

Title:	MEASURES AGAINST THE LAUNDERING OF THE PROCEEDS OF CRIME
Internal Regulation No.:	1/2023
Contents:	Measures against money laundering and terrorist financing; application of the system to comply with international sanctions
Annexes:	Annex No. 1 – List of countries at risk and sanctioned persons Annex No. 2 – Template for notification to the Financial Analytical Office Annex No. 3 – Template for internal reporting Annex No. 4 – List of national functions of politically exposed persons
Intended for:	To all employees and workers of the company APF DIGITAL AGRIFUND CR s.r.o.
Created by:	Statutory body of the company
Approved by:	Statutory body of the company
Repeals Directive No.:	
Valid from:	05.04.2023
Effective from:	05.04.2023
Change No.:	
Annexes:	
Approved by:	
Valid from:	
Effective from:	

I. MEASURES AGAINST MONEY LAUNDERING AND TERRORIST FINANCING

1. Introduction

The company APF DIGITAL AGRIFUND CR s.r.o., ID No.: 143 47 296 (hereinafter the “**Company**”) is a legal person established in accordance with the relevant provisions of Act No. 90/2012 Coll., on Business Companies and Cooperatives (Business Corporations Act), as amended (hereinafter the “**Business Corporations Act**”). Within the scope of its business activities, it carries out, in accordance with Act No. 253/2008 Coll., on certain measures against the legalization of proceeds from crime and terrorist financing (hereinafter the “**AML Act**”) and in connection with Decree No. 67/2018 Coll., on certain requirements for a system of internal policies, procedures and control measures against the laundering of the proceeds of crime and the financing of terrorism (hereinafter the “**Decree**”), identifies and screens clients with whom it enters into business relations, monitors the nature, volume and other parameters of the transactions carried out by them, and thereby effectively prevents the laundering of the proceeds of crime and the financing of terrorism (hereinafter the “**money laundering**”) through the financial institution. The prerequisite is the continuous monitoring of Transactions, with emphasis on the frequency and extent of certain deviations from the client’s normal trading regime.

2. Purpose of the Internal Regulation

The Internal Regulation regulate the Company’s procedures to prevent money laundering through the Company, the fulfilment of information obligations to the Financial Analytical Office (hereinafter the “**FAO**”) and set out a system of policies and measures to prevent money laundering and the prevention of the financing of terrorism. In establishing the internal policies, the Company takes into account recognised standards, a summary of which is published by the FAO. The Internal Regulation also regulate the procedures leading to the implementation of the obligations under Act No. 69/2006 Coll., on the Implementation of International Sanctions (hereinafter the “**Act on the Implementation of International Sanctions**”) and Act No. 240/2013 Coll. on Investment Companies and Investment Funds (hereinafter the “**Investment Companies and Investment Funds Act**”).

3. Definition of certain terms

Client (client)

A natural or legal person with whom the Company has a Business Relationship on the basis of a concluded agreement on the entrustment of funds for the purpose of their joint investment (hereinafter the “**Agreement**”). The Company does not allow and the Client Officer is not entitled to execute the Client’s Transaction without a concluded Agreement.

Client Officer

A worker of the Company who deals with the Client at the conclusion of the Agreement, identifies the Client and communicates with the Client regarding the services provided.

Identification data

regarding a natural person: all names and surnames, national identification number and, if not assigned, date of birth and sex, place of birth, permanent or other residence and nationality;

regarding a natural person entrepreneur: all names and surnames, national identification number and, if not assigned, date of birth and sex, place of birth, permanent or other residence and nationality, business name, distinctive supplement or other designation, registered office and identification number;

regarding a legal person:

1. basic identification data of the legal person, which are the business name or name including a distinctive supplement or other designation, the registered office and the legal person's identification number or similar number assigned abroad,
2. data 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,

regarding a trust fund: its designation and the identifying information of its trustee, to the extent of the above identifying information.

If justified by a risk assessment pursuant to Section 21a of the AML Act, in addition to the identification data defined above, further identification data may be collected, such as, in particular, telephone numbers, e-mail addresses, employment or employer's data.

Legalization of proceeds of crime

conduct intended to conceal the illicit origin of any economic advantage resulting from criminal activity in order to give the appearance of a lawfully obtained financial benefit, such as:

- in the conversion or transfer of property knowing it to be the proceeds of crime, for the purpose of concealing or disguising its origin, or for the purpose of assisting a person engaged in the commission of such an activity to escape the legal consequences of their conduct;
- in concealing or disguising the true nature, source, location, movement or disposition of the property or a change in the rights relating to the property knowing that the property is the proceeds of crime;
- in the acquisition, possession, use or disposal of property knowing it to be the proceeds of crime, or;
- in a criminal conspiracy of persons or any other form of collaboration for the purpose of the conduct referred to in the paragraphs above.

It is irrelevant whether the aforementioned conduct occurred or is intended to occur in whole or in part in the Czech Republic or abroad.

Terrorist financing

- a) the collection or provision of funds or other property knowing that it will be used, even in part, to commit an act of terrorism, a terrorist attack or an offence intended to enable or facilitate the commission of such an offence, or to support a person or group of persons preparing to commit such an offence; or
- b) conduct leading to the granting of a reward or compensation to the perpetrator of an offence of terror, terrorist attack or an offence intended to enable or facilitate the commission of such an offence, or to a person close to the perpetrator, or the raising of funds for such reward or compensation;
- c) financing the proliferation of weapons of mass destruction, which means the collection or provision of funds or other property knowing that it will be used, even in part, by a proliferator of weapons of mass destruction or used to promote the proliferation of such weapons in violation of the requirements of international law.

It is irrelevant whether the aforementioned conduct occurred or is intended to occur in whole or in part in the Czech Republic or abroad

Opaque ownership structure

a situation where the beneficial owner of the client or the ownership and management structure of the

client cannot be ascertained from:

1. the public register, the register of trusts or the register of beneficial owners kept by a public authority of the Czech Republic,
2. a similar register or record of another state, or
3. any other source or combination of sources which the Company reasonably believes to be reliable and which the Company reasonably believes, taken as a whole, will provide complete and up-to-date information about the beneficial owner and the ownership and management structure of the client, in particular if it is issued by a public authority or officially certified.

A joint stock company or other legal person for which all the necessary documents are provided, but the beneficial owner cannot be verified from the public register or other public records, or the company's representative fails to provide an extract from the shareholders' register or other document containing reliable information on the beneficial owner of the client, will be classified under Profile No. 2 (risky client).

An opaque ownership structure does not apply if the client is a legal person whose securities are admitted to trading on a European regulated market or a foreign market equivalent to a European regulated market, provided that it is subject to disclosure requirements equivalent to those of European Union law.

A prospective client who has an opaque ownership structure and who does not already provide the necessary documentation to clarify the true owner of the client and its entire ownership structure when signing the agreement is classified under Profile No. 3 (unacceptable client) and will not be contracted.

Transaction

any conduct of the Company acting in the capacity of an obligated person under the AML Act with a client, if such conduct is aimed at the disposal of the client's property or the provision of a service to the client, e.g., the receipt of funds for the management of property. Where a payment is divided into several separate transactions, the value of the transaction or payment is the sum of the transactions or payments if they are related.

Business Relationship

a contractual relationship between the Company acting in the capacity of an obligated person under the AML Act and a client, the purpose of which is to dispose of the client's property or to provide services to the client, if it is clear at the inception of the contractual relationship, taking into account all the circumstances, that it will be ongoing or involve recurring performance. The conclusion of a third Transaction shall be deemed to be an obvious recurring performance. All of the Company's clients are in a Business Relationship. The Company does not conduct one-off Transactions.

Politically Exposed Person

- a) a natural person who holds or has held in the last 12 months a significant public office of national or regional importance (see Annex No. 4 for a list of such persons), or a natural person who holds or has held a similar office in another state, in a body of the European Union or in an international organisation,
- b) a natural person who
 1. is or has been in the last 12 months a person close to the person referred to in paragraph a),
 2. is or has been within the last 12 months a partner or Beneficial Owner of the same legal person or trust, as the person referred to in paragraph a), or is known to the Company to be in any other close business relationship with the person referred to in paragraph a); or

3. is or has been in the last 12 months the Beneficial Owner of a body corporate or trust known to the Company to have been created for the benefit of a person referred to in paragraph a).

The provisions regarding Politically Exposed Persons apply until the company has ruled out a risk specific to Politically Exposed Persons regarding the client based on a risk assessment. During this period, it shall also apply to the same extent to a client who is a legal person whose beneficial owner is a Politically Exposed Person and to a person known to the company to be acting for the benefit of a Politically Exposed Person.

Identity document

an identity card, passport, driving licence, or other document issued by a public authority, which shows the name and surname, date of birth, and from which the person presenting the document can be identified as its authorised holder.

In the case of a foreigner, only an ID card, passport or foreigner's residence permit is an acceptable Identity document.

For the purpose of proving the client's identity, an identity document which is damaged beyond the usual level of wear and tear (missing pages, glued, overwritten, illegible), an identity card bearing the owner's likeness, the appearance of which does not correspond to their actual form, or which is so indistinct or damaged, cannot be accepted, that it is not possible to identify the person with a sufficient degree of probability, a document from which it is not possible to determine unambiguously which authority of which state issued it, as well as a document which for other reasons raises doubts as to its authenticity, and a document which is found in a database of invalid documents cannot be accepted – <https://aplikace.mvcr.cz/neplatne-doklady/>.

In case of doubt about the authenticity of the Identity document, the Company is obliged not to carry out the given Transaction or refuse to establish a Business Relationship or terminate the existing relationship. Following this, the Company must assess whether the conditions for reporting a suspicious transaction pursuant to Article 10 of this Internal Regulation are not met.

Client's instruction

An act of the Client whereby the Company is to dispose of the client's property. For each Transaction, the Company/Client Officer must have a Client's instruction.

Sanctioned entity

A person who appears on any of the lists of sanctioned persons and persons suspected of cooperation and support for terrorism (Annex No. 1). Every client is subject to verification, and in the case of a legal person, also persons involved in its management or activities (members of the statutory body, beneficial owners, other participants in the relevant Transaction, e.g., persons authorised or in the Business Relationship. For each Client, a check shall be carried out regarding their possible registration in the sanction lists before the conclusion of the Business Relationship and then subsequently before each Transaction.

Beneficial owner

Beneficial owner means:

- a) the beneficial owner according to the Act on the Registration of Beneficial Owners (hereinafter the "Act on the Registration of Beneficial Owners"), it means
 - any natural person who ultimately owns or controls a legal person or legal arrangement
 - in the case of a corporation, any natural person who, directly or indirectly through another person or legal arrangement:
 - has a share in the corporation or a voting share greater than 25%,

- has a share of the profits, other own resources or the liquidation balance greater than 25%,
- exercises a controlling influence over a corporation or corporations that individually or collectively have a greater than 25%, or
- exercises a controlling influence over a corporation by another means
 - o Controlling influence in a corporation is exercised by a person who, at their own discretion, whether or not and on the basis of what legal fact, can directly or indirectly, through another person or legal arrangement, cause the decision of the highest body of the corporation to conform to their will.
 - o Controlling influence in a corporation is exercised by a controlling person pursuant to the Act regulating the legal relations of business corporations.
 - o Controlling influence in a corporation other than a business corporation, a housing or social cooperative or an investment fund in the legal form of a joint-stock company with variable share capital is exercised by any natural person who is a member of their statutory body or a person in a similar position or a person representing a legal person in that body.
- is in the top management of the business corporation (the person who ensures the day-to-day management of the company or a direct member of the statutory body) and the conditions according to Section 5(1) of the Act on the Registration of Beneficial Owners;
- in the case of a foundation, institute, charitable company or legal arrangement, any natural person who exercises a controlling influence therein
 - o Controlling influence in a foundation, institute, charitable company is exercised by a person who, at their own discretion, whether or not and on the basis of what legal fact, can directly or indirectly, through another person or legal arrangement, cause the decision of the statutory or other body to conform to their will.
 - o Controlling influence over the administration of a legal arrangement is exercised by the person who, by virtue of their own discretion, regardless of whether and on the basis of what legal fact, can directly or indirectly, through another person or through the legal arrangement, make the decisions of the trustee conform to their will.
- in the case of a foundation, also each natural person who:
 - is its founder,
 - is a member of its administrative or supervisory board, or its auditor, or a person in a similar capacity;
 - in the personal support of whom, according to the founding legal act of the foundation, its purpose lies.
- in the case of an institute or a charitable company, also each natural person who:
 - is its founder,
 - is its directors or a member of its administrative or supervisory board, or a person in a similar capacity,
- in the case of a trust, also each natural person who:
 - is its founder,
 - is its trustee,
 - is empowered to supervise the administration of the legal arrangement and who may appoint or remove the beneficiary,
 - is its beneficiary,
 - is from the circle in whose interest the trust was established or is administered,

- if there is not any beneficiary,
b) the natural person for whom the Transaction is carried out.

Information about the beneficial owner is collected through the contract or the AML questionnaire, which is filled in when signing the agreement with the client.

Country of origin

for

1. a natural person, each state of which that person is a national and, at the same time, all other states in which they are registered to reside for more than 1 year or to reside permanently, if known to the Company,
2. a natural person carrying on business, the state referred to in point 1, and at the same time the state in which they have their registered office, if known to the Company,
3. a legal person which is subject to obligations under Section 24a of the AML Act or equivalent obligations under the law of another state, the state in which it has its registered office,
4. a legal person which is not subject to obligations under Section 24a of the AML Act or equivalent obligations under the law of another state, the state in which it has its registered office and, at the same time, all the states in which it has a branch,
5. a trust, the state under the law of which the trust is established and any state of which the trustee or person in a similar capacity is a national or in which the trustee is domiciled and, at the same time, if known to the institution, any other states in which the trustee or person in a similar capacity is registered to reside for more than one year or to reside permanently.

Higher risk country or country at risk

Country listed in Annex No. 1, = client with the Risk Profile No. 2 or No. 3.

Tax haven

Country on the European Council list:

<https://www.consilium.europa.eu/media/31945/st15429en17.pdf>. = client with the Risk Profile No. 2 or No. 3.

Agreement

Agreement on the entrustment of funds for the purpose of joint investment

Assigned officer

Worker of the Company assigned to a specific task.

Responsible person

Worker responsible for a specific task.

Contact person

The person designated by the Company to fulfil the reporting obligation and to ensure ongoing liaison with the FAO.

4. Obligation to identify clients

The Company will always make the identification at the beginning of the contractual relationship, i.e., at the time of signing the agreement, and whenever there is a suspicious transaction or if it is clear that the value of the Transaction exceeds EUR 1,000.

5. Methods of client identification

5.1. Face-to-face identification

The initial identification of a client who is a natural person, and if a legal person or a trust on whose behalf the natural person is acting, shall be made by a Client Officer of the Company in the physical presence of this person. Exceptions to this rule are set out below.

5.1.1. Identification of the client who is a natural person

When concluding a Business Relationship or executing a Transaction with a Client – a natural person, the Client Officer of the Company shall identify the Client by recording and verifying the Client's Identity Document (i.e. The Client's name, surname, birth number and, if not assigned, date of birth and sex, place of birth, permanent or other residence and nationality; in the case of a natural person engaged in business, also their business name, distinctive supplement or other designation, registered office and identification number) and records the type, number of the Identity Document, the state or authority that issued it and the period of its validity, at the same time verifying the conformity of the person's appearance with the depiction in the Identity Document. If the Identity Document does not contain all the necessary Identification Data, another document or certificate – typically a combination of a passport (does not contain an address) and a residence permit (contains an address) – is usually used as a supporting document.

As part of the identification of the client, the Client Officer shall further determine and record in the Company's AML questionnaire whether the client or the person acting on behalf of the client is not a Politically Exposed Person or a person against whom the Czech Republic applies international sanctions pursuant to the Act on the Implementation of International Sanctions.

5.1.2. Identification of the client who is a legal person or a trust

When entering into a Business Relationship or executing a Transaction with a Client – a legal person, the Company's Client Officer shall identify the Client as follows:

- record and verify from a document of existence of the legal person obtained from a reliable source the Identification Data of the legal person (business name or name including a distinctive addition or further designation, registered office, identification number or similar number assigned abroad);
- identify the natural persons (e.g., the statutory body or a member thereof) who act for the legal entity in a given Transaction or in the establishment of a Business Relationship with the Company by recording and verifying from the Identity Document, if any, the Identification Data of the natural person (i.e., all names, surname, birth number and, if not assigned, date of birth and sex, place of birth, permanent or other residence and nationality) and record the type, number of the Identity Document, the state or authority issuing it and the period of validity of the Identity Document, while at the same time verifying that the person's likeness matches the representation on the Identity Document;
- identify the natural persons who are members of the statutory body of a legal person but do not act within the framework of the Business Relationship in question, the data of such persons are ascertained and recorded to establish and verify their identity. These data are those that can be obtained from available sources, typically the commercial register, i.e., in particular name, surname, date of birth and address.

If the statutory body, its member or controlling person of the client is another legal person, it shall be identified in the same way as the client itself.

As part of the client identification process, the Client Officer will also determine and record whether:

- a) the client, the natural person acting on behalf of the client in a given Transaction or Business Relationship and its beneficial owner, if known to the Company, is not a Politically Exposed Person or a person against whom the Czech Republic applies international sanctions pursuant to the Act on the Implementation of International Sanctions,
- b) another person in the ownership or management structure of the client, if known to the Company, is not a person against whom the Czech Republic applies international sanctions under the Act on the Implementation of International Sanctions.

When first identifying a client who is a trust, the Company's Client Officer shall identify the client by recording and verifying from a document of trust existence obtained from a reliable source the Identification Data of the natural person who is acting for the trust in a given Transaction or at the inception of the Business Relationship. It shall record these details from the Identity Document.

Obtaining a copy of the Identity Document

When identifying a natural person (a Client or a person acting in a given Transaction or when a Business Relationship is established on behalf of a client) whose Country of Origin is the Czech Republic, the Identification Data is obtained on a priority basis by obtaining a copy of the relevant parts of the identity document from which the Identification Data can be obtained, as well as the type and number of the identity document, the country or authority that issued it and the period of its validity. When identifying a natural person (a client or a person acting in a given Transaction or when a Business Relationship is established on behalf of a client) whose Country of Origin is not the Czech Republic, the Identification Data shall be obtained by obtaining a copy of the relevant Identity Document as a priority.

In the event that the natural person does not give the Company consent (even implied consent is sufficient) to make a copy of the Identity Document, the Company's Client Officer performing the identification shall make a copy of the Identification Data to the extent provided for in this Internal Regulation.

The copy (scan) of the Identity Document shall be made in written form in such a way that the relevant Identification Data is legible and can be preserved for the period of time specified in this Internal Regulation and shall contain a copy of the representation of the identified natural person in such quality as to enable verification of the conformity of the likeness.

The Company's Client Officer who has identified the client is obliged to record this fact in the Company's information system and to indicate and confirm it with their handwritten signature in the relevant contractual documentation (especially in the AML questionnaire), which is the basis for the establishment of the Business Relationship between the Company and the client.

5.2. Client identification when concluding distance agreements

The Company may substitute for identification in the physical presence of the client by identifying the natural person who is the client, or the natural person acting for the client, by:

- a) for the client who is
 1. a natural person, sends the Company copies of the relevant parts of the identity document and at least one other supporting document (e.g., passport, driving licence, health insurance card, birth certificate, marriage certificate) from which the Identification Data can be ascertained,
 2. a legal person, sends the Company proof of its existence and its Identification Data or the Company obtains the existence and Identification Data of the client from the public register or the register of trusts,

3. a trust, sends the Company proof of its existence and its Identification Data,
- b) in the event that another person acts for the client, the client shall send copies of the documents referred to in paragraph (a)(1) to the natural person authorised to act for the client in this Transaction or Business Relationship and the authorisation of that natural person to act for the client,
 - c) the Company shall record and verify the details and authorisations sent under (a) and (b) and shall have no doubt as to the true identity of the client or the person acting for the client,
 - d) the Company shall enter into a Business Relationship Agreement with the client, the contents of which shall be recorded in text form,
 - e) the client provides credible evidence of the existence of a payment account in his name with a credit institution or a foreign credit institution operating in the territory of a member state of the European Union or a state forming the European Economic Area,
 - f) the first payment under this Agreement shall be made by the client through the account referred to in paragraph (e), and
 - g) where the payment system permits, the payment shall be accompanied by information identifying the purpose and designation of the Company, together with the name of the natural person who gave the order for payment in accordance with point (f); where the client is a natural person for whom no other person is acting and where the risk assessment under section 21a so justifies, a copy of the supporting document referred to in point (a)(1) need not be sent if the payment is accompanied by this information.

The choice of the second identity document is made by the Company taking into account the risk assessment for the specific case.

The Client Officer shall verify whether the above conditions are met and whether, according to the information available to them, any of the clients, any of the products or any particular Transaction poses an increased risk of misuse for money laundering or terrorist financing, which is assessed in particular on the basis of the information in the agreement, the AML questionnaire and the client's check of the relevant sanction lists (see Annex No. 1 to this Internal Regulation).

Copies (scans) of all Identity Document and other documents must be made in such a way that the relevant Identification Data is legible and can be retained for the period of time specified in this Internal Regulation and must contain a copy of the image of the identified natural person in such quality as to enable verification of the conformity of the image.

Client identification by remote means shall only be applied to clients, products or specific Transactions in the sense of low risk. Low risk means a client who is classified under Risk Profile No. 1 (see Chapter 7. Risk assessment and Client risk profile: 7.3 Client risk profiles). The distance client identification procedure does not apply if the client is a Politically Exposed Person.

Distance client identification is not possible for clients whose domicile, permanent residence or country of origin is a country that does not adequately apply measures against money laundering and terrorist financing, i.e., a country listed in Annex No. 1 to this Internal Regulation and flagged as 2.

5.3. Electronic identification

The Company does not provide electronic identification.

5.4. Acceptance of client identification by a credit or financial institution

The Company does not accept any client identification by a credit or financial institution .

5.5. Common provisions on client identification

Politically Exposed Persons

As part of the client identification process, the Client Officer shall determine whether the client, the natural person acting on behalf of the client in a given Transaction or Business Relationship and the beneficial owner of the client, if known to the Company, is a Politically Exposed Person. They shall do this by verifying that the Client has completed the answer to the question whether or not they are a Politically Exposed Person in the agreement or AML questionnaire. The Client Officer shall also determine whether the person is a Politically Exposed Person:

1. using the national list of politically exposed persons (see Annex No. 4),
2. using own investigation (e.g., using open sources of information, Central Register of Notifications, see <https://cro.justice.cz/>),
3. where appropriate, using a system for screening and tracing “risky” clients based on information from public sources and provided as a paid service by some specialised business entities.

The Company does not rely solely on the client’s statement and verifies the information from the client. In the event that the client is a Politically Exposed Person, the Client Officer shall conduct enhanced identification and verification of the Client in accordance with Article 5.7. and further inquire about the source of funds (or other assets) used in the Transaction and determine the origin of the Politically Exposed Person’s assets. The Client Officer is then obliged to record this information for the Transaction being executed and to ask the statutory body for consent to the transaction before executing the Transaction. The client shall answer these questions in writing in a questionnaire submitted to the client by the Client Officer.

The Company is required to regularly update information relating to the identification and assessment of risk in relation to clients who are Politically Exposed Persons. The Company is obliged to verify periodically whether the Politically Exposed Person status is still valid or whether any of the existing clients has become a Politically Exposed Person during the course of the business relationship by always sending out an inquiry at least after the elections (regional, senate, Chamber of Deputies and presidential elections) whether there has been such a change in the client that they have become or ceased to be a Politically Exposed Person.

Obligations and restrictions relating to Politically Exposed Persons shall continue to apply to the Company for at least 12 months from the date on which the Politically Exposed Person ceases to hold the relevant office; however, in any event until the obliged person has eliminated the politically exposed person-specific risk for the client on the basis of a risk assessment. During this period, it shall also apply to the same extent to a client whose beneficial owner is a Politically Exposed Person and to a person known to the Company to be acting for the benefit of a Politically Exposed Person.

Sanctioned entity

As part of the identification process, the Client Officer shall ascertain and record whether the client, the natural person acting on behalf of the client in the relevant Transaction or Business Relationship and the beneficial owner of the client, if known to the Company, or any other person in the ownership or management structure of the client, if known to the Company, is on the list of sanctioned entities and persons suspected of cooperation with and support for terrorism, and likewise, whether, in the case of a legal person, persons involved in its management or activities (members of the statutory body, beneficial owners, other participants in the Transaction or Business Relationship) are also on this list and whether they are from a state subject to international sanctions (see Annex No. 1). The check is carried out at the conclusion of the Business Relationship and then subsequently before each Transaction. Both new and existing clients and all persons acting on behalf of a person or their beneficial owners are subject to the check.

Identification of the client's representative

If the client is represented at the commencement of the Business Relationship or execution of an individual Transaction on the basis of an authorisation pursuant to Section 8 (4) - (6) or Section 11 (7) of the AML Act, the identification of the representative is carried out in the same manner as the identification of the client and furthermore by presenting an authorisation issued by the client which contains the officially certified signature of the principal. The authorisation shall become an integral part of the documentation kept by the Company with the client.

Identification of the legal representative or guardian

If a legal representative or guardian acts on behalf of the client, the Client Officer shall identify the legal representative or guardian in the same manner as the identification of a natural person client. The person acting on behalf of the client is required to provide the client's identification data, provided that the physical presence of the represented person is not required.

If another person acts on behalf of the client, that person must provide proof of authorisation to act, unless the authorisation to act is ascertainable from the public register. The Client Officer shall verify whether and to what extent that person is authorised to act for the client.

Throughout the duration of the Business Relationship with the client, the Company's Client Officers shall check the validity and completeness of the information obtained as part of the identification and verification of the client and record any changes thereto. In determining the frequency and extent of such checks, the Client Officer shall base the client's risk profile.

If the Client Officer of the Company suspects at the conclusion of the Business Relationship or during the course thereof that the client is not acting on their own behalf or that they are trying to conceal that they are acting for a third party, they shall call upon the client to provide evidence of authorisation pursuant to Section 8 (4) - (6) or Section 11 (7) of the AML Act.

On further Transactions with the client who has already been identified, or if another person is acting on behalf of the client if both the client and the natural person acting have already been identified, the Client Officer shall verify the identity of the client or the natural person acting in an appropriate manner.

Detection of a discrepancy

If the Client Officer reasonably believes that in the course of the identification or verification of the client they have discovered an irregularity under the law governing the registration of beneficial owners (hereinafter the "discrepancy"), they shall notify the client thereof. In the notice, the Client Officer shall state the nature of the discrepancy. If it is reasonable to do so in the circumstances, the Company will allow the client to comment on the discrepancy.

If the client fails to rectify or refute the discrepancy without undue delay after being notified, the Client Officer shall report the discrepancy to the AML Officer, who shall then report the discrepancy to the court having jurisdiction over the discrepancy under the law governing the registration of beneficial owners.

The notification of the discrepancy to the AML Officer and subsequently to the court shall be supported by the facts or documents evidencing the discrepancy and the client's statement, if any.

5.6. Simplified client identification and check

The Company does not perform any simplified client identification and check.

5.7. Enhanced client identification and check

During the enhanced identification and check, the Company to the extent necessary to effectively manage the identified risk beyond the measures applied during client identification and check:

- a) shall obtain additional documents or information on
 - i. a beneficial owner,
 - ii. intended nature of the Business Relationship, and
 - iii. the sources of the client's and beneficial owner's cash and other assets,
- b) shall verify the documents or information obtained from multiple trusted sources,
- c) shall regularly and intensively monitor the Business Relationship and the Transactions within the Business Relationship,
- d) shall obtain the consent of a member of its statutory body or a person authorised by it to manage in the area of measures against money laundering and financing of terrorism to conclude the Business Relationship or to continue it,
- e) shall require the first payment to be made under the Business Relationship or from an account held in the name of the client with a credit institution or a foreign credit institution which is subject to client identification and check obligations at least equivalent to the requirements of European Union law, or
- f) shall take other measures having regard to the nature of the Company, its activities and its own risk assessment.

Enhanced identification and check shall be applied always:

- at the inception and during the course of the Business Relationship with a person established in a high-risk third country (at least the measures under (a) to (d) and (f)),
- before executing a Transaction related to a high-risk third country (at least the measures under points (a) to (d) and (f)),
- before executing a Transaction or when entering into a Business Relationship with a Politically Exposed Person (at least the measures under point a) iii. and points c) and d)),
- when the client, Transaction or Business Relationship presents an increased risk of money laundering or terrorist financing based on a risk assessment.

6. Client check

The Company is obliged to carry out a check on the client:

- a) Before executing the Transaction outside the business relationship,
 - i. no later than the time when it is apparent that it will reach a value of EUR 15,000 or more, or the equivalent in another currency,
 - ii. with a Politically Exposed Person,
 - iii. with a person established in a country which, by virtue of a designation by the European Commission or otherwise, is to be regarded as high risk,
 - iv. with a person identified in accordance with Section 11(7) of the AML Act,
- b) Before executing a transaction with the characteristics of a suspicious transaction, irrespective of the threshold for such a transaction,
- c) Before the establishment of the Business Relationship (e.g., conclusion of an agreement),
- d) During the Business Relationship.

If a payment is split into several separate transactions, the value of the Transaction is the sum of the transactions if they are related.

The client shall provide the Client Officer with the information necessary to carry out the check, including the submission of relevant documents. The Company may, for the purposes of this Act, make copies or extracts of the documents submitted and process the information so obtained to fulfil

the purposes of the AML Act. Information about the client is recorded by the Client Officer in the Company's business system. In the event that the client refuses to cooperate, the Company will refuse to execute the Transaction or conclude the Business Relationship and will notify the AML Officer of this fact at the same time.

As part of the client check, the Company identifies and evaluates:

- a) client's identification data;
- b) information about the purpose and intended nature of the Business Relationship with the client and information about the nature of the client's business;
- c) the identity of the beneficial owner and taking measures to verify the identity of the beneficial owner from reliable sources, provided that if the client is subject to registration in the register of beneficial owners or a similar register, the Company shall always verify the beneficial owner from at least that register or a similar register and one other source, and determine whether the beneficial owner is a Politically Exposed Person or a person against whom the Czech Republic applies international sanctions pursuant to the Act on the Implementation of International Sanctions; if the Company does not identify the beneficial owner, it shall automatically assign the client the Risk Profile No. 2;
- d) if the client is a legal person or a trust, ascertaining the ownership and management structure of the client, and ascertaining whether the person in this structure is a person against whom the Czech Republic applies international sanctions pursuant to the Act on the Implementation of International Sanctions;
- e) information necessary to conduct ongoing monitoring of the Business Relationship, including reviewing Transaction executed during the course of the Business Relationship to determine whether the Transaction executed are consistent with what the Company knows about the client and its risk profile;
- f) information on the source of funds for the Transactions;
- g) within the framework of the Business Relationship with the Politically Exposed Person, also reasonable measures to ascertain the origin of their assets (the origin can be ascertained through an affidavit, a tax return or an extract from the Central Register of Notifications).

The Company collects the above information to the extent necessary to assess the potential risk of Money Laundering and Terrorist Financing depending on the type of client, type and scope of the service or product provided. The AML Officer will explain and justify to the client the extent of the client's check, taking into account the risks to the client.

The above information is collected mainly through the client AML questionnaire, which is an annex to the agreement, and also on the basis of any questions from the Client Officer to the client. During the course of the Business Relationship, the above information is obtained from the Company's information system and from information provided and documented by the client.

7. Risk Assessment and Client risk profile

7.1. General procedure for determining the client's Risk Profile in relation to risks

On the basis of the information obtained during the identification and check of the client, the Company shall categorize the clients in terms of the risk of Legalization of Proceeds of Crime and Financing of Terrorism, determine the conditions under which it shall not enter into a Business Relationship with the client or shall terminate an existing Business Relationship with the Client and determine the **client's Risk Profile** for each client on the basis of the **risk factors** listed below, the identification of which for new clients, the ongoing identification during the duration of the Business

Relationship with the client and the procedure to be followed with respect to clients for whom a risk factor has been identified, the Company hereby determines.

The risk profile of the client is determined through the agreement and the AML questionnaire. These documents are presented to each new client in order to provide a wealth management service comparable to co-investment management.

Risk level		Probability of occurrence	
non-serious	1	unlikely	a
medium serious	2	medium probable	b
serious	3	probable	c

The client's risk profile is evaluated by the Client Officer. In the event that any of the risk factors under Article 7.2 below are present during the assessment of the client's Risk Profile, the Risk Profile must be determined by the AML Officer. The AML Officer shall communicate the client's assessed Risk Profile to the Client Officer, the Client Officer shall enter the client's Risk Profile on the client's card in the Company's information system.

The Company carries out, through automated procedures in the Company's information system and random checks, active testing of clients and Transactions for the occurrence of risk factors, also during the course of the Business Relationship, see further Article 7.4.

In assessing risks, the Company takes into account:

- a) a national risk assessment prepared in accordance with Section 30a of the AML Act;
- b) the European risk assessment prepared by the European Commission;
- c) methodical and interpretative materials and decisions of the CNB and FAO;
- d) information provided by the FAO and law enforcement authorities;
- e) information obtained in the identification and checks of clients.

7.2. Risk categorisation of client types with regard to risk factors

Risk factors when entering into a Business Relationship:

- a) the beneficial owner of the client cannot be identified (3b);
- b) unclear purpose and reason for entering into the Business Relationship (2a);
- c) unclear origin of the client's funds (the client declares the origin of the funds e.g., as a cash win in a casino, receipt of a gift – cash, etc.) (2a);
- d) they use transactions that could facilitate anonymity (2a);
- e) the company not engaged in economic activity (2a);
- f) the client is a company based in the so-called off-shore zones (Tax havens) (2b);
- g) the client is directly or indirectly controlled by a person based in the so-called off-shore zones (Tax havens) (2b);
- h) the registered office of the client or of the person directly or indirectly controlling the client is located in an office house (formal relocation of corporate headquarters to large cities and large office houses, especially to Prague). The aim is to delay as far as possible the inspections of the territorial tax authorities) (2b);
- i) a fact giving rise to the suspicion that the client is not acting on their own account or that they are concealing that they are following the instructions of a third party (3a);
- j) contact details are identical for multiple accounts of multiple clients (2a);
- k) the client, or a person acting on behalf of the client, is registered as a permanent resident at the address of an authority (2a);

- l) the Business Relationship is conducted under unusual circumstances (2a);
- m) the client is located in a higher risk geographic area, see below (2b);
- n) the legal person or trust is a personal asset holding vehicle (2a);
- o) the client is a corporation in which there may be authorized shareholders or members or which issues shares in bearer form (2b);
- p) the ownership structure of the client appears unusual or overly complex given the nature of its business (2b);
- q) the client's business: purchase/sale of weapons, ammunition, trading in military material (3a), trading in dangerous substances (3a), gambling houses, casinos, bazaars and pawnshops (2a);
- r) the client, beneficial owner, person representing the client or any person in the management or ownership structure of the client is on the sanctions lists of the Czech Republic, EU, OFAC (Annex No. 2) (3a) or
- s) other facts indicating that the client is conducting a suspicious transaction.

In addition, factors when entering into a Business Relationship with **increased risk**:

- a) the fact that any of the client's countries of origin or the country of origin of the beneficial owner of the client or of a person acting on behalf of the client is a country which does not sufficiently or at all apply measures against money laundering and terrorist financing, or a country which the Company considers, on the basis of its assessment, to be a risk (see Annex No. 1);
- b) the fact that any of the client's countries of origin, or the country of origin of the beneficial owner of the client or a person acting on the client's behalf, is a state subject to sanctions, embargoes or similar restrictive measures (see Annex No. 1);
- c) the fact that any of the client's countries of origin, or the country of origin of the beneficial owner of the client or a person acting on the client's behalf, is a country that has been identified by credible sources as having a significant level of corruption or other criminal activity (see Annex No. 1);
- d) the country of origin of the person with whom the client conducts the Transaction is a country that does not sufficiently or at all apply measures against the laundering of proceeds of crime and terrorist financing, or is a country that the Company, based on its assessment, considers to be a risk;
- e) the registration of the client, the beneficial owner of the client or the person with whom the client transacts business on the list of persons and movements against whom sanction measures are applied;
- f) the Business Relationship is conducted under unusual circumstances;
- g) the client uses products or transactions that could facilitate anonymity;
- h) the client uses cash extensively in its business activities;
- i) the legal person or trust is a personal asset holding vehicle;
- j) the fact that, according to the information available to the Company, there is an increased risk of laundering the proceeds of crime or terrorist financing associated with the client's business;
- k) the ownership structure of the client appears unusual or overly complex given the nature of its business;
- l) the ownership structure is opaque
- m) the subject matter of the client's activities is associated with increased risk.

The level of risk varies from factor to factor, and some of them (such as unclear origin of funds, or inclusion of clients on a sanctioned list) are considered features of suspicious transactions.

The risk profile of the client is determined by the procedure according to Article 7.1. above.

Risk factors may also be identified by inspection during the course of the Business Relationship. The method of conducting the inspection and its frequency is set out in Article 6 or 7.4.

Risk factors within the duration of the Business Relationship and individual Transactions

The Company controls risk factors during the duration of the Business Relationship. Clients are required to report changes that are contained in the contract and AML questionnaire. During the course of the Business Relationship, the Company may also assign the status of Risk Client to a client who was identified as risk-free at the conclusion of the Business Relationship, move the client to a higher Risk Category, or assess the client as unacceptable. Such classification or reclassification is made on the basis of a determination of the client's riskiness if the following risk factors are identified for the client:

- a) the Country of Origin of the client or the Country of Origin of the Beneficial Owner of the client or of a person acting on behalf of the client changes to a country that does not sufficiently or at all apply measures against money laundering and terrorist financing, or to a country that the Company, based on its assessment, considers to be at risk;
- b) there is a change in the Country of Origin of the person with whom the client conducts the Transaction, where such new domicile is a country that does not sufficiently or at all apply measures against the laundering of proceeds of crime and terrorist financing, or is a country that the Company, based on its assessment, considers to be at risk;
- c) the client, the Beneficial Owner of the client, a person acting on behalf of the client, the ultimate recipient of the subject matter of the Transaction or the Beneficial Owner of a person with whom the client executes a Transaction or a person with whom the client executes a Transaction is entered on the list of persons and movements against whom sanction measures are applied;
- d) the ownership structure of the client becomes opaque (the ultimate owner – a natural person – cannot be identified);
- e) the registered office of the client or of a person directly or indirectly controlling the client is moved to an offshore zone;
- f) the registered office of the client or a person directly or indirectly controlling the client is moved to an office house;
- g) the company ceases economic activity;
- h) a fact giving rise to suspicion that the client is not acting on their own account or that they are concealing that they are following the instructions of a third party; and
- i) other facts indicating that the client is conducting a suspicious transaction.

In addition, there are factors in the duration of the Business Relationship with **increased risk**:

- a) the Country of Origin of the client or the Country of Origin of the Beneficial Owner of the client or of a person acting on behalf of the client changes to a country that does not sufficiently or at all apply measures against money laundering and terrorist financing, or to a country that the Company, based on its assessment, considers to be at risk (see Annex No. 1);
- b) there is a change in the Country of Origin of the person with whom the client conducts the Transaction, where such new domicile is a country that does not sufficiently or at all apply measures against the laundering of proceeds of crime and terrorist financing, or is a country that the Company, based on its assessment, considers to be at risk;
- c) the client, the Beneficial Owner of the client, a person acting on behalf of the client, the ultimate recipient of the subject matter of the Transaction or the Beneficial Owner of a person with whom the client executes a Transaction or a person with whom the client executes a Transaction is entered in the list of persons and movements against whom sanction measures are applied;
- d) the Business Relationship is conducted under unusual circumstances.

During the term of the Business Relationship, the client is obliged to inform the Company of any changes specified in the agreement and the AML questionnaire (e.g., change of identification data, etc.). Based on the Company's notification or its own findings, the Client Officer responsible for the client's Business Relationship is obliged to evaluate the new information and, if applicable, the new Risk Factor and proceed in a similar manner as when concluding the Business Relationship.

Risk factors within the duration of the Business Relationship are controlled mainly through the Company's information system, information updates and spot checks. The person responsible for the control is the Client Officer.

7.3. Risk profiles of clients

Based on the above risk factors, the Company distinguishes the following AML profiles of clients:

Profile No. 1 – non-risk (client) profile – clients who do not exhibit risk characteristics in terms of AML risk factors when establishing a Business Relationship (conclusion of an agreement) and during subsequent business cooperation.

Profile No. 2 – risk (client) profile – clients who have been identified as having one or more risk factors when filling in the AML questionnaire and signing the agreement, which, however, do not preclude the establishment of a Business Relationship after evaluation. For these clients, increased monitoring of trading activities must be carried out by the responsible persons (this includes, in particular, a more detailed determination of the origin of the sources of each Transaction, ascertaining the details of the risk factor in question, both by means of the client's declaration and by verifying the facts from public sources) in order to detect deviations and possible signs of suspiciousness. For these clients, the client questionnaire (AML questionnaire) is also updated more frequently, after 12 months.

Profile No. 3 – unacceptable (client) profile – clients with one or more risk factors which, after evaluation of the AML questionnaire, lead to the conclusion that the client is unacceptable in terms of AML measures. A Business Relationship must not be concluded with the client.

Each new Business Relationship is considered individually in relation to the documents submitted, the type of client, the purpose of the Transaction, the regularity and length of cooperation with the Company, the value of the Transaction, the client's representations, generally available information and other documents or references from other sources.

The Client Officer shall enter this fact into the information system for a client for whom one or more risk factors have been identified. In the event that a risk factor is identified for a client, it is reported to the AML Officer who, together with the Client Officer, assesses the risk factor and assigns the client a Risk Profile No. 2 or 3. The occurrence of multiple risk factors in a client and the assignment of Risk Profile No. 2 will result in the client being placed on increased monitoring of the Business Relationship by the Internal Control Unit. The Client Officer and the AML Officer will thus assess each individual case in the context of the supporting documents, the type of client, the purpose of the Transaction, the regularity and duration of the Business Relationship, the type of product, the value and method of settlement of the Transaction, the client's representations, generally available information and supporting documents, and references from other sources, where appropriate, while also considering the factors of increased risk. In particular, the AML Officer will consider the client's position and the client's potential business and the potential for misuse of the Company's services. The final assessment of the client's Risk Profile (Risk Profile No. 2 and 3) is the responsibility of the AML Officer. Their decision can only be changed by the Company's statutory body. A client against

whom the Czech Republic applies international sanctions of a financial nature is always included in Risk Profile No. 3.

The AML Officer shall identify and assess the risks of Money Laundering and Terrorist Financing that may arise in the Company's operations and reflect them in this Internal Regulation.

Higher requirements are placed on the risk client in terms of the requirement to provide supporting explanations and documents in the event that some of the characteristics of a suspicious transaction are present. The specific requirements for explanations and additional documents are determined on an individual basis as directed by the AML Officer.

In the event that the Company enters into a Business Relationship with a foreign person, the Client Officer shall always request the assistance of the AML Officer for the purpose of identification and control of the client. The AML Officer shall always verify on an ad hoc basis that the person does not come from a state subject to EU sanctions or from countries at risk, the current list of which is set out in Annex No. 1.

The list of Risk Clients (Profile No. 2), or clients with Risk Profiles, are maintained in the Company's information system. Each client's card in the information system shows the client's Risk Profile.

Client's risk factors:

- a) the Business Relationship is conducted under unusual circumstances (the client is accompanied, guided), (1b)
- b) the client is located in a higher risk geographic area, (2b)
- c) the legal person or trust is a personal asset holding vehicle, (2a)
- d) the client is a corporation in which there may be authorized shareholders or members or which issues shares in bearer form, (1b)
- e) the client uses cash extensively in its business activities (e.g. exchange offices, newsagents, stall sales), or (1b)
- f) the client's ownership structure appears unusual or overly complex due to the nature of its business (3 or more other companies in the client's ownership structure). (1b)
- g) subject of the client's business:
 1. purchase / sale of weapons ammunition, trading with military material (3a)
 2. trade in hazardous substances (3a),
 3. gambling halls, casinos, pawn shops (2a)
- h) the client contacts the Company e.g., 3 times a month, then does not contact the company for more than 10 months, then resumes communication and this pattern repeats, (1b)
- i) the client terminates the relationship after a short period of time from the conclusion of the Business Relationship (within a month) and then re-establishes the Business Relationship within two months (2b).

The client will always have Profile No. 2 if:

- a) any of the countries of origin of the client, of the person authorised to deal with the Company on behalf of the client, or any of the countries of origin of the beneficial owner of the client, is a country which **does not adequately** apply measures against money laundering and terrorist financing and is so designated in a directly applicable regulation of the European Union or is so designated by the Financial Action Task Force (FATF) in a public statement published on its website (i.e., if the country in question has the number 2 in the table in Annex No. 1);
- b) the client or its beneficial owner are politically exposed persons or are known to the Company to be acting on behalf of a politically exposed person;

- c) the client has an opaque ownership structure; an opaque ownership structure does not exist if the client is a legal person whose securities are admitted to trading on a European regulated market or a foreign market equivalent to a European regulated market if it is subject to disclosure requirements equivalent to those of European Union law;
- d) to the best of the Company's knowledge, the subject matter of the Transaction has been or is to be transferred or provided in connection with the Transaction from a country which does not sufficiently or at all apply measures against money laundering and terrorist financing and is so designated in a directly applicable European Union regulation or is so designated by the FATF, or the subject matter of the Transaction has been or is to be transferred or provided to such a country in connection with the Transaction;
- e) the client is not the natural person for whom the transaction is executed;
- f) the client, who is a legal person, does not, to the Company's knowledge, carry out any economic activity;
- g) any of the activities of the client which is a legal person is risky, as defined in paragraph 1(g) of the Client's Risk Factors section of this Article;
- h) if the client wishes to enter into an unusually complex or unusually voluminous Transaction, a method of trading (the Transaction in question differs by 300% from the arithmetic average of the client's previously made payments), or a Transaction for which its economic and legal purpose is not clear (a Transaction that does not fall within the client's subject of business or appears to be potentially contrary to the law);
- i) the client, the sender of the payment or its recipient has links to countries subject to international sanctions (see Annex No. 1).

The client **will always have Profile No. 3** if:

- a) the client, a person authorised to deal with the Company on behalf of the client, the beneficial owner of the client or, as far as the Company is aware, the person with whom the client conducts the transaction, the ultimate beneficiary of the subject matter of the Transaction or the beneficial owner of the person with whom the client conducts the transaction, is registered on the list of persons and movements against whom sanctions measures are applied in accordance with other legislation serving to implement international sanctions (see Annex No. 1),
- b) any of the countries of origin of the client, a person authorised to act with the Company on behalf of the client, is a country which **does not apply** measures against money laundering and terrorist financing **at all** and is so designated in a directly applicable regulation of the European Union or is so designated by the Financial Action Task Force (FATF) in a public statement published on its website (i.e., the country in question has the number 3 in the table in Annex No. 1).

7.4. Risk factors of the Company's products and services

a) Specification of risk factors for the Company's products

The Company checks the risk factors related to the misuse of the Company's products and services for Legalization of Proceeds of Crime and Terrorist Financing. On the basis of the facts found, the Company may, during the course of the Business Relationship, assign the status of a Risky Client to a client who was identified as risk-free at the conclusion of the Business Relationship, or terminate the Business Relationship with the client.

The Company is a financial institution that provides clients with a money management service for the purpose of co-investing their funds. The Company is registered with the CNB for this activity. The possibility of misuse of the services by the client is therefore a consideration when using money management, where the client may entrust funds with illegal origin to the management. Abuse may be accompanied by so-called structuring, where the client sends funds just below the control threshold

or untypical Transaction for the client (unusual amount or demanding special conditions, e.g., demanding cash deposit without logical justification). Another means of abuse may be a false identification card or insufficient control by the client's employee or even their facilitation in this criminal activity (involvement of the so-called "insider").

The Company is a financial institution that manages funds entrusted to it. In providing the services, the company considers the following possibilities for misuse of the services for money laundering:

- a) the value of executed Transactions
 1. Transactions executed in an amount untypical for the client, deviating from the client's transaction history (e.g., significantly higher volume, untypical currency, increased frequency of transactions);
 2. the client requests to execute a Transaction for which there is no apparent economic reason (e.g., the client requests the withdrawal of funds deposited the day before);
 3. amount of transactions executed does not correspond to the amount of the client's income/revenue;
 4. client's transactions correspond to the so-called structuring, i.e., entrusting the funds to the management or their withdrawal by one client to the Company's account, where the client makes 3 or more transactions within 1 month, each of which does not exceed CZK 350,000;
 5. incoming payments to the Company's account above CZK 5 million from persons other than the client;
- b) the payment method
 1. the client requests a cash payment method without any logical justification and has used only non-cash payments in previous Transactions;
- c) the involvement of insiders
 1. the risk of involvement of insiders (employees of the Company) in criminal activities, where the employee tries to help conceal or directly participate in money laundering.

There are also increased risk factors associated with the Company's products and services, which are:

- a) the use of transactions that could facilitate anonymity,
- b) deposits from unknown or unrelated third parties; or
- c) new products and new business practices, including new distribution systems, and the use of new or emerging technologies for new or existing products.

Client and service risk factors may be intertwined and should always be considered in relation to each other.

b) Monitoring of Risk Factors and Business Relationships of the Company's clients

Ongoing monitoring of the client's Risk Factors is closely related to the monitoring and control of the client during the course of the Business Relationship.

The Company uses monitoring to monitor the client during the course of the Business Relationship, including Risk Factors, through:

- a) client personnel who, through continuous communication with clients, know the procedures and needs of clients and can detect deviations from the client's "norm" in the Transactions,
- b) mandatory updates of the data provided by clients,
- c) random checks by internal control staff.

Monitoring by Client Officers

Each Client Officer shall:

- on the basis of knowledge of the client's usual behaviour, evaluate each Transaction and any requests for service provision, in the event of a non-standard or unusual request for a Transaction by the client, carry out a review of the Transaction or request assistance from the AML Officer,
- promptly update client information in accordance with this Internal Regulation.

Mandatory updates of data provided by clients

The agreement requires the clients to notify the Company of any changes communicated in the agreement and the AML questionnaire. In the event that clients fail to properly comply with their information obligations to the Company, the Company has implemented periodic updates of client information relating to client identification and information contained in the AML questionnaire. The update of information is done by re-completing the AML questionnaire. The following deadlines for updating the information are set:

- a) client with Risk Profile No. 1, always after 36 months from the establishment of the Business Relationship or the last update of information;
- b) with Risk Profile No. 2, always after 12 months from the establishment of the Business Relationship or the last update of information.

Updating the information on whether or not a person is politically exposed must always take place after an election (regional, senate, chamber of deputies or presidential) by asking clients within 60 days from the date of the election result whether the previously stated fact still applies.

Checks by the AML Officer

AML Officer performs:

1. performs quarterly inspections, during which they randomly check:
 - performance of checks on clients when establishing a Business Relationship, i.e., the correctness of the completion of contracts and AML questionnaires and the delivery of the documents and information required by this internal regulation to establish a Business Relationship,
 - performance of checks of clients during the course of the Business Relationship in accordance with this Internal Regulation,
 - the output of the inspection is a quarterly report on the inspection carried out and the results found, sent to the member of the statutory body.
2. weekly checks of all executed Transactions of clients with Risk Profile No. 2 and their evaluation in relation to the obligations set out in this Internal Regulation.

Deployment of new products and technologies by the Company

In the case of the introduction of new products and services, distribution channels or technological processes, caution should always be exercised and the possibility of their misuse for money laundering should be considered, given that this is an unestablished activity and the Company may not be able to comply with all anti-money laundering measures. When new products, services or technologies are introduced, the AML Officer has established Anti-Money Laundering and Anti-Terrorist Financing Procedures.

8. Entering into a Business Relationship, Failure to execute a Transaction

The Company will refuse to execute a Transaction or enter into a Business Relationship in the following cases:

- the client refuses to submit to identification;

- the client fails to provide the necessary data for identification and control;
- the client, in cases where an employee of the Company suspects at the conclusion of the Business Relationship, during its duration or during the execution of the Transaction that the client is not acting on their own behalf or that they are representing that they are acting for a third party, and asks the client to provide the authorization, does not provide the authorization;
- the client refuses to cooperate with the inspection;
- the client cannot be identified and/or checked for any other reason;
- the Client Officer of the Company conducting the identification or verification has doubts about the veracity of the information provided by the client or the veracity of the documents submitted;
- the client is a person against whom the Czech Republic applies international sanctions of a financial nature (see Annex No. 1);
- a Politically Exposed Person, unless the Company knows the origin of the property intended for the Transaction;
- the client, the beneficial owner of the client or a person acting on behalf of the client or a member of the client's statutory body is a person on the list of sanctioned entities.

In the event that the Company discovers any of the aforementioned facts during the course of the Business Relationship, it will not execute the client's Transaction or will proceed to terminate the Business Relationship.

The person responsible for the initial identification of the client, signing the agreement and checking the documents submitted before signing the agreement with the client is the Client Officer. The Client Officer is responsible for the ongoing review of the client and is also responsible for updating the client's details and updating the AML questionnaire where applicable. The statutory body is responsible for the final check of the client and the documentation submitted at the signing of the contract (application of the 4 eyes check principle).

9. Definition of a suspicious transaction

A suspicious transaction is a transaction carried out under circumstances giving rise to suspicion of an attempt to launder the proceeds of crime or suspicion that the funds used in the Transaction are intended for the financing of terrorism or that the Transaction is otherwise related or connected to the financing of terrorism, i.e., a Transaction which, on the basis of certain indications, can be presumed, even with a lower degree of probability, to be the proceeds of, or to be used to commit, a criminal offence or to be used to commit an act of terrorism or other terrorism-related activities (hereinafter the "**Suspicious Transaction**"). The Company does not need to know what the offence is or who has committed it, nor does it need to know any other facts that meet the elements of the offence.

General characteristics of a suspicious transaction

- a) There are problems in identifying the client
- b) Unusual conditions are demanded and offered by the client
- c) The Transaction is untypical for the given client
- d) The client's documents appear to be forged or otherwise defaced or have an otherwise questionable appearance
- e) The client is nervous during personal contact for unknown reasons
- f) The client is accompanied and watched
- g) The client acts as an intermediary
- h) There is no apparent economic, factual or legal reason for the transaction or its discernible relationship to the client's normal business activities
- i) Unusual ways of transferring large sums of money (deposit at the bank's cash desk out of the normal range)
- j) Seeking minimal contact with the Company and delegating such contact to others by proxy
- k) A Transaction that is opaque in terms of its economic objective or appears illogical and its design

may signal an illegal act

- l) Transactions in which funds are withdrawn again shortly after being deposited, unless there is no logical reason for such action from the client's business activities
- m) The client discloses false or misleading information to the Company, or refuses without justification to disclose or provide the Company with routine information and documents relating to the Transaction, or discloses information to the Company which is difficult for the Company to verify or which is unreliable
- n) The Transaction is executed with a Risk Client
- o) The client refuses to submit to a check or refuses to provide the identification data of the person for whom they are acting

Signs of a suspicious transaction in the management of assets for the purpose of joint investment

- a) Deposits with volume just below the control threshold (structuring)
- b) Unusual requirements for the execution of Transactions, in particular with regard to the type of client, its previous business activity, the subject matter, amount and method of settlement of the Transaction and the subject matter of the client's business
- c) Deposits are made with large amounts of lower-value currency
- d) Unusual carrying of large amounts of cash, e.g., in a plastic bag, pocket, etc.
- e) Deposits in currencies not frequently used in the domestic market (e.g., Ukrainian Hryvnia, Vietnamese Dong, Belarusian Ruble)
- f) Deposits and withdrawals of entrusted funds from/to risky and sanctioned countries
- g) The client requests a so-called semi-cash transaction without a logical explanation, e.g., they send the deposit by bank transfer and withdraws the deposited money in cash
- h) The client changes contact details or transaction instructions without logical explanation
- i) Available information indicates that the client has links to perpetrators of criminal activity
- j) For unclear reasons, the client is represented by another person on the basis of a power of attorney
- k) Client's Transactions show a seasonal pattern and there is no apparent legal reason for this
- l) The client submits documents issued by a foreign institution that can hardly be verified
- m) The frequency or amount of deposits does not match the client's wealth profile

It is always a Suspicious Transaction if:

- **the client, a person in the ownership or management structure of the client, the beneficial owner of the client, a person acting on behalf of the client or a person involved in the transaction is known to the Company is a person against whom the Czech Republic applies international sanctions pursuant to Act No. 69/2006 Coll., on the Implementation of International Sanctions, as amended,**
- **the subject of the Transaction is or is to be goods or services against which the Czech Republic applies sanctions under the Act on the Implementation of International Sanctions.**

Suspicious transactions can be identified in particular by:

1. continuous monitoring of transactions by an employee of the Company with emphasis on the frequency and extent of deviations from the normal regime
2. continuous contacts with the client and informing the Company's Client Officer about the client's activities
3. third party information (press, internet, etc.)
4. procedures specified in Article 7.4.b).

10. Evaluation process of a Suspicious Transaction, records

The application of the “know your client” principle, i.e., the identification and control of the client and the monitoring of the nature, volume and other parameters of the Transactions carried out by the client, is a basic rule for the detection of Suspicious Transactions and thus for the effective prevention of Money Laundering and Terrorist Financing through the Company. This knowledge is based on the continuous monitoring of Transactions with an emphasis on the frequency and extent of certain deviations from the client’s normal trading pattern (see Article 7.4.b). The identification of Suspicious Transactions must be based on an individual assessment of the characteristics of each Transaction.

As part of the assessment and evaluation of Suspicious Transactions, the Company’s personnel focus in particular on:

- the Transactions executed by risk clients;
- the Transactions of Politically Exposed Persons;
- the Transactions that show any of the signs of a Suspicious Transaction.

In doing so, they shall take particular account of:

- the nature of the Transaction and the circumstances of its execution;
- the nature and volume of the client’s usual Transactions;
- client’s Risk Profile.

If an executed Transaction shows one of the “partially suspicious signs”, it may not always be a Suspicious Transaction, but a comprehensive assessment is required.

The primary responsibility for monitoring a client’s Transactions rests with the Client Officer who provides the service to the client on behalf of the Company.

If there is a change in the nature of the Transactions by the client or a significant increase in the number or volume of Transactions compared to a comparable period in the past, the Company’s Client Officer is required to determine the cause of this development. In case of doubt, the Company’s Client Officer is also entitled to request the client to provide documents proving the reason for such changes.

The Company records information about the client and its Transactions through the information system. All employees of the Company have access to the information regarding the client and its Transactions recorded in the information system. The persons responsible for the proper recording of the information are the Client Officers.

The client information for the information system includes in particular:

- (i) the contractual documentation entered into with the client, including the AML questionnaire(s);
- (ii) where applicable, an authorisation under the AML Act issued by the client;
- (iii) source documents for the Identification Data (copy of the Identity Document, proof of existence of a legal person, etc.).

The individual documents must show when and by whom they were obtained and how they were updated. The rules in Article 7.4(b) apply to the updating of client information.

11. Notification of a suspicious transaction

If a Client Officer or other employee of the Company assesses a client’s Transaction as a Suspicious Transaction, they shall immediately prepare an internal Suspicious Transaction report and inform the statutory body and the AML Officer by email or telephone

An internal Suspicious Transaction report containing details of the client and the Suspicious Transaction will be sent by the employee to the AML Officer without delay. The AML Officer will acknowledge receipt of the internal Suspicious Transaction report by telephone or email. A template of the internal report is attached as Annex No. 3 to this Internal Regulation.

Where there are clear facts that a Suspicious Transaction is involved and the Company's AML Officer fails to report the Suspicious Transaction, this will be considered a serious breach of the Company's internal regulations.

The AML Officer has passive access to the Company's information system for the purpose of reviewing internal reports, documentation and information relating to the Suspicious Transaction. The AML Officer shall make a comprehensive assessment of whether the transaction is a Suspicious Transaction.

In the event that the AML Officer evaluates a Transaction as Suspicious, the AML Officer shall notify the FAO, without undue delay. If the circumstances of the case so require, in particular if there is a risk of default, the AML Officer shall report the Suspicious Transaction immediately upon its identification.

In the Notification of Suspicious Transaction, the AML Officer shall state:

- identification data of the Company employee reporting the Suspicious Transaction;
- identification data of the client to whom the notification relates, or identification details of the person acting on behalf of the client to whom the notification relates;
- a description of the subject matter and material circumstances of the Transaction, a description of what makes the Transaction suspicious; details of the underlying transactions, a description of the cash or other means of payment used and other circumstances of the cash payment, the timing of the Transaction, the account numbers in which the funds in respect of which the notification is made are concentrated, the numbers of any accounts into or out of which funds have been or are to be transferred, including identification of the owners of the disposition, if known to the participant;
- the current date.

A Notification of Suspicious Transaction is submitted in writing using the form on the FAO¹ website, via the MoneyWeb app, or by data mail. The AML Officer will always verify the delivery of the Notification of Suspicious Transaction to the FAO.

A template for the FAO notification is attached as Annex No. 2 to this Internal Regulation.

12. Postponement of the Client's Order

Where there is a risk that the immediate execution of a Client's Order could frustrate or materially impede the seizure of proceeds of crime or funds intended to finance terrorism, the Company will execute the Client's Order in respect of the Suspicious Transaction no earlier than 24 hours after receipt of notification of the Suspicious Transaction to the FAO. The Company shall secure the property to which the Client's Order relates in an appropriate manner against tampering. In such cases, the AML Officer/statutory body shall give a notification of a Suspicious Transaction on the same day as the receipt of the Client's Order, and the notification of a Suspicious Transaction shall include information about the delay in executing the Client's Order

¹ <https://formulare.financnianalytickyurad.cz/fas/FormService/filler.open?name=FAU-OPO.fo>

The preceding paragraph shall not apply where a postponement of the Order is not possible or where such postponement would frustrate the investigation of the Suspicious Transaction. The Company shall notify the FAO of the execution of such Transaction immediately upon execution.

In the event that, following notification of a Suspicious Transaction, the FAO decides to extend the period for which execution of the Client's Order is postponed or to seize the property to be the subject of the Suspicious Transaction, the Company shall make the seizure of the property in the manner specified in FAO's decision.

The decision to postpone the execution of the Client's Order or the seizure of assets shall become effective upon its announcement. The announcement may be made orally, by telephone, by telefax or electronically; however, a copy of the written copy shall always be delivered to the Company thereafter.

If the investigation of a suspicious transaction requires a longer period of time due to its complexity, the FAO shall decide on

- a) a prolongation of the period for which the execution of the client's order is postponed, but no longer than a further 2 working days; or
- b) a postponement of the execution of the client's order or the seizure of the property to be the subject of the suspicious transaction by the obliged person with whom the property is located for up to 3 working days.

If the FAO makes a decision under (b), the Company shall notify the FAO of the implementation of the decision and confirm the time from which the time limit is to run. The FAO shall also keep the FAO informed of all material facts concerning the property referred to in the decision.

If the FAO fails to notify the Company that it has filed a criminal complaint within the time limit set out above, the obliged person shall execute the client's order. If the FAO notifies the Company within the time period set forth above that a criminal complaint has been filed, the delay in executing the client's order or seizing the property shall extend for 3 business days from the date of the criminal complaint if the law enforcement agency has not made a decision to remove or seize the subject of the Suspicious Transaction by the end of the time period.

During the period of suspension of the Order, the Company shall appropriately safeguard the assets to which the Client's Order relates so that they cannot be handled in contravention of this Internal Regulation, specifically instructing the AML Officer/statutory body of the Company to instruct the staff who will be prohibited from executing the Transaction to which the notice of the Suspicious Transaction relates until further notice.

Upon receipt of the notification by the FAO or, as the case may be, after the expiry of the relevant time limit, the AML Officer/statutory body shall inform the officer of the Company who reported the Suspicious Transaction as to the earliest date on which the Client's Order can be executed.

13. Internal control system

The Company shall exercise internal control over compliance with the rules set out in this Internal Regulation and the AML Act through:

- managers, specifically the statutory body, exercising management control,
- and internal control staff, specifically the AML Officer, carrying out continuous compliance checks.

The AML Officer within the internal control:

- examines, tests and evaluates the effectiveness and functionality of the system of measures to prevent money laundering;

- examines, tests and evaluates the effectiveness and functionality of the system of measures to prevent Legalization of Proceeds of Crime and Financing of Terrorism in connection with the introduction of a new product or service;
- verifies the Company's compliance with legal regulations;
- verifies the compliance of this Internal Regulation with the applicable laws and regulations;
- performs random checks on the practices of client employees as a prevention against so-called "insiders";
- in the event that deficiencies are detected, propose the implementation of the necessary measures (modifications in internal regulations, improvement of the information system, improvement of the training system, etc.).

The statutory body within the internal control:

- evaluates the effectiveness and functionality of the system of measures to prevent money laundering;
- approves the introduction of new products after all obligations in terms of AML measures have been met;
- approves changes to this Internal Regulation and related processes.

The Company's statutory body and the AML Officer have access to all information relating to clients and their Transactions and have the right to request all necessary information and documents from all Company personnel. The Company's personnel are obliged to produce these and provide all necessary cooperation.

Any employee is entitled to submit an anonymous notification to the Company of a violation of the AML Act. To ensure anonymity, the Company has established an internal notification system - a notification box where an employee can submit their notification anonymously in case of a suspected violation of the AML Act in the Company.

The specific internal control of the obligations under this Internal Regulation and the AML Act is carried out by the procedures set out in Article 7.4.b).

14. Information obligations of the Company

The Company shall, upon the FAO's instruction, disclose, within a time period specified by the FAO, details of Business Relationships and Transactions related to the obligation to identify or in respect of which the FAO is conducting an investigation, provide documents relating to such Transactions, or allow access to such documents to authorised FAO personnel when investigating the notification, and provide information on persons who have participated in any way in such Transactions.

The Company shall, at the direction of the FAO, within a time period specified by the FAO, disclose information as to whether it maintains or has maintained in the previous 10 years a Business Relationship with a specific natural or legal person in respect of whom it had a duty to identify and the nature of that Business Relationship.

The Company shall follow a similar procedure in the case of requests from any authorities under administrative supervision.

The Company shall provide the client, prior to the establishment of the Business Relationship, with the information on the processing of personal data required under the legislation governing the protection and processing of personal data, including a general notice of the obligation to process personal data for the purposes of preventing the laundering of the proceeds of crime and the financing of terrorism.

15. Archiving obligation

The Company identifies and stores in the client information system all information relating to the Business Relationship on the basis of which the Company identifies and checks the client, verifies the validity and completeness of the data and, if necessary, updates it.

The Company shall retain the following information and documents for a period of 10 years after the termination of the Business Relationship or the execution of a Transaction with the client:

- Identification and other data regarding the client obtained in the course of identification;
- copies of documents submitted for identification and control;
- an indication of who made the initial identification of the client and when;
- in the case of representation of the client, the relevant authorisation, a certified copy of the power of attorney or, where applicable, the reference number of the court decision appointing the guardian;
- evidence of the client's Transactions and Orders;
- information and copies of documents obtained during the audit of the client,
- records of all steps taken in the identification and control of the client, including information on any difficulties related to these steps,
- records of the process used to assess and determine the risk profile of the client, including the choice of appropriate action taken against the client and the assessment of the facts relating to the submission of a suspicious trade report,
- other information and documents related to the Business Relationship.

The 10-year period begins on the first day of the calendar month following the calendar month in which the last Transaction was executed.

The Company shall archive the aforementioned data in a manner and to the extent that ensures the evidentiary validity of individual Transactions and the procedures related thereto.

In addition, the Company shall archive the approval and decision-making processes and control activities under the Internal Policy System, including the reasons for them, the related responsibilities, authorities, supporting documentation, and including the process for identifying and controlling the client and selecting the appropriate action taken against the client or the assessment related to the submission of a Suspicious Transaction report, as well as information on the findings made during the control of the client and during the review of Transactions and correspondence related to Transactions and Business Relationships, so as to ensure the reconstructability of these processes.

The Company shall provide the requested documents and information at any time upon the request of the FAO or any other authorised inspection body. The information is provided through the statutory body.

The Company carries out periodic back-up of all approval and decision-making processes and control activities under the AML Policy in such a way as to enable their reconstruction.

16. Confidentiality obligation

The Company and its employees are obliged to maintain the confidentiality of the facts they have learned in connection with the Suspicious Transaction. This obligation applies both to third parties and to the persons to whom the information is disclosed.

The duty of confidentiality of an employee of the Company does not cease upon termination of their employment or other contractual relationship with the Company or upon their transfer to another job. The disclosure of such information to state authorities and other entities shall not be considered a breach of the duty of confidentiality in cases where the law so provides.

17. Training of workers

The Company, through the AML Officer, will provide training at least once during a 12-calendar month period to staff who may encounter Suspicious Transactions in the course of their work, in particular Client Officers.

New employees who may encounter Suspicious Transactions in the course of their work must always be made aware of the AML Internal Regulations prior to being assigned to such a position.

The subject of training of the Company's workers is then mainly:

- a. a system of internal anti-money laundering policies;
- b. typology and characteristics of Suspicious Transactions;
- c. procedures for identifying and evaluating Suspicious Transactions;
- d. determination of the risk profile of the client;
- e. the procedures for entering into a Business Relationship, the correct procedure for identifying the client and its control;
- f. cases of failure to enter into or terminate a Business Relationship, failure to execute a Transaction;
- g. changes in the AML Act, internal regulations containing a system of internal policies against Money Laundering;
- h. the procedure for reporting a Suspicious Transaction;
- i. review of risk factor identification procedures.

The Company's workers shall confirm their participation in the training by signing the attendance list. These attendance sheets, together with records of the training and topics covered, are archived within the Company.

Records of attendance and training content shall be kept for at least 5 years after the training has taken place.

18. Contact person

In the area of measures against laundering of proceeds of crime and financing of terrorism, the Company represents during any contact with the FAO and the CNB:

AML Officer

Mgr. Zuzana Hrabalová

+420734393793

zhrabalova@agrarnipudnifond.cz

the absence of the designated person, she shall be represented by:

Executive Director

Ms. Andrea Mičulková

+420606438398

info@apfdigitalagrifund.com

In this context, the contact person is obliged to:

- receive and analyse internal Suspicious Trade reports to evaluate whether a trade is a Suspicious Transaction;
- fulfil on behalf of the Company the information obligation to the FAO;
- inform the Company's statutory body of information provided to the FAO;
- ensure that the necessary records are maintained;
- ensure that documentation relating to Suspicious Transactions is archived;
- ensure the training of the Company's workers;

- inform the FAO of changes to the internal policy system within 30 days of their adoption by the Company.

In this context, the contact person is entitled to:

- request from all employees of the Company all information and documents relating to Clients and their Transactions;
- request the cooperation of individual departments and employees of the Company.

It is also the duty of the contact person to monitor current developments in the field of anti-money laundering and the recommendations of the Financial Action Task Force on Money Laundering, the European Union authorities and other international organisations active in the field of anti-money laundering and to ensure that the Company's internal regulations comply with the applicable legislation.

The Company shall promptly inform the FAO of the contact person's learning and change of contact person, indicating the name, surname, job title, and contact details, including telephone and electronic contact details.

19. Delegated person

A member of the statutory body
Ms. Andrea Mičulková
+420606438398
info@apfdigitalagrifund.com

The delegated person is responsible for ensuring compliance with the obligations under the AML Act. The written delegation of a member of the Company's statutory body must be made within 60 days of the date on which the Company became an obligated person under the AML Act or within 60 days of the date on which the membership of the person previously delegated in the statutory body ceased. The delegated person shall have all the powers necessary to comply with the obligations under this Internal Regulation.

II. THE APPLICATION OF THE SYSTEM OF INTERNATIONAL SANCTIONS TO THE COMPANY'S ACTIVITIES

1. Application of international sanctions

In the course of its business activities, the Company applies, in accordance with Act No. 69/2006 Coll., on the Implementation of International Sanctions, a system of measures for the implementation of international sanctions in order to maintain or restore international peace and security, protect fundamental human rights and combat terrorism.

In screening individual transactions, both the sender and the recipient are checked against lists issued by both the EU and the US OFAC. The current list of persons subject to international sanctions can be found on the website http://eeas.europa.eu/archives/docs/cfsp/sanctions/docs/measures_en.pdf.

In case of a technological failure, a file with all relevant sanction lists in Excel format is used, which is updated on a daily basis and is accessible in the information system.

The company has set up a check on clients coming from countries subject to international sanctions. Checking is carried out according to the lists of the government and international institutions by the staff checking and registering clients in the trading system.

2. Notification obligation

If, in the course of providing asset management for the purpose of co-investment, the Company's workers become aware in a credible manner that the Company has assets subject to international sanctions, they shall notify the statutory body, which shall notify the FAO without undue delay.

If, in the course of preparing or concluding the Business Relationship, the Client Officer suspects that one of the parties to the Business Relationship is subject to international sanctions or that the subject of the Business Relationship is or is to be property subject to international sanctions, but this suspicion cannot be verified credibly before or at the time of concluding the agreement, the notification obligation under the preceding paragraph shall arise immediately after the conclusion of the agreement.

In the notification of property subject to international sanctions, the Company shall state:

- a brief description of the property, its value, if known to the Company, and its location at the time of the announcement,
- who owns the property, if known to the Company,
- whether there is an imminent danger of damage to or deterioration of the property or its use in violation of the law,
- other relevant information about the property,
- the contact address, telephone and email address of the Company and the person responsible for the Company.

The Company shall give notice in writing or orally on the record and, if there is a risk of default, by electronic or facsimile transmission. A notice given by electronic means with a guaranteed electronic signature shall also be deemed to be a written notice.

3. Contact data of the FAO

Postal address: Financial Analytical Office, Washingtonova 1621/11, 110 00 Prague 1

Delivery address: P.O.BOX 675, Jindřišská 14, 111 21 Prague 1

Telephone: +420 257 044 501, or +420 603 587 663 outside normal working hours (working days)

08:00 to 16:00);
Fax: +420 257 044 502;
E-mail: fau@mfcz.cz

4. Disposal of identified assets subject to international sanctions

If the Company has credible knowledge that it is in possession of, or has made notification of, internationally sanctioned property, it shall not dispose of such property other than to protect it from loss, deterioration, destruction or other damage from the time it becomes aware that the property is deemed to be internationally sanctioned.

On behalf of APF DIGITAL AGRIFUND CR s.r.o.

.....
Andrea Mičulková, Executive

ANNEX NO. 1**LIST OF SANCTIONED PERSONS AND COUNTRIES AT RISK****List of sanctioned persons**

The Annex contains links to lists of sanctioned persons and persons suspected of supporting terrorism. This list is continuously updated.

- **Consolidated list of persons, groups and entities subject to EU financial sanctions**
<https://webgate.ec.europa.eu/cas/>
- **OFAC sanctions are published on the website at:**
<https://www.treasury.gov/about/organizational-structure/offices/Pages/Office-of-Foreign-Assets-Control.aspx>
- **List of persons and entities pursuant to Government Regulation No. 210/2008 Coll., on the implementation of special measures to combat terrorism, as amended:**
 - <https://www.zakonyprolidi.cz/cs/2008-210>
- **Further relevant information is published at:**
 - <http://www.treas.gov/offices/enforcement/ofac/>

List of countries at risk

European Union Commission Regulation 2016/1675 of 14 July 2016 supplementing EU Directive 2015/849 of the European Parliament and of the Council by identifying countries with strategic deficiencies

<http://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX:32016R1675>

Other relevant lists for assessing countries at risk:

[http://www.fatf-gafi.org/publications/high-risk-and-other-monitored-jurisdictions/?hf=10&b=0&s=desc\(fatf_releasedate\)](http://www.fatf-gafi.org/publications/high-risk-and-other-monitored-jurisdictions/?hf=10&b=0&s=desc(fatf_releasedate))

Sources for assessing the level of corruption in a country: <https://www.transparency.org/cpi2018>
Further information is also available on the website of the FAO.

List of countries at risk

Country	Risk Profile
Afghanistan	3
Albania	3
Bahamas	3
Barbados	3
Belarus	3
Burkina Faso	3
Bosna and Hercegovina	3
Botswana	3
Ethiopia	3
Egypt	2
Philipines	3

Gibraltar	3
Guyana	3
Ghana	3
Chad	3
Haiti	3
Iraq	3
Iran	3
Jamaka	3
Yemen	3
Republic of South Africa	3
Jordan	3
Cayman Islands	3
Cambodia	3
Kongo	3
Democratic People's Republic of Korea (DPRK)	3
Lao People's Democratic Republic	3
Libya	3
Mali	3
Morocco	3
Mauricius	3
Marshall Islands	3
Mongolia	3
Mozambique	3
Myanmar	3
Nicaragua	3
Nigeria	3
Pakistan	3
Panama	3
Russia	3
Senegal	3
United Arab Emirates	3
Syria	3
Serbia	3
Sudan / South Sudan	3
Sri Lanka	3
Somalia	3
Tanzania	3
Trinidad and Tobago	3
Tunisia	2
Turkey	3
Turkmenistan	3
Uzbekistan	3
Ukraine	2
Uganda	3
USA	2
Vanuatu	3
Venezuela	2
Zimbabwe	3

ANNEX NO. 2

NOTIFICATION OF A SUSPICIOUS TRANSACTION – TEMPLATE

Financial Analytical Office
Poštovní příhrádka 675, Jindřišská 14
111 21 Prague 1

In Prague on

Subject: Notification of a suspicious transaction**Obliged person according to Section 2(1)(b)(4) of the AML Act:**

APF AGRICULTURAL LAND CR s.r.o., ID No.: 143 47 296, with its registered office at Pražákova 1008/69, Štýřice, 639 00 Brno, registered in the Commercial Registry at the Regional Court in Brno, File C 132084

Identification of the person to whom the notification relates:

First name and surname/Trade name:

National identification number (date of birth)/ID No.:

Place of birth:

Gender:

Permanent or other residence:

Citizenship:

Represented by (if it is a legal person):

Identification details of all other participants in the transaction:**Type of the transaction:**

Information on the material circumstances of the transaction and other information that may be relevant to the suspicious transaction and relevant to its assessment from the point of view of measures against money laundering and terrorist financing:

* delete as appropriate

Information about the execution or postponement of the transaction

(Indicate whether and when the transaction was executed or postponed, or the reason why the transaction was or was not executed.)

On behalf of APF AGRICULTURAL LAND CR s.r.o

.....
Andrea Mičulková, Executive

ANNEX NO. 3

INTERNAL REPORTING OF A SUSPICIOUS TRANSACTION

Identification of the employee reporting the suspicious transaction

first name and surname:

department:

Identification of the person to whom the notification relates:

First name and surname/Trade name:

National identification number (date of birth)/ID No.:

Place of birth:

Gender:

Permanent or other residence:

Citizenship:

Represented by (if it is a legal person):

Identification details of all other participants in the transaction:

Information on the material circumstances of the transaction and other information that may be relevant to the suspicious transaction and relevant to its assessment from the point of view of measures against money laundering and terrorist financing (indicate the timing, account numbers of the accounts holding the funds in respect of which the notification is made, the currency, the suspicious transaction, etc.):

Information about the execution or postponement of the transaction

(Indicate whether and when the transaction was executed or postponed, or the reason why the transaction was or was not executed.)

Time and date of notification of the suspicious transaction:

.....

First name/surname

Signature

ANNEX NO. 4**LIST OF NATIONAL FUNCTIONS OF POLITICALLY EXPOSED PERSONS**

President of the Republic + Head of the Office of the President of the Republic

Prime Minister

Head of a central government body and their deputy (deputy, state secretary):

- Ministry – Minister, Deputy Minister, Deputy for Section Management, State Secretary,
- Czech Statistical Office – Chairman, Deputy Chairman,
- Czech Office of Surveying and Cadastre – Chairman, Deputy Chairman,
- Czech Mining Authority – Chairman, Deputy Chairman - Director of the Mining Administration Section,
- Industrial Property Office – Chairman, Deputy Chairman,
- Office for the Protection of Competition – Chairman, Deputy Chairman,
- State Material Reserves Administration – Chairman, Deputy Chairman,
- State Office for Nuclear Safety – Chairman, section directors,
- National Security Office – Director, Deputy Directors,
- Energy Regulatory Office - Chairman of the ERO Council, members of the ERO Council,
- Office of the Government of the Czech Republic – Head of the Office of the Government, Deputy for Section Management, State Secretary,
- Czech Telecommunications Office – Chairman of the CTU Council, members of the CTU Council,
- Office for Personal Data Protection – Chairman, Deputy Chairman,
- Council for Radio and Television Broadcasting – Chairman, Vice-Chairmen,
- Office for Supervision of the Management of Political Parties and Political Movements – Chairman, members of the Office,
- Authority for Access to Transport Infrastructure – Chairman, Vice-Chairman,
- National Office for Cyber and Information Security – Director, deputies,
- National Sports Agency – Chairman, Vice-Chairmen,

Member of the Parliament of the Czech Republic

- Deputy,
- Senator,
- Head of the Office of the Chamber of Deputies,
- Head of the Office of the Senate,

Member of the governing body of a political party or political movement – Chairman, Vice-Chairmen

Head of local government

- Mayor,
- Deputy Mayor,
- Secretary of the Municipality,
- Director of the Prague City Hall,
- Governor,
- Deputy Governor,
- director of the regional office,
- Mayor of a municipality with extended jurisdiction

A judge of a supreme court, constitutional court or other supreme judicial body whose decision is generally, with some exceptions, not subject to appeal

- Judge of the Constitutional Court,
- Judge of the Supreme Administrative Court,
- Judge of the Supreme Court,
- Attorney General,

Member of the central bank board

- Governor,
- Vice-Governor,
- Member of the bank board of the Czech National Bank

A senior officer of the armed forces or corps

- Police of the Czech Republic – the President of the Police, directors of regional directorates of the Police of the Czech Republic,
- General Inspectorate of Security Forces – Director,
- Security Information Service – Director,
- Military Intelligence – Director,
- Office for Foreign Relations and Information – Director,
- Army of the Czech Republic – Chief of the General Staff of the Army of the Czech Republic, directors of regional military headquarters,
- Castle Guard – Commander,
- Military Office of the President of the Republic – Chief,

Member or representative of a member, if a legal person, of the statutory body of a state-controlled commercial corporation

- a member of the Board, as well as any other member of the administrative, management or controlling body of a state-owned commercial corporation (a commercial corporation in which the Czech Republic directly or indirectly owns more than 50% of the shares),
- director and deputy director of a state enterprise, members of the supervisory board of a state enterprise

An ambassador or head of a diplomatic mission, or a natural person who performs or has performed a similar function in another state, in an institution of the European Union or in an international organisation

- ambassadors,
- -consuls general,
- chargé d'affaires,
- judges of the European Court of Human Rights, the International Court of Justice, the International Criminal Court or any other international court,
- Heads of Permanent Missions of the Czech Republic to the EU, NATO, UN, OSCE, OECD and the Council of Europe

Representation of international organisations accredited for the Czech Republic ²

- International Organization for Migration – Head of Office,
- World Health Organization – Office of the World Health Organization – Head of Office,
- United Nations High Commissioner for Refugees – UNHCR – Office of the United Nations High Commissioner for Refugees – UNHCR Office in the Czech Republic – Head of Office,

² List of international organizations accredited for the Czech Republic, available at: https://www.mzv.cz/jnp/cz/o_ministerstvu/adresar_diplomatickych_misi/mise_mezinarodnich_organizaci_v_cr/index.html

- Organization for Security and Cooperation in Europe – OSCE – Documentation Centre in Prague – Head of Office,
- United Nations – UN Information Centre in Prague – Head of Office,

Supreme Audit Office

- President,
- Vice-President
- members of the Office.