Table of Contents

I. List of Abbreviations

AML Act	Act No. 253/2008 Coll., on Selected Measures against the Legitimization of Proceeds of Crime and Financing of Terrorism, as amended
AML/CFT prevention	Measures in the area of prevention of money laundering and financing of terrorism (Anti-Money Laundering / Countering the Financing of Terrorism)
FAU	Financial Analytical Office
ISM	Cabinet Regulation No. 210/2008 Coll., on the Implementation of Special Measures in Fight against Terrorism, as amended
ML/FT	Money Laundering / Financing of Terrorism
OPO	Notification of Suspicious Transaction
PEP	Politically Exposed Person
Sanctions Act	Act No. 69/2006 Coll., on the Implementation of International Sanctions, as amended
SVZ	System of Internal Principles, Procedures and Control Measures
Company	Privateum

II. Definition of Terms

Financing Terrorism	Gathering or providing financial or other assets knowing that such assets will be, in full or in part, used to commit criminal offence of terror, a terrorist attack, participation in a terrorist group, support and promotion of terrorism or the offence of threatening to commit a terrorist act or an offence intended to enable or assist the commission of such offence, or to support a person or group of persons preparing to commit such offence. Actions with intention to remunerate or compensate a person who has committed criminal offence of terror, terrorist attack, participation in a terrorist group, support and promotion of terrorism or a crime of threatening a terrorist act or a crime intended to enable or facilitate the commission of such a crime, or a person close to him within the meaning of the Criminal Code, or collecting assets to pay such remuneration or compensation. For the purposes of the AML Law, financing the proliferation of weapons of mass destruction, which means the collection or provision financial or other assets knowing that it will be used, even in part, by a proliferator of weapons of mass destruction or will be used to support the proliferation of such weapons in violation of the requirements of international law. It is irrelevant whether the conduct occurred or is to occur in whole or in part in the Czech Republic or abroad.

Legitimisation of Proceeds of Crime	Conduct intended to conceal the illicit origin of any economic advantage resulting from criminal activity to give the appearance of a lawfully acquired financial benefit; that conduct is in particular: - in the conversion or transfer of assets knowing that they come from crime, for the purpose of concealing or disguising its origin or for the purpose of assisting a person who engages in such activity to escape the legal consequences of his or her conduct, - in concealing or disguising the true nature, source, location, movement or disposal of assets, or a change in the rights relating to assets, knowing that such assets derive from crime, - in the acquisition, possession, use or disposal of assets knowing that they originate from crime, - in a criminal association or any other type of cooperation for the purpose of the conduct referred to above. It is irrelevant whether the conduct occurred or is to occur in whole or in part in the Czech Republic or abroad.
Opaque Ownership Structure	A situation where the Beneficial Owner or the ownership and management structure of the Client cannot be ascertained from: - the public register, the register of trusts or the register of Beneficial Owners kept by a public authority of the Czech Republic, - similar register or records of another State, nor - another source or combination of sources that the Company reasonably believes to be reliable and which the Company reasonably believes, in its entirety, will provide complete and current information about the Beneficial Owner and the ownership and management structure of the Client, particularly if it is issued by a public authority or is officially certified.
Transaction	Any interaction of the Company acting in that capacity with another person should such interaction lead to attempted handling of the other person's property or providing services to such person. If a transaction is divided into several separate transactions that are related, the value of the transaction is the sum of these transactions.
Business Relationship	A contractual relationship between the Company, acting in that capacity, and another person, the purpose of which is to handle assets of that other person or to provide services to that other person, if it is clear at the inception of the contractual relationship, having regard to all the circumstances, that it will be continuing or involve recurring performance.
Suspicious Transaction	A transaction carried out in circumstances giving rise to a suspicion of an attempt to launder the proceeds of crime or a suspicion that the funds used in the transaction are intended to finance terrorism, or that

	the transaction is otherwise related to or connected with the financing of terrorism, or any other fact that might indicate such a suspicion.
Politically Exposed Person	a) A natural person who is or has been in an important public office of national or regional significance, such as, in particular, the Head of State, the Prime Minister, the head of a central state administration body or his deputy (deputy, state secretary), a member of parliament, a member of the governing body of a political party, the head of a local authority, a judge of the Supreme Court, the Constitutional Court or other supreme judicial body, whose decision is generally (with exceptions) not subject to appeal, a member of the board of a central bank, a high-ranking officer of the armed forces or corps, a member or representative of a member (if a legal person) of the statutory body of a state-controlled commercial corporation, an ambassador or head of a diplomatic mission, or a natural person who holds or has held a similar position in another state, EU body or international organisation, (b) a natural person who is: (1) a person close to a person referred to in point (a), 2) who is a shareholder or Beneficial Owner of the same legal entity or trust as the person referred to in point a) or is known to the Company to be in any other close Business Relationship with the person referred to in point a), 3) who is the Beneficial Owner of a legal entity or trust known to the Company to have been created for the benefit of a person referred to in (a).
Identity Card	A document issued by a public administration authority which contains the name and surname, date of birth, and which shows the form or other information enabling the person presenting the document to be identified as its authorised holder.
Risk Country	A country that is a risk in terms of money laundering, terrorist financing or proliferation of weapons of mass destruction. The list of such countries is set out in Commission Regulation (EU) 2016/1675 of 14 July 2016 supplementing Directive (EU) 2015/849 of the European Parliament and of the Council by identifying high-risk third countries with strategic deficiencies, as amended.
Risk-Based Approach	RBA (risk-based approach) is an approach to the implementation of AML/CFT measures that enables the Company to allocate resources (human and financial) appropriately while effectively managing ML/TF risks. Effective RBA is based on a carefully conducted risk assessment (their identification, understanding and assessment).

Sanctioned Person	A person against whom the Czech Republic applies international sanctions pursuant to the Sanctions Act.
Beneficial Owner	A beneficial owner according to the Act No. 37/2021 Coll, on the Register of the Beneficial Owners, as amended or an individual, on which account the transaction is provided.
Third Country	A country that is not a member of the European Union or the European Economic Area.
Country of Origin	In case of the Client – a natural person, each state of which that person is a national and, in which he or she is registered for permanent or other residence, or in which he or she has resided for more than 1 year. In case of the Client - an entrepreneur any state which is his country of origin or in which he is established, in case of the Client - a legal entity a state in which it is established and any state in which it has a branch or establishment.

III. Legal Resources

III.1. The following legal resources have been used in preparation of this Guideline:

III.1.i. Act No. 253/2008 Coll., on Selected Measures against the Legitimization of Proceeds of Crime and Financing of Terrorism, as amended,

III.1.ii. Act No. 69/2006 Coll., on the Implementation of International Sanctions, as amended,

III.1.iii. Act No. 37/2021 Coll, on the Register of the Beneficial Owners, as amended,

III.1.iv.Cabinet Regulation No. 210/2008 Coll., on the Implementation of Special Measures in Fight against Terrorism, as amended,

III.1.v. Methodological Instruction No. 1 – to the Application of international sanctions,

III.1.vi. FAU Methodological Instruction No. 3 on Determination of True Owner,

III.1.vii. Methodological Instruction No. 4 of the FAU on Submitting a Report of a Suspicious Transaction in a form other than via the MoneyWeb connection,

III.1.viii. Methodological Instruction No. 7 - Measures against PEP + national list of PEP functions,

III.1.ix. Methodological Instruction No 9 - Due Diligence,

III.1.x. Handbook for recording the Beneficial Owners - a document of the Ministry of Justice, available at

prirucka-evidovani-skutecnych-majitelu-dokument-ministerstva-spravedlnosti.pdf (gov.cz).

IV. Client Identification

IV.1. Identification Data

IV.1.i. Identification data according to Section 5 of the AML Act are:

a) all names and surnames, birth number and, if not assigned, date of birth and sex, place of birth, permanent or other residence, nationality and number and type of Identity Card, the State or, where applicable, the authority which issued the Identity Card and its period of validity; in the case of a natural person engaged in business, also his or her business name, distinctive supplement or other designation, registered office, and personal identification number,

b) in case of a legal person:

1. basic identification data of the legal entity, which are the business name or name including a distinctive supplement or other designation, the registered office and the legal entity identification number or similar number assigned abroad,
2. information to identify and verify the identity of the natural person who is a member of its statutory body, and
3. basic identification data of the legal person who is a member of its statutory body and data to establish and verify the identity of the natural person who is a member of the statutory body of that legal person or who has been authorised by that legal person to represent it in the statutory body.

IV.2. Brief Description of Company's Business Model

IV.2.i. The Company allows its Clients to use the PRI Pay Terminals, which are crypto terminals that offers instant and safe crypto transactions. It is possible to buy and sell supported cryptocurrencies via the terminals. The interconnection with the terminal is secured by the PRI Pay mobile wallet, which enables the Clients to invest, trade, and send crypto across borders.

IV.3. Moment of Identification

IV.3.i. The Company will identify the Client before the establishment of the Business Relationship in the process of concluding a contract.

IV.3.ii. All contracts concluded by the Company as an Obliged Person are in text form.

IV.3.iii. In case of the single transaction and use of PRI Pay Terminals up to the amount of EUR 1,000 the Client is identified according to Section IV.7.

IV.3.iv. The Company will perform the Identification, should any of the following occur:

a) at the latest when it is clear that the value of the single transaction amount exceeds EUR 1,000, or

b) the Company identifies a Suspicious Transaction.

IV.4. Ways of Identification

IV.4.i. The Company shall primarily use the Remote Identification in accordance with Section 11(7) of the AML Act (Section IV.5).

IV.4.ii. The Company also identifies the Clients in the personal presence of the Client in accordance with Section 8 of the AML Act (Section IV.6).

IV.5. Remote Identification

IV.5.i. Remote Identification is carried out by company SUMSUB TECH LTD ("Sumsub").

IV.5.ii. The Company, in the course of carrying out the Identification of the Client by using Remote Identification method collects via Sumsub the following data:

a) **Natural person:** copy of the relevant parts of the Identity Card and a selfie photo of the Client's face with the Identity Card and in some cases other supporting document from the Client. From Identity Card it should be possible to ascertain the information referred to in Section 8(2)(a) of the AML Act - identification details, type and number of the Identity Card, the state and authority that issued it, the period of validity, and a representation of the form.

b) **Legal entity:** proof of existence and identification data of the legal entity, which the Company may also obtain from the public register.

IV.5.iii. The Client provides credible evidence to the Company of the existence of a payment account in his/her name with a credit institution (i.e. or with a foreign credit institution that is not located in a high-risk third country,), namely an electronically signed document.

IV.5.iv. A written contract is concluded between the Client and the Company.

IV.5.v. The Client makes the first payment amounting to max EUR 1, thus fulfilling the requirement of a credible way of proving the existence of a payment account. If it is possible the payment will be accompanied also by the information on the purpose of the identification and designation of the Company, together with the name and surname of the Client

IV.5.vi. The purpose and intent of this payment is to verify that there is a relationship between the account disposer and the Client, who is also the owner of this account.

IV.5.vii. The Company shall verify whether the above conditions are met and whether, the Client, the product or any transaction poses an increased risk of money laundering or terrorist financing.

IV.5.viii. Sumsub also verifies that the Client, the natural person acting for the Client in the given transaction or Business Relationship and its Beneficial Owner, if known, is not a PEP or a Sanctioned Person, and another person in the ownership or management structure of the Client, if known, is not a Sanctioned Person. Furthermore Sumsub verifies the Identity Card if it is authentic, legitimate, and free of forgery or alteration, it verifies on a daily basis the expiry of the Identity Card, performs biometric analysis that the Identity Card and supporting document photo matches that of the holder, it provides verification of permanent or other residence, e-mail address and telephone number, it performs daily AML monitoring and fraud prevention.

IV.5.ix. If the Company suspects, when entering into a Business Relationship, that the Client is not acting on his/her own behalf or that he/she is concealing that he/she is acting on behalf of a third party, the Company will ask the Client to provide evidence of his/her authority to do so and of the identity of the mandator so an Identification can be performed (see Section IV.8). The Company states to the Client that everyone is obliged to comply with this request.

IV.5.x. If the Client is a natural person for whom no other person is acting, it is not necessary, in the circumstances specified in the written risk assessment, to send a copy of the supporting document if the payment is accompanied by the information referred to in Article IV.5.v.

IV.6. Identification in the Personal Presence of the Client

IV.6.i. The first Identification of a Client who is:

a) **Natural person**: is performed by the Company with the Client present in person at the seat of any branch of the Company,

b) **Legal person**: is performed by the Company with the person acting on behalf of the Client present in person.

IV.6.ii. In case of a natural person, the Company records Identification Data (Section IV.1) and verifies them from an Identity Card should they be included thereon, the Company verifies the holder's appearance and the holder's facial image as pictured on the Identity Card.

IV.6.iii. In case of a legal person, the Company records Identification Data (Section IV.1) and verifies them from the proof of existence of the legal person received from a reliable source and performs identification of the natural person acting on behalf of such legal person in respect of the given transaction or Business Relationship.

IV.6.iv. The Company determines and takes record of the status of the Client, natural person acting on behalf of the Client in respect of the given transaction or Business Relationship or its Beneficial Owner, as a PEP or a Sanctioned person and status of another person in the ownership or control structure of the Client, should they be known to the Company as a Sanctioned person.

IV.6.v. The Company may, without the Client´s consent, make copies or excerpts from submitted documents.

IV.7. Identification of the Client in case of single Transaction up to EUR 1,000

IV.7.i. In case of a single transaction of the Client up to the amount of EUR 1,000, the Client shall in order for the Company to be able to prevent frauds, submit to the Company (via Sumsub) copy of the relevant parts of the Identity Card and a selfie photo of the Client's face with the Identity Card and other supporting document. From Identity Card it should be possible to ascertain the information referred to in Section 8(2)(a) of the AML Act - identification details, type and number of the Identity Card, the state and authority that issued it, the period of validity, and a representation of the form.

IV.7.ii. The Company will determine via Sumsub whether the Client is not a PEP or a person subject to International Sanctions.

IV.7.iii. Sumsub also verifies the Identity Card if it is authentic, legitimate, and free of forgery or alteration, it verifies on a daily basis the expiry of the Identity Card, performs biometric analysis that the Identity Card and supporting document photo matches that of the holder, it provides verification of permanent or other residence, e-mail address and telephone number, it performs daily AML monitoring and fraud prevention.

IV.7.iv. In case that the conditions under Section 7 of the AML Act are fulfilled (the value of the transaction exceeds EUR 1,000, it is a Suspicious Transaction, or in case of establishment of a Business Relationship), the Company will re-identify the Client based on the Client's choice, either on the basis of Remote Identification (Section IV.5) or in the Client's Personal Presence (Section IV.6).

IV.7.v. If the Client chooses Remote Identification, the remaining requirements within the meaning of Section 7(11) will be requested by the Company (see IV.5.iii - IV.5.vii).

IV.8. Identification of the Client Represented by Another Person

IV.8.i. Should the Client be represented by another person, the Company performs an Identification of the Agent. Then, the Agent must submit the authorization to act (e.g. the original power of attorney or a copy of it with a certified signature of the principal, unless the authorization to act is identifiable from the public register). The Company shall verify whether and to what extent the person is authorised to act for the Client.

IV.8.ii. The Company then performs the Identification of the Client.

IV.9. PEP

IV.9.i. As part of Client Identification, the Company will determine whether the Client, the natural person acting for the Client in a given Business Relationship, and the Beneficial Owner of the Client, if known to the Company, is not a PEP.

IV.9.ii. Whether the Client is a PEP will be determined by the Client's declaration and a screening provided by Sumsub and it will be performed against commercially available databases to ascertain the truthfulness of the Client's declaration.

IV.10. Persons Subjects to International Sanctions

IV.10.i. As part of client Identification, the Company will determine whether:

a) the Client, the natural person acting for the Client in the Business Relationship and the Beneficial Owner of the Client, if known to the Company, is not a sanctioned person,

b) another person in the ownership or management structure of the Client, if known to the Company, is not a sanctioned person.

IV.10.ii. The Company obtains information on sanctioned persons via Sumsub

a) through the EU sanctions map published on the website www.sanctionsmap.eu,

b) through the EUR Lex application and

c) from ISM.

IV.10.iii. In the event of a partial match of any of the identification data with the data of a person on the mandatory sanction list, it is necessary to proceed as if it were a full match until it is clarified whether it is not a false hit based e.g. on the similarity of names.

IV.10.iv. When it is confirmed that a person is recorded on a sanctions list, an OPO is filed immediately, and the Business Relationship may only be commenced or continued if this is not contrary to the legislation based on which the sanction in question was imposed.

V. Due Diligence of the Client

V.1. Applicability of Due Diligence

V.1.i. The Due Diligence of Client is performed always prior to entering a Business Relationship with him or her. If no Business Relationship is concluded, the Company performs a Due Diligence of the Client should any of these conditions be fulfilled:

a) the value of the transaction outside the Business Relationship equals to or exceeds EUR 15 000,

b) the transaction is to be performed by a PEP or with a person established in a third country that is to be considered high-risk as defined in the Definition of Terms,

c) the transaction is to be performed by a person identified by means of Remote Identification,

d) when a Suspicious Transaction is detected,

e) when transferring assets in value of EUR 1 000 or more,

f) when a Business Relationship is established.

V.2. Process of Due Diligence

V.2.i. The Due Diligence of Client consists of the following procedures:

a) Client Due Diligence (see Section V.3)

b) Beneficial Owner Verification (see Section V.5)

c) Source of Funds Examination (see Section V.6)

d) Ongoing Monitoring (should there be an ongoing Business Relationship, see Section V.6).

e) Verification of the ownership and control structure in case of the Legal person.

V.2.ii. Once the Client is identified pursuant to Section IV, the Client Due Diligence pursuant to Section V.3 and Source of Fund Examination (see Section V.6) is performed. Then, should the Client be a legal person or a trust, a Beneficial Owner Verification (see Section V.5) is also performed.

V.3. Client Due Diligence

V.3.i. The Client Due Diligence includes:

a) obtaining and evaluating information about the purpose and intended nature of the Business Relationship to be able to determine later based on the Ongoing Monitoring that the use of services matches the stated intentions; this is done through a questionnaire,

b) obtaining and evaluating information about the nature of the Client's business, should the Client be an entrepreneur; this is done through a questionnaire,

c) ascertaining the identity of the Beneficial Owner should the Client be a legal person or a trust, this is done through a questionnaire and verified by the Company (see Section V.5), and

d) determining the ownership and management structure of the Client, should the Client be a legal person or a trust, this is done through a questionnaire and verified by the Company (see Section V.5).

V.4. Client Due Diligence shall not be carried out:

V.4.i. The Company will not carry out the Due Diligence of the Client if:

a) the performance of the Due Diligence or any part thereof could lead to the frustration or jeopardization of the OPO investigation or

b) the FAU instructs that the Due Diligence or any part thereof shall not be carried out on the grounds that the carrying out of the Due Diligence could frustrate or jeopardize an OPO investigation or ongoing criminal proceedings.

V.4.ii. All Employees are required to report to the Contact Person, via the Company's internal form or in person, their suspicions that there are conditions for an exemption from the Client's Due Diligence obligation under Article V.4.i. The Contact Person shall promptly verify that the conditions are met. In the event that the Contact Person concludes that those conditions have been met, the Contact Person shall inform the appropriate employees, that no Client Due Diligence will be conducted. Furthermore, the Contact Person shall decide whether the transaction should proceed despite this fact. The Contact Person shall state in the OPO, the circumstances and reasons for not carrying out the Due Diligence and the specific action within the Due Diligence or its part thereof that was not carried out by the Company.

V.5. Beneficial Owner Verification

V.5.i. The identity of Beneficial Owner is verified through a third party, namely the government public databases (such as Obchodní rejstřík or Evidence skutečných majitelů) are used.

V.5.ii. Should it not be possible to ascertain the identity of Beneficial Owner by the Company from these databases due to a fault of Client (e.g. a record is missing), the Business Relationship mustn't be established or has to be terminated or the Business Transaction mustn't be executed by the Company.

V.5.iii. Should it not be possible to ascertain the identity of Beneficial Owner because of objective reasons, the Company will use other means to ascertain the identity of Beneficial Owner of the Client, namely internet sources or certified documents provided by the Client issued by a government authority. Should it not be possible to ascertain the identity of Beneficial Owner by the Company from these resources, the Business Relationship mustn't be established or has to be terminated or the Business Transaction mustn't be executed by the Company.

V.5.iv. As part of the Beneficial Owner Verification, the Company also ascertains that the information on the ownership and management structure of the Client provided by him or her is correct by the same means described in Sections V.5.i - V.5.iii.

V.6. Source of Funds Examination

V.6.i. The source of funds to be used in the Business Relationship or a Transaction must be examined. This is done by a questionnaire.

V.6.ii. Should any suspicious arise to the truthfulness or relevance of the information provided by the Client, the Company will perform additional inquiry and it will require the Client to provide original of documents issued by third parties to support his or her statements.

V.7. Ongoing Monitoring

V.7.i. The Ongoing Monitoring consists of the following activities:

a) Beneficial Owner Verification,

b) whether transactions are actually related to the Client's business or usual income,

c) whether transactions are consistent with the Client's activities,

d) comparison of the activities of the Client to the local and personal aggregate data of the Clients.

V.7.ii. The Ongoing Monitoring procedures are performed at least once a calendar year should the Business Relationship be continuous.

VI. Enhanced Due Diligence of the Client

VI.1. The Company conducts Enhanced client Identification and Due Diligence in case that the Client or a Business Relationship poses an increased risk of money laundering or terrorist financing.

VI.2. Applicability of the Enhanced Due Diligence

VI.2.i. The Enhanced Due Diligence is applicable in the following cases:

a) at the inception and during a Business Relationship with a person with a country of origin in a high-risk third country,

b) prior to a transaction involving a high-risk third country,

c) prior to a transaction or entering into a Business Relationship with PEP, first identification of the Client has been carried out as remote, or

d) if the Client is determined as High Risk (see Section **Chyba! Nenalezen zdroj odkazů.**).

VI.3. Enhanced Due Diligence Measures

VI.3.i. In the course of Enhanced Due Diligence, the Company, to the extent necessary to duly manage the detected risk:

a) gathers additional documents or information,

b) verifies all documents or information received in several reliable sources,

c) monitors, on an ongoing and enhanced basis, the Business Relationship as well as transactions made as part of that Business Relationship,

d) obtains approval of a member of its governing body,

e) requires the first transaction as part of the Business Relationship or outside the Business Relationship be made from an account held in the Client´s name by a credit institution or by a foreign credit institution that has the duty to identify their Clients and perform Client Due Diligence at least to the extent comparable to the requirements stipulated by European Union law,

f) implements other measures corresponding to the nature of the obliged entity, its activities, and its own risk assessment process.

VI.4. High Risk Profile of the Client

VI.4.i. The Client is to be determined as a high risk if any of the following is true:

a) the Client or its Beneficial Owner is PEP, or they are acting in the benefit of PEP,

b) the Client has an opaque ownership structure,

c) the Client is not the natural person for which a business is executed,

d) the Client, which is a legal entity does not carry out any economic activity, or

e) a suspicion that a Beneficial Owner of the Client is covert.

VI.4.ii. A detailed categorisation of Clients with regard to their riskiness is given in the Evaluation of Risks Guideline.

VI.5. PEP Measures

VI.5.i. As part of Enhanced Due Diligence, the following procedures will be undertaken, should the Client or its Beneficial Owner be PEP, or they are acting in the benefit of PEP:

a) obtaining of additional documents or information about the Beneficial Owner, the intended nature of the Business Relationship or the source of the Client's and Beneficial Owner's money and other assets, and

b) obtaining a consent of a member of the statutory body for entering into and continuing with business relationship.

VII. Suspicious Transaction

VII.1. Demonstrative List of the Features of Suspicious Transactions

VII.1.i. the Client appears to be acting for or on behalf of someone else, is accompanied or followed by another person,

VII.1.ii. the Client carries out activities that may help to conceal his identity or the identity of the Beneficial Owner,

VII.1.iii. the Company has doubts about the truthfulness or completeness of the information obtained about the Client,

VII.1.iv. the identification cards have questionable appearance,

VII.1.v. the Client behaves nervously, refuses or is reluctant to be identified, or provides false information,

VII.1.vi. the Client has a criminal history or contacts or links to persons connected to criminal groups,

VII.1.vii. the Client is in a hurry to carry out the transaction more than is usual,

VII.1.viii. during one day or on the following days, the Client carries out noticeably more money transactions than is usual for his business,

VII.1.ix. assets handled by a Client are in obvious discrepancy with the nature and scope of its business or financial situation, transactions are made in amounts just below the threshold of mandatory client Identification or Due Diligence.

VII.2. Suspicious Transactions

VII.3. The following conduct of business will always be recognized as a Suspicious Transaction:

VII.3.i. The Client, a person in the ownership or control structure of the Client, the Beneficial Owner of the Client, a person acting on behalf of the Client or a person who is otherwise involved in the transaction is a person to which the Czech Republic applies sanctions according to Sanctions Act.

VII.3.ii. The subject of the business is or is intended to be goods or services against which the Czech Republic applies sanctions according to Sanctions Act.

VIII. Declined Transaction

VIII.1. The Company refuses to enter into a Business Relationship, or terminates a Business Relationship by the Company if:

VIII.1.i. the Client rejects the Identification,

VIII.1.ii. refuses to submit an authorisation if it is probable that he or she represents another person,

VIII.1.iii. fails to cooperate within the Due Diligence,

VIII.1.iv. the Identification and/or Due Diligence cannot be performed for other reasons,

VIII.1.v. the Company has doubts concerning accuracy of information or authenticity of documents provided within the Identification or Due Diligence or

VIII.1.vi. with a PEP or within a Business Relationship, if the origin of assets used in the transaction is unknown even after investigation conducted by the Company.

IX. Data Keeping

IX.1. The Company shall maintain for a period of 10 years from the year end of the execution of a transaction or termination of Business Relationship the following data:

IX.1.i. the identification data and other data obtained within the Identification process,

IX.1.ii. copies of documents provided for Identification, if such copies were taken,

IX.1.iii. data about who and when has performed Identification of the Client for the first time,

IX.1.iv. information and copies of documents received as part of the Client's Due Diligence,

IX.1.v. documents justifying the exemption from Identification and Due Diligence,

IX.1.vi. in case of representing the original or verified copy of power of attorney or a reference number of a court decision on appointment of a guardian,

IX.1.vii. records of all steps taken in the Identification and Due Diligence of the Client,

IX.1.viii. records of the process of assessment and determination of the risk profile of the Client.

IX.2. The period for data keeping shall start on the first day of a calendar year following the year of the last transaction known to the Company. Upon expiration of the period the relevant deletion of stored data and destruction of documents is executed.

IX.3. All data and documents will be stored by the Company in a way to prevent the deterioration of the stored information and documents and to ensure the ongoing monitoring of the Business Relationship. The data will be stored at the data warehouseso that this information is available to the regulatory authorities upon request within a reasonable period of time. In case of a request by a regulatory authority for access to such data, all necessary assistance will be promptly provided to such authorities by the Company's employees, in particular the Contact Person.

X. The Rules for Processing a Suspicious Transaction

X.1. The Company will report Suspicious Transaction in the following cases:

X.1.i. there are doubts about possible ML/FT persist even after the Client's Due Diligence,

X.1.ii. the Client refuses to Identify,

X.1.iii. the Client does not cooperate in obtaining data and information in the context of the Identification and/or Due Diligence,

X.1.iv. the Company does not know the origin of the assets from the public sources used in the PEP transaction and the origin is unclear even after the Company conducts an investigation, or

X.1.v. for other reasons as they may see fit, namely if any of the feature listed in Section VII.1 and VII.5 are present.

X.2. The Company shall report to the FAU the OPO whenever it fails to carry out the Due Diligence or its part. If the Company detects in relation with its business activity a Suspicious Transaction, such detection shall be reported to the FAU without undue delay. In certain circumstances, especially in danger of delay, the Company shall report the Suspicious Transaction immediately after its detection. The OPO shall be submitted in writing, in paper form by registered letter or electronically in a manner that ensures the confidentiality of the data transmitted.

X.3. The Company shall provide in OPO the identification data of a person who is the subject of the OPO, identification data of all other participants of the transaction available at the moment of filing the OPO, information about relevant circumstances of the transaction and any other information which may relate to the Suspicious Transaction and are relevant for its assessment.

X.4. The data about the employee or about the person persons working for the Company other than in a primary employment relationship who detected the Suspicious Transaction shall not be provided in OPO. The Company shall provide FAU the name and job title of the Contact Person or the person who processed the OPO.

X.5. Should an immediate execution of the Client's transaction thwart or significantly hinder seizure of proceeds of crime or funds intended for financing of terrorism, the Company shall execute the transaction order no sooner than 24 hours after the FAU received an OPO on such transaction.

X.6. The OPO shall be submitted to the FAU, either in writing by registered letter or orally on the record. A written notification shall also be deemed to be a notification submitted electronically via the FAU website.

X.7. Suspicious Transactions are reported to the Contact Person by the relevant employees of the Company via the Company's internal form or personally. It will be recorded and retained by the Contact Person even if the transaction is not suspicious. Investigation of possible suspected ML/FT will be carried out by the Contact Person without delay, up to a maximum of 24 hours from the time of the notification. The Contact Person shall have access to all information necessary to evaluate the Suspicious Transaction and shall have access to the information contained in the Company's information system. If the Contact Person identifies a Suspicious Transaction, it shall notify the FAU without undue delay. If the circumstances of the transaction require so, in particular if there is a risk of default, the Contact Person shall report the Suspicious Transaction immediately.

X.8. FAU Contacts:

X.8.i. Telephone: +420 257 044 501 or +420 603 587 66, FAX: +420 257 044 502, address for personal delivery: 1621/11 Washingtonova Street, 110 00 Prague 1, address for mail delivery: P. O. BOX 675, Jindřišská 14, 111 21 Prague 1, e-mail: fau@mfcr.cz (cannot be used for OPO submission), Data box no.: egi8zyh.

X.9. Essentials of the OPO:

X.9.i. OPO contains all information available to the Company about the transaction, its context and its participants, specifically:

c) identification data of the Company,

d) data of the person concerned by the OPO,

e) the identification details of all other participants in the transaction,

f) a detailed description of the subject matter and material circumstances of the Suspicious Transaction,

g) a notice in case that the notification also relates to property subject to international sanctions,

h) whether and when the transaction was executed or postponed, or the reason why it was or was not executed,

i) contact information of the Contact Person or person filling the OPO.

X.9.ii. The Company shall not inform the Client of filing the OPO.

X.10. Suspension of Client's Transaction

X.10.i. Client's transaction may be suspended according to Section X.5. In case that the suspension of client's transaction is not possible or if suspension could thwart or otherwise jeopardize the investigation of the Suspicious Transaction the transaction order is not suspended.

X.10.ii. Should there be a danger as set out in Section X.5, FAU may decide on extension of the suspension of client's transaction, but no longer than additional 2 working days, or on suspension of client's transaction or on seizure of assets which is subject of the Suspicious Transaction, for a period of up to 3 working days.

X.10.iii. The decision on the suspension of client's transaction or on seizure of assets shall become effective by its announcement. The announcement may be done orally, by phone, by fax or electronically; a written copy shall always follow. An appeal against the decision on the suspension of customer's transaction or seizure of assets shall not be allowed.

X.11. Information Duties

X.11.i. The identification details of the Contact Person are set out in Annex 1 to this Guidelines. The Company shall notify the Contact Person to FAU using the model form provided on FAU website.

X.11.ii. The Company shall comply with FAU's instructions within the time limit set by the FAU.

X.11.iii. The Company shall:

a) disclose to FAU details of Business Relationships and transactions related to the Identification obligation or Due Diligence,

b) submit to FAU documents about transactions or allow access to authorised FAU employees during the examination of the OPO and during the exercise of administrative supervision,

c) provide FAU with information about the persons who participated on the transactions.

X.11.iv. The Contact Person will provide the relevant data and supporting documents to the FAU immediately upon receipt of the instruction, primarily electronically, or, if this is not possible, in writing to the FAU address.

X.11.v. The Company informs the Clients about Company's obligation to process personal data for the purpose of preventing ML/FT.

XI. Staff Training

XI.1. The Company shall ensure that employees who may in the course of their work encounter Suspicious Transactions are trained at least once within 12 calendar months and that all employees are trained prior to being assigned to such positions. Persons who are involved in the Company's business other than in a basic employment relationship will also be trained.

XI.2. The training materials are regularly updated depending on the findings and changes obtained from the AML system. The records and content of the training are retained for a period of 5 years from the date of the training.

XI.3. The training shall include in particular typologies and indicators of Suspicious Transactions, requirements determined by the Company for the Identification and Due Diligence and procedures for detecting client’s risk factors and Suspicious Transactions.

XII. Final Provisions

XII.1. Despite the Company intends to conduct business solely with physical persons, this Guideline also includes provisions on the AML/CTF rules for legal persons and trusts should new products be tested.

XII.2. The Company and its employees and persons working for the Company other than in a primary employment relationship are obliged to keep confidential all facts relating to OPO and their investigation or fulfilment of information duties to FAU.

XII.3. The Company shall update the Guidelines at least once per calendar year and also before the expiry of this period if it is needed from the reason of the risk assessment, change in the Company's business activities or strategy and/or a change in legislation. The result of the assessment under the previous sentence shall be recorded and retained by the Company.

XII.4. This Guidelines shall enter into force on the date that it is signed by the statutory body for publication.