Risk Assessment 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

Telephone number: +44 7429548578

Email address: support@cryptos-engine.com

I General Points

I.1 Introduction

§1. Meaning of the document

(1) This Risk Assessment identifies and assesses risks arising from the legalization of proceeds of crime and financing of terrorism that may potentially occur in the company of

(2) CryptoEngine s.r.o. within the scope of provision of virtual assets services.

(3) This risk assessment forms part of the System of Internal Rules, Procedures and Measures for the fulfilment of obligations arising from Act No. 253/2008 Coll., on selected measures against legalization of proceeds of crime and financing of terrorism, as amended (further as AML law). Definitions and abbreviations used throughout this document are explained in the System of Internal Rules.

§2. Explanation of the Purpose of the Risk Assessment

(1) The norm in the fight against ML-FT has been the application of the so-called risk-based approach (abbreviated as RBA in English). The AML Act prescribes the required minimum of obligations that must be fulfilled.

§3. Basic Obligations

(1) In relation to this Risk Assessment and pursuant to the AML Act,

(2) CryptoEngine s.r.o. is obligated to fulfil the following obligations:

(a) to prepare and approve this Risk Assessment

(b) to apply measures to reduce the ML-FT risks listed in this Risk Assessment (Chapter II)

(c) to carry out internal supervision and monitoring of compliance with legal regulations (Chapter II.3)

(d) to check employees (Chapter II.4)

(e) to update this Risk Assessment periodically (Chapter II.5).

I.2 Starting points

§4. Information Sources

(1) The following sources were used in the process of ML-FT risk identification and assessment:

(f) Sector analyses from the sphere of ML-FT (especially by FATF-GAFI)

(g) National risk assessment processed in compliance with Section 30a of the Act[1]

(h) European risk assessment processed by the European Commission[2],

[1] Act No. 253/2008 Coll., on Certain Measures Against Money Laundering and Terrorism Financing, as amended

[2] Article 6 (1) to (3) of the Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on preventing the use of the financial system for the purpose of money laundering or terrorism financing, amending Regulation (EU) No 648 / 2012 and repealing Directive 2005/60 / EC of the European Parliament and of the Council and Commission Directive 2006/70 / EC.

(i) Sources considered by the Czech National Bank to be so called approved standards

(j) Methodological and explanation materials and resolutions of the Czech National Bank and FAU

(k) Information provided by the FAU and law enforcement authorities

(l) Information obtained during identification and check of clients.

I.3 Identification of risk factors

§5. Vulnerabilities

(1) In connection with the above listed threats,

(2) CryptoEngine s.r.o. has identified the following vulnerabilities (i.e., "weak spots" that may facilitate a client's abuse of the services for ML-FT):

(m) client identification: a person who does not wish to be associated with the virtual assets service is interested in the services and therefore another person (appearing to be the client), who is only the identity provider, acts on his behalf and conceals that he is acting on behalf of another person who does not actually wish to be associated with the virtual assets service

(n) client check: a client provides false, superficial or incomplete information about the source of the financial resources because the client expects that reviewing the source of the financial resources is a very difficult or impossible process and expects the employee to neglect this obligation or fail to perform it appropriately;

(o) Persons against whom the Czech Republic applies international sanctions (including persons involved in terrorism) are hidden in complex and non-transparent ownership and management structures of legal entities; such client expects that to uncover the ownership and management structure of the client-legal entity and expects the company to neglect this obligation or to perform it incompletely.

§6. Types of risk

(1) CryptoEngine s.r.o. has identified and assessed the following threats:

(p) High risk: abuse of the virtual assets services as a technique for the legalization of resources originating from criminal activity, especially resources originating from tax fraud, subsidy fraud, corruption activity, breach of trust in administration others´ property, etc.

(q) medium risk: international sanction evasion (i.e., changing the nature of and transferring property of persons subject to international sanctions)

(r) medium risk: financing of terrorism

(s) low risk: all other threats.

§7. Risk Factors

(1) The risk factor is the characteristics of the client, the product provided to him/her, or the way in which it is provided, which increases the risk that services of the company

(2) CryptoEngine s.r.o. might be misused by the client for the purpose of money laundering or terrorism financing, based on which the client is assigned a risk profile of the type A, B, C, D or E.

§8. Risk profile - type A

(1) The client is assigned a type A risk profile (client with no risk or with minimal risk) in the absence of known risk factors to be assigned a type B, C, D or E risk profile. These are therefore clients with no or only very small and negligible risk that they could use the services of the company

(2) CryptoEngine s.r.o. for ML-FT purposes. This is a risk the company is willing to accept.

§9. Risk profile - type B, C or D

(1) The client is assigned a risk profile of the type B, C or D or E.

(2) A client with a risk profile of the type B, C or D represents for the company

(3) CryptoEngine s.r.o. a potential risk from the ML-FT perspective and therefore all the employees, including the AML Officer, must pay close attention to the assessment of any suspicion character of this client's behavior and place increased demands on the accuracy of the information provided by the client during the first or ongoing review, where appropriate, to substantiate the information disclosed by a specific document.

(4) The following risk factors relate to the type B, C or D risk profile, while on the fact whether a risk profile of type B, C or D will be assigned to the client based on the risk factors described here the employee will decide in accordance with a special document for a risk assessment profile of the client annexed to this Risk Assessment:

(t) the client uses services that include transaction to or from a country or territory that is identified as risky from the ML-FT perspective; a list of these countries is given in Annex 5 of the Internal Rules System;

(u) the client requires a transaction that is unusually complex or large-volume, or involves an unusual way of trading, or the economic and legal purpose of which is not obvious;

(v) the client or its beneficial owner engages in a business or other activity that is "cash intensive" - that is, an activity that generates large amounts of cash or other valuable commodities of a purely anonymous nature, including virtual currencies (e.g., currency exchange, trade in precious metals, virtual currency, etc.);

(w) the client or its beneficial owner carries on business or other activity in the field of gambling, military industry and services, nuclear energy;

(x) in the course of business, the client or its beneficial owner handles content accessible only to adults, with the exception of products designed for direct consumption, such as cigarettes, alcohol, etc.;

(y) the client is a non-entrepreneurial legal entity whose activity is not traceable in

trustworthy sources and the client has difficulty to prove its activity or proves it in such a way that doubts arise;

(z) a client who has previously been the subject of a suspicious transaction notification;

(aa) a client whose behavior has previously shown some signs of a suspicious transaction but ultimately has not been classified as a suspicious transaction, although doubts remain;

(bb) the client or its beneficial owner is a PEP, or the client is a person acting in the interest of such a PEP;

(cc) any country of origin (including the registered office or residence) of the client, its beneficial owner or the person authorized to act on behalf of the client is a risk country from the ML-FT perspective; the list of these countries is given in Annex 5 of the System of Internal Rules;

(dd) the country of origin of the person having direct or indirect participation in the client is a risk country from the ML-FT perspective; the list of these countries is given in Annex 5 of the System of Internal Rules;

(ee) the country of origin of a person who is a member of the statutory body of a client, a representative of a legal entity in that body, or is in a position similar to that of a member of a statutory body or otherwise has the possibility to apply influence at the client, being a legal entity, is a risk country from the ML-FT perspective; the list of these countries is given in Annex 5 of the System of Internal Rules;

(ff) the client is a trust fund;

(gg) the ownership structure of the client is non-transparent;

(hh) the behavior of the client or the person representing it is abnormal in or during the establishment of a business relationship compared to a typical client similar to it (e.g., non - standard requirements, unusual ways of transaction performance, requirements for special or complex types of representation, etc.);

(ii) uncertainties arise as to the origin of the client's property or the beneficial owner's property or the funds held by the client or the beneficial owner of the client;

(jj) open trusted sources (e.g., news media) indicate that the client or related persons have been or are involved in criminal or other unfair activities;

(kk) there is a suspicion that the client is not acting on his / her own name, i.e., the property that is the subject of the service actually belongs to someone else and the client is only an intermediary or identity provider;

(ll) the client or a related person (member of the statutory body, the beneficial owner) is linked to another client (factually or legally) whose risk profile is of the type B;

(mm) another fact that, according to the information held by

(nn) CryptoEngine s.r.o. available, there is an increased risk of money

laundering or terrorist financing associated with the client's business activity and its beneficial owner;

(oo) according to the information held by

(pp) CryptoEngine s.r.o. available, there is an increased risk of money laundering or terrorist financing related to the high client's turnover;

(qq) the payment or other service used by the client, or its nature or the nature of individual transactions, is non-standard for the given type of client;

(rr) any of the factors listed above, if it occurs in a legal entity in which the client has a direct or indirect participation, or otherwise has the opportunity to exercise influence over it.

(5) A risk country in this chapter is a country included in a list of countries where measures against money laundering or terrorist financing are not being applied to any extent or insufficiently. This list is included in Annex 5 to the System of Internal Rules and it is necessary to keep it up to date.

(6) The country of origin is understood in this chapter:

(ss) for a natural person, any state of which he or she is a national and, at the same time, all other states in which he / she is registered for a residence of more than 1 year or for permanent residence, if known,

(tt) for a legal entity that is a bank or financial institution, the state in which it has its registered office,

(uu) for a legal entity that is not a bank or financial institution, the state in which it has its registered office and simultaneously all the states in which it has a branch.

(7) The non-transparent ownership structure in this chapter means a situation where the beneficial owner or ownership and management structure of the client cannot be established based on:

(vv) a public register, records of trust funds or records of beneficial owners kept by a public authority of the Czech Republic, or

(ww) a similar register or register of another state, or

(xx) any other source or combination of sources that the company reasonably believes to be trustworthy and which it reasonably believes to provide, in its entirety, complete and up-to-date information on the beneficial owner and ownership and management structure of the client, in particular when issued by a public authority or officially legalized.

(8) The ownership structure is not non-transparent if the client is a company whose securities are admitted to trading on a European regulated market or a foreign market similar to that of a European regulated market if it is subject to disclosure requirements equivalent to those of European Union law.

§10. Risk profile - type E

(1) The client is assigned an E-type risk profile (unacceptable client) if any of the risk factors listed below are present.

(2) A client with a risk profile of the type E represents for

(3) CryptoEngine s.r.o. a high risk in terms of money laundering and terrorist financing. If the client is assigned a risk profile of the type E, the client will not be provided with a virtual assets service or a business relationship with the client, or the business relationship with him will be terminated and no other service will be provided. In this situation, the client is considered to no longer meet the client's acceptability criteria.

(4) In this case, termination of the business relationship or failure to provide service will be ensured by the AML officer. It shall take all necessary steps without undue delay to ensure that the business relationship is effectively and legally terminated. In addition, it will prevent the Client from being provided with any new services until the business relationship is terminated.

(5) Furthermore, great care must be taken when assessing whether the client's conduct is showing signs of a suspicious transaction.

(6) The following risk factors relate to the type E risk profile:

(yy) there is a reasonable suspicion that the purpose of the business relationship is to provide services to a person other than himself (i.e., the client acts only as an intermediary or identity provider) and the client does not refute the suspicion;

(zz) the client or a person associated with it (a member of the statutory body, beneficial owner, etc.) or another payment recipient (if known) is a person against whom the Czech Republic applies international sanctions;

(aaa) information provided by the client about himself / herself and his / her activities are grossly contrary to the reality, which was found from credible sources and the client did not justify the non-compliance;

(bbb) there is a reasonable suspicion that the client is providing false, misrepresented or incomplete information in the course of duration of the business relationship or that he is submitting false or altered documents;

(ccc) business relationship with this client has been terminated in the past due to the initiative of the company

(ddd) CryptoEngine s.r.o. and the client tries to establish it repeatedly;

(eee) the client or a person associated with it (a member of the statutory body, the beneficial owner, etc.) is connected with another client with whom the business relation was terminated in the past due to the initiative of the company

(fff) CryptoEngine s.r.o.;

(ggg) for other reasons, the client represents a significant risk to the company in terms of money laundering or terrorism financing

(hhh) any of the factors listed above, if it occurs with a legal entity in which the client has a direct or indirect participation, or otherwise has the ability to exercise influence over it.

II Measures adopted to mitigate threats

II.1 Measures for Client Identification

§11. Expansion of PEP Risk Status

(1) As stated in AML law, the company

(2) CryptoEngine s.r.o. considers a person to be PEP one year after the termination of its function.

§12. Exclusion of simplified identification and control

(1) Simplified identification is applied only in case of clients with risk profile of type A.

§13. Interval of updates

(1) The employee will update the identification data, information on whether or not the client is a PEP, whether the Czech Republic applies international sanctions against him or his related persons whenever the company

(2) CryptoEngine s.r.o. gets to know about any change and at least once in the following time intervals:

(iii) every 12 calendar months for a client with a risk profile of the type A

(jjj) every 9 calendar months for a client with a risk profile of the type B,

(kkk) every 6 calendar months for a client with a risk profile of the type C and D.

(3) The update is done by searching for identification and other data in public trusted sources or by asking the client if the identification and other data (PEP flag) are still current. In the case of a client with a risk profile of type B, C or D, it is not always sufficient within the framework of the update to provide written confirmation of the timeliness of the identification data, which

(4) CryptoEngine s.r.o. keeps about the client.

(5) The employee is obliged to create a record on the verification of international sanctions and on the result, which always corresponds to the requirement of retrospectivity according to chapter V.6 of the System of Internal Rules, i.e., it contains at least the following information:

(lll) date of verification and name of the person who performed the verification (whether performed by a specific employee or automated);

(mmm) a list of natural and legal persons that have been checked in the sanction lists;

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

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

II.2 Measures during Client's Control/Check

§14. Increase of intensity of the first control/check of the client

(1) If the client is assigned a risk profile of the type B, C or D, at the first check of the client before establishing a business relationship:

(ppp) the employee must check the source of client's financial resources from an independent source, as opposed to only relying on the client's oral or written statement (i.e., from bookkeeping records, third party issued documents, audited documents etc.); the employee shall obtain and keep a copy of such document (a simple Xerox copy shall suffice) or shall keep the original document; otherwise the employee will not execute the transaction with all the consequences (the client is obliged to comply with such a request and if he refuses it, it is a suspicious transaction that must be reported)

(qqq) if the employee is not able to establish the controlling and ownership structure of the client – a legal entity (up to the beneficial owner) from public trustworthy sources (e.g., extracts from the register of persons), he will require from the client not only to declare, but also to demonstrate the control and ownership structure to the beneficial owner;

(rrr) if the client is a legal entity or a natural person doing business, the employee will find out and record a detailed description of all the client's activities in a really detailed way and he will verify it from publicly available information (existence of appropriate business licenses, officially available service offerings on the website, publicly available client references, etc.) and if this information is not available, it will request the client to evidence the activities.

§15. Approval of a business relation and its changes by an AML officer

(1) If the client is assigned a risk profile of the type B, C or D, the establishment of a business relationship must be approved by the AML officer or the Managing Director of the company

(2) CryptoEngine s.r.o. and creates a record of approval. Similarly, the AML officer or Managing Director of the company

(3) CryptoEngine s.r.o. must approve all and any substantial changes in the framework contract for the provision of virtual assets services that have been triggered by the client's request (e.g., request to increase limits, a new joint holder, etc.) and on approval to create a record.

§16. Update of information

(1) The employee shall update the information concerning the purpose of the business relationship and risk profile:

(sss) every 12 calendar months for a client with a risk profile of the type A

(ttt) every 9 calendar months for a client with a risk profile of the type B,

(uuu) every 6 calendar months for a client with a risk profile of the type C and D.

(2) In case of change of the information concerning the purpose of the business relationship, or in case of the changes in ownership and management structure. Clients with the risk profiles B, C or D are obliged to prove the mentioned structure up to UBOs.

§17. Circumstances causing continuous re-viewing of trades and intensity of re-views

(1) Every 6 months, the employee checks:

(a) for a client with risk profile of the type A – of other 3 randomly selected transaction of any volume. The employee may also request additional proof of economic activity in the form of 2 invoices from the suppliers.

(b) for a client with risk profile of the type B – of 5 other randomly selected transaction of any volume. An employee may also request additional proof of economic activity in the form of 2 invoices from the suppliers.

(c) for a client with risk profile of the type C – and of 10 other randomly selected transaction of any volume. An employee may also request additional proof of economic activity in the form of 4 invoices from the suppliers and 4 actual contracts.

(a) for a client with risk profile of the type D – of 20 transactions exceeding 15 000 EUR and of other 20 randomly selected transactions of any volume. An employee may also request additional proof of economic activity in the form of 4 invoices from the suppliers and 4 actual contracts.

(3) Business control of the client is focused on comparison of the real business activity of the client to the one that was declared. It is performed if the expected amount and volume of transactions is exceeded by 50%. The client is supposed to provide confirmation about his income and business activity and new limits should be set.

(4) In case the criteria for the mentioned business control were met, it is necessary to ask the client to submit confirmation of income and business activity (in case of using services for business purposes). Once the business control happened, the new limits should be set for funds.

(2) If a client has been assigned a risk profile of the type D, the client's source of funds must be verified from an independent source, not simply relying on the client's oral or written statement (i.e., accounting documents, third party documents, audited documents, etc.); the employee shall make and keep a copy of such a document (a standard copy is sufficient to be kept) or keep the original of the document; otherwise the employee will not execute the transaction with all the consequences (the client is obliged to comply with such a request and if he refuses, it is a suspicious transaction that must be reported).

(3) Furthermore, in case of a client with a risk profile of the type B, C or D, when:

(a) the client uses services that include payment to or from a country or territory that is identified as risky from the ML-FT perspective; the list of these countries is given in Annex 5 to the System of Internal Rules;

(b) the client requires a transaction that is unusually complex or large-volume, or involves an unusual way of trading, or the economic and legal purpose of which is not obvious;

(c) the client or its beneficial owner engages in a business or other activity that is "cash intensive" - that is, an activity that generates large amounts of cash or other valuable commodities of a purely anonymous nature, including virtual currencies (e.g., currency exchange, trade in precious metals, virtual currency,

etc.);

(d) the client or its beneficial owner carries on business or other activity in the field of gambling, military industry and services, nuclear energy;

(e) in the course of business, the client or its beneficial owner handles content accessible only to adults, with the exception of products designed for direct consumption, such as cigarettes, alcohol, etc.;

(4) The employee will always ask the client for a wider range of the required information (if it does not already have it) and will always investigate the background and purpose and method of performing such transactions.

II.3 Measures for Employees Screening

§18. Requirements towards Employees

(1) An executive staff member shall screen and permit only such employee or contact person to perform the job that has no record in the Criminal Register of any EU country.

II.4 Obligation to Periodically Update This Document

§19. Updates and frequency

(1) An executive staff member shall ensure that this Risk Assessment be periodically updated at least once in two years. The Risk Assessment shall also have to be updated especially in case that:

(f) notice is approved about the next round of the national risk assessment process in the sphere of ML-FT

(g) a significant change occurs in the manner services are provided and new services are introduced, or potentially a new client group is targeted

(h) new threats are discovered, especially following a notice of a suspicious business transaction related to a situation not covered by this Risk Assessment.

(2) This Risk Assessment is approved by the corporate statutory body.