in accordance with the present document, including related responsibilities, and also

(c) All the background documents and evaluation of the assessment report, and also

(d) All the findings which resulted from the verification of a customer, pursuant to Chapter II.4, and within the reviewing procedure of the businesses, and eventually a correspondence related to specific business, customer or business

relationship, and also

(e) All the assessment procedures of possibly suspicious business, which resulted in the fact that none suspicious business was notified.

(3) Due to this reason is necessary that all the records (digital or documentary), which are made in accordance with the present document and archived, contain at least the following information (if this kind of information is not apparent or cannot be deduced from other documents):

(a) To which business relationship, customer or case these are related

(b) The employee who entered the data, amended the data or completed the data, etc.

(c) Date and eventually time when it was performed

(d) All the other relevant information (reason, background documents supporting the decision, references to external data, etc.).

V.7. Obligation to Assess Regulations and Update Them

§ 96. **Frequency of assessment of AML rules and updates**

(1) The responsible person shall assess, at least every 12 calendar months, whether the provisions set out in this document and in the Risk Assessment document are current, proportionate to the nature, scale and complexity of currency exchange services and related activities. If necessary, it performs or arranges for updates to keep the regulations current and in line with the actual situation.

(2) In addition to this regular 12-month interval, the responsible person shall, without undue delay (ideally in advance), review and update this document and the Risk Assessment if any such need arises:

(a) the conclusion made in the Risk Assessment; or

(b) information provided by CryptoEngine s.r.o. obtains and leads to the conclusion that the Risk Assessment or the supporting documents used for it are no longer up - to - date, or

(c) a change in the business or strategy of CryptoEngine s.r.o., or

(d) amendments to legal regulations published especially on the website of the Financial Analytical Office http://www.financnianalytickyurad.cz/, on http://www.amlsystems.cz/AML-documents and on the website of the Czech National Bank https://www.cnb.cz/cs/dohled-financni-trh/legislativni-zakladna/legalizace-vynosu-z-trestne-cinnosti/; these pages are informative only and the responsible person is supposed to be active

(3) The responsible person will always create a written record of the assessment result and any further steps (whether the update and other details have been made).

(4) If there is a change in the Risk Assessment, the responsible person shall record the procedures used to draw up or update the Risk Assessment and shall also record the reasons on which it has drawn the conclusions contained therein.

(5) Furthermore, if the procedures set out in this document or in the Risk Assessment are substantially changed, the responsible person will organize training for the staff affected. It will record the content and attendance of the training according to the Chapter V.4.

(6) Changes in this document and in the Risk Assessment are approved by the Company's statutory body.

§ 97. **Customer´s data updates**

(1) If the procedures set out in this document or in the Risk Assessment are changed, the responsible person shall verify that the information provided by CryptoEngine s.r.o. about customers (information obtained during the identification and control of the customer and any other information used to prevent ML-FT), its content and scope correspond to new obligations. If not, the responsible person will oblige the employees to supplement or update this information. The employee shall always do so at the latest before making another trade with the customer.

VI. Internal verification

VI.1. Monitoring and Sanctions

§ 98. **Monitoring performance**

(1) Monitoring of the compliance with rules and procedures stated herein shall be performed by a person responsible. A person responsible may forward a partial monitoring towards an AML officer or other person. All the employees and an AML officer are obliged to undergo such a monitoring. The monitoring is to be performed in place, analysing the data and documents, or applying other ways of monitoring.

(2) The monitoring shall be performed regularly, ideally once a month. A person performing the monitoring selects a control sample, on which he/she checks whether the procedures stated herein and prescribed by legal regulations were adhered to. The ideal situation is when a control sample is in compliance with all the business relationships or services provided within the monitored period, however, this is not possible due to capacity reasons, thus a random selection is sufficient.

§ 99. **Report on internal monitoring performance**

(1) A person that performs the internal monitoring shall, when the monitoring is finished, draw up a report. This report sample is shown in the Annex No. 1.

§ 100. **Infringement's detection**

(1) Each person that has found out any infringement shall report this state immediately to a person responsible, also in the case when the infringement was caused by this person.

§ 101. **Evaluation of infringements and further procedure**

(1) In the event when a breach of rules and procedures prescribed herein are found out from the monitoring or notification, such a breach shall be assessed individually, in particular upon the level of seriousness and the extent, up to which these could jeopardize the effectiveness of measures applied against the legalization of the proceeds of crime and terrorism financing. A personal responsibility shall be then inferred on employees within the scope of applicable labour legal regulations. A person responsible shall, within the scope of his/her possibilities, simultaneously adopt the measures to prevent a repeated breach (repeated training of the employees, approval of additional measures, etc.).

§ 102. **Advice of consequences of rules infringement**

(1) All the persons to which is the present document shall be aware of the fact that any breach (infringement) of the rules and procedures stated herein would most probably result also in a breach of the provisions stated within the AML Act, and therefore the company CryptoEngine s.r.o. may be subject to a sanction or even the withdrawal of business license may be applied.

VI.2. Amendments to Regulations

§ 103. Monitoring of Amendments to Regulations

(1) Persons responsible, i.e., an AML officers, are obliged to perform permanent monitoring of the development in the field of measures against legalization of proceeds of crime and financing of terrorism (i.e., the Acts, Decrees, Notices, etc.). Relevant regulations are published by the FAU (Financial Analytical Office) on its websites www.financnianalytickyurad.cz, and also on the websites of the Czech National Bank at: https://www.cnb.cz/cs/dohled-financni-trh/legislativni- zakladna/legalizace-vynosu-z-trestne-cinnosti/. The websites shall be understood as information source only, and a person responsible shall be actively involved in this kind of activity.

§ 104. Implementation of the Present Document Amendments

(1) In the event when the mentioned regulations are amended, or the new regulations come into force, the person responsible, i.e., an AML officer, shall implement such amendments to the present document to ensure the compliance of the present document with these regulations, a AML officer is also obliged to ensure the training of all the persons who shall be familiarized with such amendments.