Variance HODLING Kft.

Anti-Money Laundering Policies and Procedures

March 2023

1.1 In response to the global concern about money laundering and terrorist financing, **Variance HODLING Kft.** (hereinafter referred to as "**Company**") recognises the importance of its compliance with the Anti-Money Laundering and Countering the Financing of Terrorism ("**AML/CFT**").

1.2 This Policy lays down comprehensive policies and procedures with regard to AML/CFT which the Company shall observe. Adherence to this Policy is absolutely fundamental to ensuring that the Company complies fully with all applicable AML/CFT laws and regulations, including the Prevention of Money Laundering and Terrorist Financing Law of the Hungarian Republic and other related legislations.

1.3 This Policy is designed:

(1) to endorse the Company's strict compliance with the legal framework of the jurisdiction it operates governing anti-money laundering and terrorist financing;
(2) to appoint an Anti-Money Laundering Compliance Officer ("AMLCO") at the management level to be responsible for the implementation and ongoing compliance with this Policy, including establishing and conducting AML/CFT training programmes for all employees
(3) to appoint a Money Laundering Reporting Officer ("MLRO") to report knowledge or suspicion of ML/FT or of a person's connection with ML/FT to the FCIS and respond promptly to any request for information made by the authorities.
(4) to ensure training sessions regarding anti-money laundering are provided to all employees so that all such employees are aware of all applicable laws and regulations relating to AML/CFT, and their responsibilities with respect to these policies;
(5) to require all appropriate employees to be vigilant to any suspicious activities used for money laundering, terrorist financing, and other illegal activities, and report them immediately to the established internal bodies, in accordance with specified policies and procedures;

1.4 Compliance with the contents of this Policy is required for the entire staff of the Company. Non-compliance with the criteria and guidelines contained in this Policy will lead to penalties, sanctions and other disciplinary actions.

2. WHAT IS AML

2.1 Money laundering is the term used for a number of offences referring to the same process that is defined by the United Nations (**"UN"**) as "the surreptitious introduction of illegally obtained funds into the legitimate channels of the formal economy."

2.2 Thus, money laundering is defined as the process by which a natural or legal person, who is in possession of any funds derived from unlawful activities, transfers them to the financial system to disguise or conceal the true origin and ownership of the illicit proceeds; thus, providing a legitimate cover for the source of the illegally obtained money and making them appear to be legitimate.

2.3 According to the law money laundering shall mean:

1) the conversion or transfer of property, in the knowledge that such property is derived from a criminal act or from involvement in such an act, for the purpose of concealing or disguising the illicit origin of the property or of assisting any person who is involved in the commission of such a criminal act to evade the legal consequences of this act;
2) the concealment or disguise of the true nature, origin, source, location, disposition, movement, rights with respect to, or ownership of property, in the knowledge that such property is derived from a criminal act or from involvement in such an act;
3) the acquisition, possession or use of property, in the knowledge, at the time of acquisition/transfer, that such property was derived from a criminal act or from involvement in such an act;
4) preparation, attempts to commit and association to commit any of the acts referred to in points 1, 2 and 3.

2.4 Despite the variety of methods employed in money laundering transactions, the laundering process, closely linked to terrorist financing, generally consists of three stages:

(1) Placement, through which the funds (often in cash) originating from unlawful

or criminal activities enter into the financial systems;

(2) Concealment, by which the funds are separated from their illicit sources through a complex layer of financial or non-financial transactions, which are designed to disguise the origin of the funds and make it impossible for any investigators to trail back to the origin; and

(3) Integration, via which the laundered proceeds are placed back into the financial system, appearing as legitimate funds, and in such a way, they are unrecognisable as the illicit proceeds of unlawful activities.

2.5 Money laundering may often involve the proceeds of drug dealings, terrorist activities, arms dealings, mail fraud, bank fraud, wire fraud or securities fraud, and other activities.

3. AML/CFT REGULATORY REGIME

Hungary has a high level of commitment to establishing a robust and complete AML/CFT regime, as updated from time to time, based on relevant international standards and cooperation with other authorities. The Central Management of the National Tax and Customs Administration (**NAV**) is the main AML supervising body in Hungary. The NAV is responsible for ensuring that affected institutions follow the AML Law, in addition to analyzing and responding to suspicious transaction reports. The NAV also cooperates with the Prosecutor General's Office and the National Courts Office.

3.1 Prevention of Money Laundering and Terrorist Financing

Act LIII of 2017 on Preventing and Combating Money Laundering and Terrorist Financing (AML law) is the main regulation dealing with AML requirements in Hungary.

The regulation sets out the obligations and procedures that subject persons are required to fulfil and implement, without which an AML/CFT regime cannot be effective. These procedures mainly consist of the following:

(1) procedures on internal control, risk assessment, risk management, compliance management and communications;
(2) customer due diligence;
(3) record-keeping;
(4) transaction monitoring;
(5) reporting; and
(6) training and awareness.

The Risk-Based Approach (RBA) obliges a subject person to take appropriate steps (in proportion to the nature and size of its business) to identify and assess the risks of ML/FT, taking into account risk factors, including those relating to their customers, countries or geographic areas, products, services, transactions or delivery channels, and to take ensuing mitigating measures commensurate to the risks identified.

4. RISK ASSESSMENT

4.1 Risk-based Approach

The Company will adopt an overall risk-based approach to review Client and Client transactions to identify and assess the degree of potential money laundering and terrorist financing risks associated with Client and Client transactions.

The risk assessment shall be undertaken on a matter-by-matter basis on the Client and Client's transactions. The risk assessment may be undertaken both formally and informally throughout a Client Relationship.

The conclusions of the risk assessment will determine the appropriate levels of initial Client Due Diligence (**"CDD"**) measures to be taken and the appropriate types of mitigation policies and procedures to be applied to address the conclusions of the assessment.

The Company shall take into account various risk factors when evaluating the possibility and degree of money laundering and terrorist financing risks relating to Clients and Client transactions, including but not limited to, type of Clients, geographic locations of Clients (e.g. where the Client is incorporated in, formed in, or a resident of an Anti-Money Laundering Steering Group (**"AMLSG"**) List country), Politically Exposed Persons (**"PEPs"**) classification, professional activities and nature of business of Clients, source of funds, source of wealth, the complexity of structure requested and the use of intermediate corporate vehicles, and other relevant risk factors.

4.2 Client Risk Categories

The Company divides the Client Relationship into three risk categories, low, medium, and high risk. The lists below provide relevant characteristics of each of these risk categories, which are not exclusive and will be reviewed on a regular basis.

4.2.1 Low Risk

(i) Clients have been correctly identified;
(ii) Clients are known to the Company;
(iii) Clients are residents in or operating in countries identified by credible sources as having:
(a) effective AML/CFT systems;
(b) a low level of corruption or other criminal activities; or
(c) equivalent jurisdiction and appearing on the AMLSG List.
(iv) less than ten (10) transactions per year are anticipated under the Client relationship; and
(v) a thorough and complete risk assessment has been accomplished and all supporting documentation has been submitted for reference purposes.

4.2.2 Medium Risk

(i) Clients have been correctly identified, including Beneficial Owners;
(ii) Clients are not residents in or operating in high-risk countries;
(iii) more than ten (10) transactions per year are anticipated under the Client Relationship; and
(iv) the risk assessment does not provide clear information about the nature of the Client's business or professional activities and the total assets held by the Client.

4.2.3 High Risk

(i) the nature of the Client Relationship is complex, where the Clients or any other parties involved in the Client Relationship are not necessarily known to the Company;
(ii) where no face-to-face meeting has been held with the Beneficial Owners;
(iii) Clients are residents or operating in high-risk countries;
(iv) Clients are PEPs, including family members of a PEP (*See Chapter 7 below*);
(v) Client Relationships requiring frequent payments to and from high-risk countries;
(vi) the Client is a public body or state-owned entity from a jurisdiction with high levels of corruption and/or organised crime;
(vii) the Clients are legal persons or arrangements that are personal asset-holding vehicles;
(viii) intensive and significant cash payments are involved in the course of the Client's business; or

(ix) where a high risk of money laundering or terrorist financing has been identified following a risk assessment.

4.3 Money Laundering Risk

The Company shall take into account all relevant risk factors before determining the overall level of risk for Client and Client's transactions and proportionate the level of CDD measures. When identifying whether there is a higher risk of money laundering and/or terrorist financing, the Company must assess at least the following factors:

4.3.1 Customer Risk Factors:

a) the business relationship of the customer is conducted in unusual circumstances without any apparent economic or visible lawful purpose;

b) the customer is resident in a third country;

c) legal persons or entities not having legal personality are personal asset-holding vehicles;

d) a company has nominee shareholders acting for another person, or shares in bearer form;

e) business is cash-intensive;

f) the ownership structure of the legal person appears unusual or excessively complex given the nature of the legal person's business;

4.3.2 Product, Service, Transaction or Delivery Channel Risk Factors:

a) private banking;

b) a product or transaction might favour anonymity;

c) customer's business relationships or transactions are established or conducted without the physical presence of the customer in cases other than those specified in the Law;

d) payments are received from unknown or unassociated third parties;

e) products and business practices, including delivery mechanism, are new and new or developing technologies are used for both new and pre-existing products;

4.3.3 Geographical Risk Factors:

a) countries identified, on the basis of data of reports or similar documents by the Financial Action Task Force on Money Laundering and Terrorist Financing or a similar regional organisation, as having significant non-conformities with international requirements in their anti-money laundering and/or combating the financing of terrorism systems;

b) countries identified, on the basis of data by governmental and universally-recognised non-governmental organisations monitoring and assessing the level of corruption, as having significant levels of corruption or other criminal activity;

c) countries subject to sanctions, embargos or similar measures issued by, for example, the European Union or the United Nations;

d) countries provide funding or support for terrorist activities or have designated terrorist organisations operating within their country.

5. CLIENT IDENTIFICATION

The Company considers that it is essential and effective to confirm, prior to establishing a Client Relationship, the true identity of every Client, no matter new potential Clients or existing Clients.

Client Identification is a dynamic process by which the Company requests identification information from Clients, screens it to ensure that it is dealing with a real person (natural or legal), and the Company may then request supporting documentation when it is appropriate to do so. The requests made by the Company in all cases are to obtain satisfactory and consistent evidence that the Client is who he/she claims to be and actually exists.

The Company takes all necessary, proportionate measures in order to identify its Client and to verify the identity of the Client and the Clients' Beneficial Owners. The Company takes measures and determines the identity of the Client or his representative in the following cases:

a) before establishing a Business relationship;
b) before conducting one or several related Virtual Currency transactions (exchanges) or allowing a deposit of Virtual Currency on a Virtual Wallet;

c) if there is suspicion that information previously provided about the Client or his representative is incorrect and/or incomplete;
d) in any other case, when there are suspicions that an act of money laundering and/or terrorist financing is, was or will be carried out.

The Company establishes the Client's identity only remotely, i. e. when the Client is not physically present.

5.1 Remote Client Identification

When establishing the Clients' identity remotely, the Company shall:

a) verify whether there are any circumstances to apply enhanced Client due diligence. If such circumstances are present the procedures for enhanced Client due diligence accordingly shall be followed;
b) assess whether the Client provides copies of valid identity documents or corresponding travel documents which photographs are matching. This requirement does not apply if the identity is being determined using a qualified electronic signature;
c) find out whether the Client will act on his own behalf or someone else's interests;
d) verify whether a representative has a legal permit or power of attorney to act in the name of the Client;
e) to receive additional documents with the necessary information, if additional information is required from the Client;
f) check whether the Client or the Clients' beneficiary is included in the list of people that are financially sanctioned by Hungary, the European Union (EU sanctioned person list) and the United Nations;
g) use reliable and independent sources to verify whether the Client is a PEP.

If the Client is represented by another person, the Company shall request proof of power of attorney and, if possible, check its validity (i.e. if the Client or its representative has the right to issue such a power of attorney), expiry date, actions that representative can undertake in the name of the Client. Power of attorney shall comply with rules established in the Civil Code of the Republic of Hungary. In case the power of attorney is given by the Client natural person, such power of attorney on behalf of the Client shall be certified by the notary.

5.2 Reliance on Client Identification by Third Parties

When establishing the identity of the Client or of the beneficial owner, the Company may make use of information about the Client or the beneficial owner from third parties, provided that they have sufficient means to ensure that the third party will voluntarily comply with both of the following conditions:

1) it will, upon request, immediately provide to the requesting financial institution or another obliged entity all the requested information and data which are required to be held in compliance with the Client's due diligence requirements laid down in the Law;

2) it will, upon request, immediately provide to the requesting financial institution or another obliged entity copies of the documents relating to the identification of the Client or of the beneficial owner and other documents relating to the Client or the beneficial owner which are required to be held in compliance with the Client due diligence requirements laid down in the Law.

5.3 Client classification for due diligence purposes

All Clients should be classified according to the risks of being involved in money laundering or terrorist financing (TF).

Risk categorization shall encompass three different Customers' risk levels (low, medium, and high).

Such categorization shall be based on multiple parameters, including, but not limited to:

a) Client's identity;

b) Clients' residency (registration place, if Client is a legal entity);

c) Nature of business activity;

d) The actual location of business activities;

e) Client's (legal entity's) ownership and complexity of control structure;

f) Nationality of Beneficial Owner;

g) Volume and nature of transactions carried out by the Client;

h) Social/financial status;

The following Client risk classification is used:

5.3.1 Low-risk Clients:

a) In the cases specified by the European Supervisory Authorities and the European Commission.

b) In the cases where the Clients are legal persons whose securities are admitted to trading on a regulated market in one or more EU Member States;

c) In the cases where the Clients are entities of public administration – state and municipal institutions and institutions, the Bank of Hungary;

d) In the cases where the Client is a financial institution covered by the Law (or a financial institution registered in another European Union Member State).

e) The Client is identified as low risk in accordance with the Company's Risk Assessment Procedure.

5.3.2 Medium-risk Clients:

a) All other Clients are not identified as low or high risk.

5.3.3 High-risk Clients

The Clients are categorized as high-risk if one of the following criteria is applicable:

a) The Client or his/her representative or at least one of the Client's Beneficial Owners is a PEP;

b) During the identification procedure the Client avoids performing actions necessary for the verification of his/her identity and providing information about him/herself;

c) At the request of the Company, the Client did not provide the documents evidencing the financial activities (documents evidencing the transactions concluded or being concluded by the Client and other documents evidencing the financial activities performed or being performed by the Client);

d) The Responsible Employee of the Company establishes the existence of the features unusual to the ordinary activities performed by the Client (performance of monetary operations with larger amounts, complex transactions, transactions are carried out in an unusual pattern etc.);

e) The Clients' age, official position, status and/or financial condition (low income of the Client when compared with the extent of the Client's financial activities) do not comply objectively with the financial activities performed by the said Client;

f) If suspicion is raised during the monitoring of the Client's business relations with the Company.

g) The Client is determined to be of high risk in accordance with the Company's Risk Assessment Procedure.

5.4 Establishing a beneficial owner's identity

The Company shall always establish the identity of the Beneficial Owner of the Client (in

accordance with the Law and these Rules).

The Client shall submit the following data on the Beneficial Owner:

a) Name/names;

b) Surname/surnames;

c) Personal identification number (in the case of a foreigner: date of birth (where available – personal number or any other unique sequence of symbols granted to that person, intended for personal identification, the number and period of validity of the residence permit in the Republic of Lithuania and the place and date of its issuance);

d) Citizenship.

The data submitted by the Client shall be validated using electronic identification means issued in the European Union, which operate under the electronic identification schemes with the assurance levels high or substantial, or with a qualified electronic signature supported by a qualified certificate for electronic signature which conforms to the requirements of Regulation (EU) No 910/2014, or using electronic means allowing direct video streaming.

6. PROHIBITION TO ENTER INTO A BUSINESS RELATIONSHIP

It is forbidden to start a business relationship if the Client and/or his representative:

a) fails to submit the data confirming his identity;

b) submits not all the data or where the data are incorrect;

c) avoids submitting the information required for establishing his identity,

d) conceals the identity of the Beneficial Owner or avoids submitting the information required for establishing the identity of the Beneficial Owner or the submitted data are insufficient for that purpose;

e) the Company, due to the Customer's actions or omissions, is not able to ensure proper compliance with the Law and the related legal acts.

In such cases, the Company shall, upon assessment of the threat posed by money laundering and/or terrorist financing, decide on the appropriateness of forwarding a report on a suspicious monetary operation or transaction to the authority.

If the Company is unable to comply with the points above, the Company shall not conduct business relations with such Customer. In these cases, the Responsible Employee of the Company has to evaluate possible money laundering or terrorist financing threat and inform the CEO and the authority.

If the Customer avoids or declines a request by the Company to provide information on the source of assets, money and etc., the Responsible Employee has to inform the CEO. In that case, the CEO shall make a decision to terminate the Business relationship with the Customer and the Responsible Employee shall inform the authority. The Responsible Employee has a responsibility to take immediate action to interrupt money laundering and/or terrorist financing.

The information gained identifying the Customer and beneficiary owner, monitoring Customer activities have to be documented either physically or electronically.

7. IDENTIFICATION OF POLITICALLY EXPOSED PERSONS

The Company shall consider its Customers to be PEPs when at least one of the following criteria is met:

a) A citizen of the Republic of Hungary or the European Union declares that they have been entrusted with Prominent Public Functions or that they are Close Family Members or Close Associates of such a person;

b) The Company's employees determine that the natural person is a PEP by using public sources and (or) by obtaining such information from third parties, such sources may include, but are not limited to the Chief Official Ethics Commission and commercial databases which list PEP's;

c) A representative of a legal person declares that the shareholders (natural persons) of the legal person have been entrusted with Prominent Public Functions or that they are Close Family Members or Close Associates of such a person.

8. ENHANCED CUSTOMER IDENTIFICATION PROCEDURE

8.1 The enhanced Customer identification is performed:

a) Where transactions or Business relationships are carried out with a PEP;

b) In the cases indicated by the European supervisory authorities and the European Commission;

c) If according to the risk assessment and management procedures established by the Company a higher risk of money laundering and/or terrorist financing is determined. When assessing the risks of money laundering and/or terrorist financing, it is necessary to assess the risk factors of possible increased money laundering and/or terrorist financing identified in these Rules.

8.2 When applying an enhanced Customer identification procedure for Customers that are PEPs, the Company shall:

a) Identify whether the Customer and (or) the Beneficial Owner of the Customer are PEPs;

b) Get consent from the CEO of the Company to start or maintain a Business relationship with that Customer, when he becomes a PEP;

c) Take adequate measures in order to determine the source of assets and funds involved in Business relationships and contracts;

d) Ensure identification of unusual transactions and regular review of the information about such Customer and its Transactions that the Company holds;

e) Maintain enhanced activity monitoring of PEP's.

8.3 When a PEP stops holding important public positions, the Company shall, for at least 12 months, continue to consider the ongoing risks of that person and apply appropriate measures at the risk level, until it is determined that the person concerned no longer has the risk inherent in the Customer being considered a PEP.

8.4 When applying enhanced Customer identification procedure in the cases specified by the European Supervisory Authorities and the European Commission, the Company shall choose the measures referred to in the documents of the European Supervisory Authorities and the European Commission which identify such cases.

8.5 When applying enhanced Customer identification procedure if according to the Risk assessment procedure a high risk of money laundering and/or terrorist financing is determined, the Company shall in all cases:

a) Collect additional information on the Customer and/or its Beneficial Owner;

b) Collect additional information about the nature of the Business relationship;

c) Collect information about the purpose of the planned and/or executed Transactions;

8.6 Additionally, the Company in its discretion may apply any of the following measures in addition to the measures described in this Policy:

a) Take necessary measures to identify the source of the Customer's and Beneficial Owner's funds and assets related to the Business relationship or Transaction;

b) Obtain approval of the CEO for establishing or continuing the Business relationship;

c) Conduct enhanced ongoing monitoring of the Business relationship by increasing the number and timing of control applied, and by categorising types of Transactions that will need further investigation;

8.7 It is required to re-establish the Customer's identity using enhanced Customer identification procedure if:

a) The Customer knowingly provides wrong information about beneficiary or himself;

b) The Customer hides information.

9. ASSESSMENT OF THE RISK

9.1 The Company shall assess the risk of the operations being used for money laundering and terrorist financing.

9.2 The risk assessment shall be conducted on an annual basis.

9.3 Risk Assessment Procedure provided in the Risk Assessment Policy outlines the principal methodology which shall be used to conduct and update the risk assessment for purposes of anti-money laundering and terrorist financing prevention.

10. PERIODIC UPDATE OF CUSTOMER'S INFORMATION

10.1 By considering the Customer categorisation the Customer's information shall be updated and the Customer's identity shall be verified repeatedly:

a) If the Customer is a low-risk Customer – every 2 years;

b) If the Customer is a medium-risk Customer – every year;

c) If the Customer is high-risk Customers – every 6 months.

10.2 The Customer categorisation to the respective risk group shall be registered. When necessary, the data shall be updated.

11. MONITORING, PRESENTATION OF INFORMATION TO THE AUTORITHY, DETERMINATION AND SUSPENSION OF SUSPECTED MONEY OPERATIONS AND TRANSACTIONS

11.1 The Company gathers information about the Customer risk profile and expected behaviour when the Customer applies for Company's services. The gathered information provides information about the expected behaviour of the Customer and a baseline for the identification of suspicious activity.

11.2 When suspicious activity is identified, or the Customer otherwise has a suspicious behaviour or pattern that indicates a risk for money laundering, the Company shall seek to investigate the behaviour and to provide a rationale for the identified suspicious behaviour by asking the Customer for additional information to rule out inappropriate behaviour or attempt to launder money. Examples of questions that could be asked:

- What is the purpose of the requested financing?
- Where does the income/revenue come from?
- Why do you want the money to be transferred to this specific account?

11.3 The Company has identified indicators, presented below, which shall lead to an inquiry to find out more information about the rationale of the activity. When adequate information about the rationale behind the transaction or behaviours is collected and if the explanation seems reasonable a transaction may be performed. The Company shall notify the Authority of cases in which the Company:

a) Knows, receives information or has reasonable grounds to suspect that money

laundering and/or terrorist financing has been, is being or will be committed or has been attempted;

b) Suspects or has reasonable grounds to suspect that Customer's funds are derived from criminal activity;

c) Suspects or have reasonable grounds to suspect that transactions or activities involve terrorist financing.

11.4 The Company shall notify the Authority about the Customer's suspicious (and not only executed but also intended to be executed suspicious) transactions (irrespective of the size of the monetary transaction), taking into account:

11.4.1 Criteria for identifying money laundering and suspicious monetary transactions or transactions related to the **Customer behaviour**:

a) During the establishment of business relations, the Customer or his representative avoids providing the information necessary to determine his identity, hides the identity of the beneficiary or avoids providing the information necessary for determining the beneficiary, presents documents with doubtful authenticity, etc.;
b) It is difficult to obtain information or documents from the Customer necessary for the monitoring of business relations: it is difficult to contact the Customer, the Customer is often changing its place of residence and contact information; no one responds when trying to call the phone number provided by the Customer or his representative or it is permanently disabled; the Customer or his representative does not answer e-mails;
c) The Customer is not able to answer the questions asked about his/her financial activity or planned financial activity, its nature, and behaves too nervously;
d) The Customer declares his willingness to end the business relations with the Company when asked to provide the information necessary for monitoring his business relations;
e) The Customer refuses to provide data on the origin of money or attempted to do so and/or to substantiate it by appropriate documents
f) Several companies are registered at the address of the Customer or their representative.

11.4.2 Criteria related to monetary **transactions** or transactions executed by the Customer or his representative:

a) Monetary transactions or transactions do not correspond to the regular cooperation with the Company;

b) Customer identification data and information on performed Virtual Currency exchange operations or transactions in Virtual Currency, if the value of such monetary operations or transaction is equal to or exceeds EUR 125,000 or the equivalent amount in foreign or virtual currency, notwithstanding whether the

transaction is in one or more related monetary transactions. Several interconnected monetary transactions shall be considered to be several Virtual Currency exchange operations or transactions in Virtual Currency in one day, where the total amount of transactions and transactions is equal to or exceeds EUR 120,000 or the equivalent amount in foreign or virtual currency at the time of the transaction;

c) The Customer performs monetary transactions or transactions without a clear economic basis;

d) The Customer performs monetary transactions or transactions where it is difficult or impossible to identify the beneficiary;

e) The Customer, the Customer's representative, a person who is the beneficiary of a monetary transaction or transaction, is subject to financial sanctions in accordance with the Law on the Implementation of Economic and Other International Sanctions of the Republic of Hungary;

f) The age, current position, and financial status of the Customer (the Customer's income/revenue is small compared to the amount of his financial activity), objectively do not correspond to the financial activity performed by this Customer.

11.5 The Company shall inform the Authority about monetary transactions that do not meet any of the criteria mentioned above if the Company has a suspicion of a monetary transaction and/or Customer's activity. The suspicion may be caused by various objective and subjective circumstances, for example, the Customer carries out monetary transactions that are unusual for his activity, provides incorrect information about himself or a monetary transaction, and avoids providing additional information (documents).

11.6 Suspicious monetary transactions or transactions are objectively determined by focusing on the Customer's activities that by their nature may relate to money laundering and/or terrorist financing, also by the Customer and beneficiary identification and continuous monitoring of the Customer's Business relationships, including transactions, which were concluded during such relationships. In assessing whether a monetary operation or transaction is suspicious, the Company is not required to determine whether there is a criminal offence. The subjective allegations made by the employee of the Company are sufficient for the assessment.

11.7 If the employee of the Company finds that a monetary transaction or transaction performed by the Customer is suspicious, regardless of the amount of such transaction, immediately suspends this transaction and no later than within 3 business hours informs the CEO of the suspended transaction.

11.8 In case of knowledge or suspicion of suspicious monetary transactions or transactions, the Company shall immediately notify the Authority, no later than within three working hours after such knowledge or suspicion, if the Company knows or suspects that any value asset is directly or indirectly received from or involved in a criminal offence, also if the

Company knows or suspects that the assets are intended to support one or several terrorists or a terrorist organization.

11.9 The Company, upon receipt of written instruction from the Authority to suspend suspicious monetary transactions or suspicious transactions performed by the Customer, suspends these transactions from the time of notification or the moment of the specified circumstances up to 10 business days. The Responsible Employee of the Company submits instructions to the required employees of the Company.

11.10 Upon receipt of the Authority notification that the suspension of a monetary transaction or transaction may interfere with the investigation of money laundering or terrorist financing and other criminal acts related to money laundering and/or terrorist financing, the Company shall not suspend suspicious monetary transactions or suspicious transactions performed by the Customer and renew suspended monetary transactions or transactions from the time of notification or the moment of the specified circumstances.

11.12 Notification to the Authority regarding a suspicious monetary transaction or transaction shall include:

a) The identity of the Customer, his representative (if the monetary transaction is performed or the transaction is concluded through a representative);

b) Criteria approved by the Authority, according to which a monetary transaction or transaction is identified as suspicious;

c) A suspicious monetary transaction or a suspicious transaction;

d) The date of the suspicious monetary transaction or the suspicious transaction, the description of the assets in the transaction (money, etc.) and its value (amount of money, currency in which the monetary transaction or transaction is performed, etc.);

e) Account management methods;

f) Contact information (phone numbers, email addresses, contact persons, their telephone numbers, e-mail addresses) of the Customer, his representative (if the monetary transaction is carried out or the transaction is concluded through a representative);

g) The date and time of suspicious monetary operation or suspicious transaction suspension;

h) A description of the assets the Customer cannot manage or use from the suspicious monetary transaction or suspicious transaction suspension (location and other information describing the asset);

i) If the suspicious monetary transaction or transaction has not been stopped, – the reasons for not stopping it;

j) Another relevant information in the opinion of the Company.

11.13 A notification regarding information about suspicious monetary transactions or suspicious transactions shall be submitted to the Authority upon joining the Information System of the NAV and by filling in an electronic form (e-papír).

12. FINAL PROVISIONS

16.1 These Rules may be amended, supplemented or revoked by the decision of the CEO of the Company.

16.2 These Rules shall be reviewed periodically (at least once a year) or upon any substantial events related to the operation of the Company or changes to applicable laws, and shall be amended accordingly to ensure proper implementation of the money laundering and terrorist financing prevention measures, its effectiveness and relevancy. The Responsible Employee is responsible for the timely revision of the Rules and the preparation and submission of draft amendments to the CEO.

16.3 The Company conducts special training for the employees of the Company on issues related to the prevention of money and terrorist financing, as well as the proper implementation of these Rules.

16.4 All employees of the Company shall be familiarized with these Rules by signing it.

Last revision: 06/06/2023 – Variance HODLING Kft.

Csaba Csabai

CEO