INTERNAL RULES

FOR CONTROL AND PREVENTION OF MONEY LAUNDERING AND FINANCING OF TERRORISM OF

“BEAM GROUP” Ltd

UIC 207153602

city of Sofia

I. GENERAL PROVISIONS

1.1. “BEAM GROUP” Ltd is a sole-owned limited liability company, registered under Bulgarian legislation with UIC: 207153602 with seat and management address city of Sofia 1330, Razsadnik Konyovitsa residential area 87, enter. D, 8th floor, ap. 28, registered in the public register of the NRA of persons who, by occupation, provide exchange services between virtual currencies and fiat currencies and to custodian wallet providers under number BB-123/17.11.2022, referred to as “the Company”.
1.2. The Company follows strict anti-money laundering and counter terrorist financing rules governed by local and international laws and regulations in order to prevent any kind of illegal and criminal activities, and any potential involvement of the Company in those. Thus, “BEAM GROUP” Ltd implements this policy in accordance with the Measures Against Money Laundering Act (MAMLA).
1.3. The Company provides exchange services between virtual currencies and fiat currencies and is a custodian wallet provider. According to the applicable legislation, the provision of the specified services falls under the scope of Directive (EU) 2018/843 of the European Parliament and of the Council, as well as within the scope of the Measures Against Money Laundering Act which transposes Directive (EU) 2018/843.
1.4. As a result and in order to prevent and establish preventive measures against the use of the financial system for money laundering, the Company has developed internal rules for the control and prevention of money laundering and terrorist financing, which apply to the Company's activities and the customers.
1.5. These rules were adopted on the basis of Art. 101 of the MAMLA and MAFTA and regulate the actions of the Company in the implementation of control and application of measures for the prevention and detection of ML and TF. They set out processes and measures that manage and reduce the risk of money laundering and terrorist financing. These measures include, but are not limited to, customer identification and verification, ongoing customer monitoring and inspections, collection, preparation and storage of documents and data.
1.6. The rules establish clear criteria for recognizing suspicious operations or transactions and customers, the procedure for staff training and the use of technical means to prevent and detect ML and TF, the system of internal control over the implementation of measures against ML and/or TF, as well as the other circumstances under Art. 101, para. 2 of the MAMLA.

II. DEFINITIONS

2.1. “Applicable Laws” are the laws currently in force in the territory of the country in which the Company operates;
“Identification Document(s)” refers to:

national identity cards and passports and any other official identity document;
Documents that identify the registered address of a natural person or legal entity, such as, but not limited to, a bank statement and utility bill or other documents that may be specified and required by the Company;
"Politically Exposed Person" (PEP) is a natural person who performs or has been entrusted with the following prominent public functions in the Republic of Bulgaria, in another Member State or in a third country:
heads of state, heads of government, ministers and deputy ministers or assistant ministers;

members of parliament or of similar legislative bodies;

members of supreme courts, of constitutional courts or of other high-level judicial bodies, the decisions of which are not subject to further appeal, except in exceptional circumstances;

members of courts of auditors;

members of governing bodies of central banks;

ambassadors and chargés d'affaires;

high-ranking officers in the armed forces;

members of the administrative, management or supervisory bodies of State-owned enterprises or business companies whose sole owner is the State;

mayors and deputy mayors of municipalities, mayors and deputy mayors of districts and chairmen of municipal councils;

members of the governing bodies of political parties;

directors and deputy directors of international organisations, members of the board of directors or supervisory board of international organisations or persons with equivalent function in such organisations.

"Affiliates of a politically exposed person" are the persons who are in the following relationships with a PEP:
spouses or persons living in de facto cohabitation as spouses;

descendants of first degree and their spouses or persons with whom descendants of first degree live in de facto cohabitation as spouses;

ascendants of first grade and their spouses or the persons with whom ascendants of first degree live in de facto cohabitation as spouses;

second-degree collateral relatives and their spouses or persons with whom the second-degree collateral relatives live in de facto cohabitation as spouses;

a natural person who is the beneficial owner jointly with a person under para. 2 to a legal entity or other legal body or to another close commercial, professional or other business relationship with a person under para. 2;

a natural person who is the sole owner or the beneficial owner of a legal entity or other legal formation known to have been created for the benefit of a person under para. 2.;

"Sanction Lists" are lists of natural persons, legal entities and entire countries that are involved or suspected of involvement in illegal and criminal activities. Such lists are provided by OFAC, the EU, the UN, etc.

"Beneficial Owner" means:

a person who directly or indirectly owns a sufficient percentage of the shares, units or voting rights in that legal entity or other legal body, including through bearer shareholdings, according to § 2, para. 1, item 1 of the additional provisions of the MAMLA;

a person exercising control within the meaning of § 1c of the additional provisions of the Commercial Act;

a person exercising decisive influence in making decisions to determine the composition of the management and control bodies, transformation, termination of the activity and other matters of essential importance for the activity, according to § 2, para. 3 of the additional provisions of MAMLA;

a person who exercises ultimate effective control through the exercise of rights through third parties, including, but not limited to, granted by virtue of a power of attorney, contract or other type of transaction, as well as through other legal arrangements providing the possibility of exercising decisive influence through third parties , according to § 2, para. 4 of the additional provisions of MAMLA;

settlor, trustee, protector, beneficiary, or person in whose main interest the trust is set up or operates, or a person who ultimately exercises control over the trust by direct or indirect ownership or by other means, or a person holding equivalent or similar position to those referred to above;

a person on whose behalf and/or on whose account a given operation, transaction or activity is carried out and who meets at least one of the conditions specified in § 2, para. 1, items 1 – 3 of the additional provisions of MAMLA;

a person acting as a senior executive when no other person can be identified as the beneficial owner.

"Virtual Currencies" is a digital representation of value that is not issued or guaranteed by a central bank or a public authority, is not necessarily attached to a legally established currency and does not possess a legal status of currency or money, but is accepted by natural or legal persons as a means of exchange and which can be transferred, stored and traded electronically.

"Custodian wallet provider" means a natural or legal person or other legal entity that provides services to safeguard private cryptographic keys on behalf of its customers, to hold, store and transfer virtual currencies.

The words and expressions used in the Rules, which are not defined here, have the meaning given to them by Bulgarian law and EU law applicable in Bulgaria.

III. SUSPICIOUS OPERATIONS, TRANSACTIONS AND CUSTOMERS - CRITERIA

1. Suspicious operations and transactions involving money laundering and proceeds of criminal activity.

When implementing these rules, employees are guided by the following non-exhaustively listed criteria for recognizing suspicious operations and transactions that could involve money laundering and proceeds of criminal activity:

1.1. Refusal of a Customer to provide information on the reasons for an abrupt increase in the volume of orders.

1.2. The Customer submits a large number of orders for the purchase of Virtual Currencies, followed by a large number of orders for their sale or exchange with another type of Virtual Currency in a short period of time without economic justification.

1.3. The Customer submits one or more orders, such as related operations for the purchase of Virtual Currencies of large value, when the invested funds clearly do not correspond to its financial condition.

1.4. When using the service of providing a digital wallet for storing a large amount of Virtual Currencies which were not acquired through the Company and their value does not correspond to its financial condition.

1.5. The Customer systematically submits orders for the sale of Virtual Currencies below the price at which he purchased them without a clear economic justification.

1.6. The Customer simultaneously submits orders to buy and sell the same Virtual Currencies in the same or similar volume, without a clear economic reason.

1.7. When concluding transactions with Virtual Currencies, which, in view of the collected data for the Customer- a legal entity and its beneficial owner, do not correspond to its turnover and appear unusual in terms of amount, frequency and/or basis.

1.8. Carrying out multiple transactions in Virtual Assets for small amounts that are significant in aggregate.

1.9. Refusal of the Customer to use the usual order channels or request to change these channels without a clearly objective reason justified by the Customer.

1.10. Transactions with Virtual Assets or provision of a digital wallet for storage, where there is a suspicion that the Customer is acting on behalf of a third party, but refuses to provide information about such.

1.11. When using false identification/false documents to establish business relationships.

2. Suspicious customers involved in money laundering and proceeds of criminal activity. When implementing these rules, employees are guided by the following non-exhaustively listed criteria for recognizing suspicious customers that could involve money laundering and/or proceeds of criminal activity:

2.1. The Customer does not provide enough information about the transaction, or the provided documents and information contain clear discrepancies.
2.2. Customers who demonstrate unwillingness to provide information or the documents requested by the employees when concluding a contract/placing orders arouse suspicion about their authenticity;
2.3. Representatives or proxies of natural or legal persons present documents for identity and representative authority, the authenticity of which raises doubts.
2.4. The customer refuses to provide documents for his identification.
2.5. The personal documents submitted by the customer lack basic details to fully identify him.
2.6. The customer submits identification documents that appear to be forged.
2.7. The signature in the identity document does not match the signature affixed by the customer on the contract or relating to the transaction.
2.8. The customer does not present or attempts to delay the provision of certain declarations or certificates, including ones for good standing;
2.9. The customer attempts to develop close rapport with staff of the company by offering them money, presents or favors
2.10. The customer is accompanied and watched, or the transactions are being effected in the presence of third persons can arouse reasonable suspicion for applying pressure or threat.
2.11. Persons known from the media and other sources or suspected of engaging in illegal activities.
2.12. The customer tries to dissuade the employee of the company to register the necessary information about his identity when filling out contractual forms.
2.13. The customer and the beneficial owner are located in different jurisdictions and at least one of them is a jurisdiction associated with a higher risk of ML/FT.
2.14. Beneficiary funds are generated in a jurisdiction associated with a higher risk of the ML/FT, in particular when the jurisdiction is associated with higher levels of predicate offenses of ML/FT.
2.15. The customer’s funds originate from jurisdictions associated with a higher risk of ML/FT.
2.16. The Customer- legal entity or other legal body with an ownership structure, which includes nominal owners and managers or otherwise complicates the establishment of the beneficial owners and / or presupposes anonymity;

2.17. The customer or the beneficial owner of the customer is from a country for which information on high levels of corruption is available, or from a country subject to sanctions, embargoes or similar measures by the European Parliament and the Council or the Security Council of the Organization of the United Nations, as well as in the case of specific instructions from the European Union or the United Nations;
2.18. The customer or beneficial owner is from a country that does not apply or does not fully apply international standards in combating money laundering and terrorist financing.
2.19. When concluding a contract/opening an account with false identification and using false documents when ordering/receiving transfers.

3. Suspicious operations, transactions and customers that could be linked to or directed at terrorist financing

When implementing these rules, employees are guided by the following non-exhaustively listed criteria for recognizing suspicious operations, transactions and customers that could involve terrorist financing:
3.1. In case of partial matching of the identification data of a customer - natural person or beneficial owner with those of persons for whom negative information is available in databases or information from open sources that could be linked to a terrorist organization or individual terrorists (acting independently or developing propaganda activities).
3.2. The customer or its beneficial owner appears on the lists of the UN, EU and OFAC - US Department of Finance - for example, under Resolutions 1267, 1373 of the UN Security Council and subsequent resolutions or in the list under Art. 4b, item 3 of the Measures Against the Financing of Terrorism Act (MAFTA).
3.3. The Customer- legal entity or other legal body with an ownership structure, which includes nominal owners and managers or otherwise complicates the establishment of the beneficial owners and / or presupposes anonymity;
3.4. The customer or beneficial owner is from a country that does not apply or does not fully apply international standards in combating money laundering and terrorist financing.
3.5. When concluding a contract/opening an account with false identification and using false documents when ordering/receiving transfers..
3.6. Presentation of apparently new identification documents (the date of issue does not correspond to the condition of the document regarding its state of wear).
3.7. Transfers / transactions are not economically justified, given the nature of the account holder or his profession. For example, a natural person or company uses services or products that are not related to the subject of activity or cannot be linked to the operational needs for the relevant legal activity.

IV. CUSTOMER DUE DILIGENCE

4.1. Taking into account the results and findings of the NRA for the sector in which it operates, the Company will apply due diligence measures including enhanced due diligence. Simplified due diligence could be applied only in the cases provided for in Art. 27, 28 and 29 of the MAMLA, taking into account the requirements in the section.
4.2. The company will not apply the measures for a simplified due diligence under Art. 25 of the MAMLA.
4.3. The Company applies enhanced due diligence measures in relation to potential customers, existing customers and beneficial owners of a customer who is a legal entity or other legal body, who are PEPs in the Republic of Bulgaria, in another Member State or in a third country, or in international organizations, as well as in relation to potential customers, existing customers and beneficial owners of a customer - a legal entity or other legal entity that are associated with such PEPs within the meaning of the MAMLA. The enhanced due diligence measures applied by the Company are described in detail in Section VIII of these Rules, entitled "Internal system for establishing whether a potential customer, an existing customer or the beneficial owner of a customer - legal entity or other legal body - is a PEP. Measures regarding PEPs."
4.4. Customer due diligence includes the measures specified in Article 10 of the MAMLA, namely: identification of the customer/beneficial owner, including clarification of the purpose and nature of the business relationship, ongoing monitoring of the customer's operations, clarification of the origin of funds subject of the business relationship.
4.5. The identification of customers is carried out before establishing a business relationship, as well as in the following cases:

- in case of an occasional operation or transaction of a value equal to or exceeding the BGN equivalent of EUR 15,000 or their equivalent in another currency, regardless of whether the operation or transaction was carried out through one operation or through several related operations;
- in case of an occasional operation or transaction of a value equal to or exceeding the BGN equivalent of EUR 5000 or their equivalent in another currency, when the payment is made in cash, regardless of whether the operation or transaction was carried out through one operation or through several related operations;
- in case of an occasional operation or transaction, which is a transfer of funds (money remittance) according to Art. 3, item 9 of Regulation (EU) 2015/847 of the European Parliament and of the Council of 20 May 2015 on information accompanying transfers of funds and repealing Regulation (EC) 1781/2006 (OJ L 141/1 of 5 June 2015), amounting to or exceeding the BGN equivalent of EUR 1,000 or their equivalent in another currency.
- in case of an occasional operation or transaction which is an exchange between virtual currencies and recognized currencies without gold cover, amounting to or exceeding the BGN equivalent of EUR 1,000 or their equivalent in another currency;

The Company does not allow the opening or maintenance of an anonymous or fictitious account.

4.6. The company should document the actions taken for identity verification in a designated document, and the documents for the identity verification must also contain information about the date and time of the actions taken, as well as the names and position of the person who performed them.

V. IDENTIFICATION OF NATURAL PERSONS

5.1. Before establishing a business relationship with a customer, the Company identifies and verifies the customer's identification using the established "Know Your Customer" procedure. The Company requires identification information and documentation that the customer must provide.

5.2. Natural persons are identified by producing an official identity document and taking a copy of it. The company identifies customers in the following ways:

names;

date and place of birth;

official personal identification number or other unique element for establishing the identity, contained in an official identity document, the term of validity of which has not expired and on which there is a photo of the customer;

any citizenship that the person possesses;

country of permanent residence and address (a post office box number is not sufficient).

current address;

information about the employment status and professional activity of the person;

the expected scale of the planned transactions;

information about the origin of funds and the purposes for establishing business relationships with the Company.

5.3. When the identification is performed without the presence of the identifiable natural person, the identification may also be performed by presenting a copy of an official identity document and additional documents. In these cases the verification of the collected identification data shall be carried out by the order of art. 55, para. 2 of the MAMLA.

5.4. In relation to the legal representatives of a customer – legal entity or other legal body, the proxies and other legal representatives of natural persons, proof of their powers of representation is required and the same identification measures are applied that apply to natural person customers, and when it is necessary to take measures resulting from the national, supranational risk assessment and guidelines, decisions or documents adopted by EU institutions, requirements and exceptions to this rule may also be applied, according to the RIMAMLA.

VI. IDENTIFICATION OF LEGAL ENTITIES AND OTHER LEGAL BODIES

6.1. In identifying legal entities and other legal bodies, the following data shall be collected:

name and legal form;
country of establishment of the entity;
unique identification number of the entity;
management address, correspondence address and address for tax purposes of the entity;
e-mail address, website and telephone number of the entity;
information about the activity of the entity;
information about the ownership structure of the entity;
the expected scale of the planned transactions;
information about the origin of funds and the purposes for establishing business relationships with the Company.
The representative of the legal entity is obliged to provide information about the beneficial owners, legal representatives and other persons who exercise control over the respective legal entity.

6.2. In relation to the legal representatives of a customer – a legal entity or other legal body, the proxies are required to have a document certifying the representative authority, if such is not available in a public register or other official database.

VII. IDENTIFICATION OF BENEFICIAL OWNERS

7.1. The identification of the beneficial owner of a customer – legal entity or other legal body, is carried out by collecting the following documents and making the following inquiries:
the full name of each owner with at least 25% control of the company;
an official identity document (such as an ID card and an international passport) that contains a photograph, nationality, date of birth and a unique citizen number issued by the relevant country.

7.2. In case the legal entity is owned by another legal entity, the Company also requires:
extract from a commercial register;
memorandum/articles of association;
a document certifying the address of the company (bank account statement, electricity/water bill or other utility bills);
information about the ownership structure.

7.3. Additional verification measures
Declaration of the origin of the funds and an accompanying document that clarifies them. Statement from the relevant register referred to in Article 63 and the documents referred to in Article 64 of the MAMLA;

VIII. INTERNAL SYSTEM FOR ESTABLISHING WHETHER A POTENTIAL CUSTOMER, AN EXISTING CUSTOMER OR THE BENEFICIAL OWNER OF A

CUSTOMER - LEGAL ENTITY OR OTHER LEGAL BODY - IS A PEP. MEASURES REGARDING PEPS.

8.1. The Company's internal system for establishing whether a potential customer, an existing customer or a beneficial owner of a customer - legal entity or other legal body is a PEP or a PEP associate is based on one or more of the following sources of information:
8.1.1. Information obtained through the application of enhanced due diligence measures;
8.1.2. a written declaration completed by a customer/beneficial owner of a customer in order to establish whether the person falls into one of the categories under Art. 36 of the MAMLA. The declaration can be provided to the Company by the customer, the proxy, and/or legal representative/beneficial owner.
8.1.3. information obtained through the use of internal or external databases, such as a publicly disclosed list of persons under Art. 36, paragraph 2, created and maintained by the Financial Intelligence Directorate of the State Agency National Security, Worldcheck, https://namescan.io/FreePEPCheck.aspx, etc. similar.
8.2. The company applies at least two of the methods under item 8.1 to establish whether the customer or the beneficial owner of the customer - legal entity or other legal body is a PEP or a PEP associate.
8.3. Before entering into a business relationship, the Company requires each potential customer and/or his legal representative in the case of a potential customer - legal entity to fill out a PEP declaration according to the declaration form under the RIMAMLA in order to establish whether a potential customer or its beneficial owner is a PEP.
8.4. The company classifies as high-risk and applied enhanced due diligence measures in relation to potential customers, existing customers and beneficial owners of a customer who is a legal entity or other legal body, who are PEPs in the Republic of Bulgaria, in another member state or in a third country, or in international organizations , as well as in relation to potential customers, existing customers and beneficial owners of a customer - a legal entity or other legal body that are associated with such PEPs.
8.5. In order for the Company to enter into a business relationship with PEPs, approval is required from the person performing the functions of the Specialized Service pursuant to the MAMLA, namely the Manager, according to Art. 107, para. 2 of the MAMLA, and when preparing a risk assessment of a PEP customer, the latter is always considered high-risk, regardless of the total weight of the other risk factors.
8.6. In cases where, after establishing a business relationship, it is established that a customer or the beneficial owner of a customer - legal entity or other legal body - is a PEP, the continuation of the business relationship can only take place after approval by the person performing the functions of the Specialized Service under the MAMLA, namely the Manager, according to Art. 107, paragraph 2 of the MAMLA.

IX. PROCEDURE FOR THE USE OF TECHNICAL MEANS FOR THE PURPOSE OF PREVENTING AND DETECTING MONEY LAUNDERING;

9.1. Based on the collected documents and information, employees perform manual inspections to ensure that the data provided is complete, true and accurate.
9.2. The Company does not provide services to natural persons, companies and countries that are included in international sanctions lists, and in this regard the Company checks its customers against the relevant lists of the United Nations, the European Union, and the Office of Foreign Assets Control (OFAC) as well as other sanctions lists.
In order to identify politically exposed persons among its customers, the Company does not rely only on declarations provided by the customers, but also checks all natural persons and all beneficial owners in various domestic and international PEP lists and databases such as a publicly disclosed list of persons under Art. 36, para. 2, created and maintained by the Financial Intelligence Directorate of the State Agency National Security, https://namescan.io/FreePEPCheck.aspx , etc.
9.3. The Company shall take appropriate action to clarify the source of assets of a customer or the beneficial owner of a customer who is identified as a PEP. Such appropriate actions may be:
9.3.1. submission of a questionnaire - declaration to clarify the source of assets;
9.3.2. check in public registers for owned property (e.g. check in the Commercial Register, Property Register at the Registry Agency or public declarations under CCUAAFA or similar foreign registers);
9.3.3. other appropriate measures, e.g. verifying the source of assets and the origin of funds based on reliable and independent data (e.g. the Company requiring the customer to provide documents for verification and comparing them with available information from a public register), documents or information when the risk associated with the relationship with a PEP is particularly high.
9.4. To clarify the source of assets of a customer or beneficial owner of a customer who is identified as a PEP and if a publicity mechanism is in place, the Company shall perform a periodic review and comparison between the information on the declared property of the customer or the beneficial owner of the customer and the information established as a result of the application of the due diligence measures.
9.5. The source of funds shall be established by applying at least two of the following methods:
-. collecting information from the customer about the core activity thereof, including about the actual and expected volume of transactions and of the operations or transactions that are expected to be carried out in the course of the relationship, by means of completing a questionnaire or by other appropriate means;
- collecting other information from official independent sources: data from publicly available registers and databases, etc.;
- use of information collected in connection with the implementation of the requirements of the MAMLA or other laws and by-laws which shall show a clear origin of the funds;
- tracing the cash flows in the course of the business relationship established with the customer, whereupon an explicable source of funds is evident, where applicable.
9.6. In case of impossibility to identify the origin of the funds after exhaustion of the methods above as well as in the cases where the application of at least two of these methods has led to contradictory information, the origin of the funds shall be identified by written declaration from the customer or their legal representative or

proxy. The declaration should contain the required elements according to the model of the declaration under RIMAMLA.
9.7. Checking the validity of the customer's identity documents and those of the customer's beneficial owner (when his documents are available) on the website of the Ministry of the Interior https://www.mvr.bg , and for foreign persons, on the website maintained by the Council of the European Union https://www.consilium.europa.eu/prado/en/check-document-numbers.html

9.8. When applying a non-face-to-face method of identification:
9. 8.1. The company requires from any natural person who wishes to be identified with a non-face-to-face method to provide a handwritten statement that the documents are his personal documents and are provided at his will and not under threat or coercion.
9.8.2. When applying the non-face-to-face method of identification, all communication and all documents that the individual sends to the Company are sent via email, agreed between the parties in a contract, agreement.
9.8.3. With a view to fulfilling the requirements of Article 41, Paragraph 4, Item 5 of the RIMAMLA, non-face-to-face customer identification is allowed if:
9.8.3.1. the person uses a qualified electronic signature within the meaning of Article 3, item 12 of Regulation (EU) 910/2014 and the identity documents that the customer sends are official identity documents containing security elements;
or
9.8.3.2. the person uses electronic statements signed with an electronic signature within the meaning of Article 13 of the Electronic Documents and Electronic Authentication Services Act, through which he sends official identity documents containing security elements and a document, including through the Company's electronic portal or platform;
9.8.4 The Company establishes the customer's location by requesting a document containing a current address. The document can be issued by a credit institution, and/or a document certifying the charging or payment of a utility service, and/or a screenshot of a location from the address.
9.9. The risk assessment of non-face-to-face customer identification is assumed to be “medium risk” on a three-level scale (low, medium, high). The reasons for this are as follows:
- The company has taken sufficient measures to ensure that, even in case of the slightest doubt in relation to the presented documents, it will require the physical presence of the person in the office;

9.10. In the event that the Company introduces new products, business practices, delivery channels, as well as before starting to use new technologies for its business with new or already existing products, business practices and delivery mechanisms, it should carry out an assessment of the resulting risks, according to Art. 30 of the RIMAMLA, which is approved by an employee in a senior management position, realized in a separate document and stored according to the procedure provided for in the MAMLA.
9.11. The assessment is updated periodically, according to the established risk, analogous to the established deadlines for updating the customers’ risk profiles of in these rules, as well as

in any case when changes occur that have an impact on the level ML/TF risk resulting from the introduction and use of the products, practices, technologies or mechanisms.

X. INTERNAL SYSTEM FOR RISK ASSESSMENT AND DETERMINING THE RISK PROFILE OF CUSTOMERS

10.1. In order to assess the type, degree and volume of the applied customer due diligence measures according to chapter two of the MAMLA, the Company determines the risk profile of the customer by identifying and assessing the risks that arise from establishing a business relationship with the customer. The Money Laundering/Terrorist Financing (ML/FT) risk assessment process includes three stages: identification, analysis and assessment of risks.
10.2. In order to assess the risks of entering into a relationship with the respective customer, the Company considers the following categories of risk factors:
Category 1 - the customer and the beneficial owner of the customer (if any)
Subcategory 1 - the risk factors that are taken into account to identify the risks related to the type and behavior of the customer or its beneficial owner, may include some of the factors specified in art. 17, para. 4 of the RIMAMLA.
Subcategory 2 - the risk factors that are taken into account to identify the risks related to the economic or professional activity of the customer or its beneficial owner, may include some of the factors specified in art. 17, para. 2 of the RIMAMLA. In the event that the customer or its beneficial owner is a PEP or a person associated with a PEP according to the MAMLA, it is classified as a high risk of money laundering and terrorist financing.
Subcategory 3 - the risk factors that are taken into account to identify the risks related to the reputation of the customer or its beneficial owner, may include some of the factors specified in art. 17, para. 3 of the MAMLA.

The rating numbers of the Subcategories in Category 1 can be from 1 to 5, where 1 (low risk), 2 (moderate), 3 (higher), 4 (increased), 5 (high risk) or 50 if a customer is a PEP or a person associated with a PEP there is always high risk and enhanced due diligence is applied.

Category 2 - the country or geographical area in which the customer or its beneficial owner, its main partners are registered, established or reside, or in which the customer or its beneficial owner carries out its business or professional activity or with which it is otherwise connected.
Subcategory 1 - the risk factors that are taken into account to identify the risks related to the efficiency of the ML/TF prevention systems, may include the factors specified in art. 17, para. 2 and 3 of the MAMLA.
Subcategory 2 - the risk factors that are taken into account to identify the risks related to the level of the TF risk, may include the factors specified in Art. 18, para. 4 of the MAMLA.
Subcategory 3 - the risk factors that are taken into account to identify the risks related to the transparency of and degree of the compliance with tax legislation, may include the factors specified in Art. 18, para. 5 of the RIMAMLA.
Subcategory 4 - the risk factors that are taken into account to identify the risks related to the level of criminal activity predicate to money laundering may include the factors specified in Art. 18, para 6 of the RIMAMLA.

The rating numbers of the Subcategories in Category 2 can be from 1 to 5, where 1 (low risk), 2 (moderate), 3 (higher), 4 (increased), 5 (high risk) or 100 if a customer is present in the lists of the MAFTA, EU, UN, OFAC, the Company refuses to enter a contract and/or carry out the transaction/operation.

Category 3 - the products and services that are offered to the customer, as well as the usual types of transactions or operations carried out by the customer.
Subcategory 1 - the risk factors that are taken into account to identify the risks related to the transparency of the respective product, service, transaction or operation, may include the factors specified in Art. 19, para. 2 of the RIMAMLA.
Subcategory 2 - the risk factors that are taken into account to identify the risks related with the degree of complexity of the respective product, service, transaction or operation may include the factors specified in Art. 19, para.3 of the RIMAMLA.
Subcategory 3 - the risk factors that are taken into account to identify the risks related to the amount or value of the respective product, service, transaction or operation may include the factors specified in Art. 19, para. 4 of the RIMAMLA.

The rating numbers of the Subcategories in Category 3 can be from 1 to 5, where 1 (low risk), 2 (moderate), 3 (higher), 4 (increased), 5 (high risk).

Category 4 - the delivery channels used for the customer for the Category 3 products, services, transactions and operations.
The risk factors that are taken into account to identify the risks related to delivery channels may include the factors specified in Art. 20, para. 2 of the RIMAMLA.

The rating numbers of the Subcategories in Category 4 can be from 1 to 5, where 1 (low risk), 2 (moderate), 3 (higher), 4 (increased), 5 (high risk).

10.3. **Calculating the customer's risk score**
The customer score is calculated as follows:
10.3.1. The risk of establishing a business relationship with the customer is “low” if the overall level of risk has a percentage weight of up to 30% according to the rating system. 10.3.2. The risk of establishing a business relationship with the customer is “medium” if the overall level of risk has a percentage weight of 30% to 49% according to the rating system. 10.3.3. The risk of establishing a business relationship with the customer is “high” if the overall level of risk has a percentage weight of 50% to 100% according to the rating system. 10.3.4. The risk of establishing a business relationship with the customer is “unacceptable” if the overall level of risk has a percentage weight above 100% according to the rating system.

10.4. The risk score for the risk of money laundering/terrorist financing of a customer in the Company is calculated by evaluating the risk factors in item 10.2 and placing a rating number against each reported factor. The assigned rating numbers are summed and the resulting result is divided by the number of reported risk factors. The obtained average rating number of the

overall customer profile is reflected in a percentage that shows the determined weight of ML/TF risk on the customer's profile.
10.5. Regardless of the result obtained from the calculations based on the presence/absence of the specified risk factors, the Company can always, at its own discretion, give a different level of risk assessment to a given customer when all the collected data and information about him require so.
10.6. The customer risk score is updated with the following frequency:
- if the overall risk of establishing a relationship with the customer is low - the score is updated every 2 years.
- if the overall risk of establishing a relationship with the customer is medium - the score is updated every 1 year.
- if the overall risk of establishing a relationship with the customer is high - the score is updated every six months.

XI. THE TIME INTERVALS OVER WHICH THE DATABASES AND CUSTOMER DOSSIERS ARE REVIEWED AND UPDATED IN IMPLEMENTATION OF ART. AND 16 OF THE MAMLA, TAKING ACCOUNT OF THE LEVEL OF RISK OF THE CUSTOMERS AND THE BUSINESS RELATIONSHIPS IDENTIFIED AND DOCUMENTED ACCORDING TO THE PROCEDURE ESTABLISHED BY ART. 98 OF THE MAMLA

11.1. The Company keeps up-to-date the information collected through the application of the due diligence measures for its customers and the operations and transactions carried out by them, applying the due diligence measures, including when the Company becomes aware that there has been a change in the circumstances regarding a customer.
11.2. The company updates the information it stores with the following frequency: 11.2.1. The customer's risk score is updated according to the established risk level.
11.2.2. Information about a customer or a beneficial owner of a customer who is a PEP is updated every six months or more frequently if necessary.
11.2.3. The databases and customer files in which the Company stores the information it has collected about a customer or the beneficial owner of a customer in the course of performing due diligence are updated in accordance with the established level of risk and the legal obligations arising from the established relationship.
11.3. Where necessary, the Company shall verify the information as up to date and take further action to identify and verify the identity in accordance with the requirements of the MAMLA and RIMAMLA, when:
11.3.1.An operation has been performed at a value different from the usual for the customer;
11.3.2. there is a significant change in the manner in which the account is used or in the manner in which particular operations or transactions are carried out;
11.3.3. the Company becomes aware that the information available for an existing customer is insufficient for the purposes of implementing due diligence measures.
11.3.4. The Company becomes aware that there is a change in the circumstances established through due diligence measures, in relation to the customer. In the event that any of the above

conditions are met, the Company checks that the information is up to date and performs the necessary additional actions to verify the identification after the corresponding precondition has occurred.

XII. POLICIES, CONTROLS AND PROCEDURES TO MITIGATE AND MANAGE EFFECTIVELY THE RISKS OF MONEY LAUNDERING AND TERRORIST FINANCING IDENTIFIED AT THE LEVEL OF THE EUROPEAN UNION, AT THE NATIONAL LEVEL AND AT THE LEVEL OF THE COMPANY

12.1. The company prepares and updates its own assessment of the risk of ML/TF in accordance with the requirements of the MAMLA and RIMAMLA, realizing it in a separate document and accepting it according to the procedure set out in these Rules. The Company maintains its ML/TF risk assessments related to individual business relationships with customers, as well as the key factors considered, to ensure that its own ML/TF risk assessment is up-to-date and appropriate. The Company evaluates information received as part of its ongoing monitoring of business relationships and assesses whether this impacts its own risk assessment.
12.2. The Company's risk assessment with regard to ML/TF takes into account the results and specifications in the Supranational Risk Assessment, the National Risk Assessment of ML and TF and their updates, as well as the recommendations of the European Commission.
12.3. The Company’s risk assessment was prepared taking into account the following risk factors: a) the type of offered products, services, transactions, delivery operations; b) customer structure and method of contact with customers; c) the countries or geographical areas from which the customers are; d) delivery channels and lack of anonymity; e) previously fulfilled obligations under the MAMLA, existence of rules and conducted trainings in the field of AML/CFT f) supervision.
12.4. The company updates its own risk assessment every two years. The assessment is also updated in the following cases:
- publication of a national risk assessment and/or amendment of the supranational risk assessment and other material documents on the basis of which it was prepared;
- the occurrence of a significant change in the products, services and delivery channels provided or used or in relation to customers and geographical factors; - within the framework of their control activities, the supervisory/inspecting authorities identifying violations of the MAMLA, MAFTA and RIMAMLA, which affect negatively the risk assessment carried out by the Company;
- occurrence of other events or factors that could be material to the overall level of risk arising from the Company's operations.
- control systems and mechanisms that the Company introduces in order to identify emerging risks:
- the collected information on current customers according to the MAMLA is periodically reviewed by trained employees and/or the Manager, to establish trends and emerging problems, in connection with individual business relationships and the Company's activities;
- The employees are trained in accordance with the adopted plans for annual trainings under the RIMAMLA.

XIII. TERMS AND PROCEDURE FOR THE COLLECTION, RETENTION AND DISCLOSURE OF INFORMATION

13.1. Collecting information

The company collects information from and about the (potential) customer when performing due diligence on the customer and beneficial owner, when updating the data on the customer and beneficial owner, and when clarifying the origin of funds and the source of assets, when the customer or beneficial owner is a PEP.

Prior to establishing a business relationship the Company provides customers with information about the purposes for which their personal data will be processed.

The company shall delete or destroy the personal data processed by them after the expiration of the storage period according to the MAMLA, unless a special law provides otherwise.

13.2. Information storage

The company fulfills all the requirements for the storage of the documents collected under the MAMLA and RIMAMLA, as required by these acts.

The company shall store for a period of 5 years all documents, data and information collected and prepared in accordance with these rules, MAMLA and RIMAMLA, including documents and data received in connection with the identification carried out. The term begins to run from the date of termination of relations with the customer.

The company applies the terms of storage of documents according to Art. 67 of the MAMLA.

13.3. Disclosure of information

In the event of suspicion and/or knowledge of money laundering and/or the presence of proceeds of criminal activity and/or in the event of suspicion of TF, the Company shall immediately notify the FID. The notification is sent according to the FID's standard form. The notification is sent by the Manager, appointed to perform the functions of internal control over the implementation of the MAMLA and RIMAMLA in the Company, according to Art. 107, paragraph 2 of the MAMLA. The customer is not notified of the notification sent to the Financial Intelligence Directorate (FID).

Every employee of the Company is obliged to notify the Manager in case of suspicion and/or knowledge of money laundering and/or the presence of proceeds of criminal activity. The employee is obliged to notify immediately. The Manager in the capacity of performing the functions of internal control over the implementation of the MAMLA and RIMAMLA under Art. 107, para. 2 of the MAMLA for the Company processes the information received from the employee, and upon conclusion that there is indeed suspicion and/or knowledge of money laundering and/or the presence of proceeds of criminal activity, the Company immediately notifies the FID.

Upon learning of ML or the presence of proceeds of criminal activity, the Company shall also notify the competent authorities in accordance with the Criminal Procedure Code, the Ministry of Interior Act and the State Agency for National Security Act.

In cases when the delay of the operation or transaction is objectively impossible or is likely to frustrate the actions of prosecuting the beneficiaries of a suspicious transaction or operation, the Company notifies the FID immediately after its execution, stating the reasons due to which delay was impossible.

The notification to the FID can also be carried out by any employee of the Company, when the employee has suspicions or is aware of ML and/or the presence of proceeds of criminal activity.

Any employee of the Company who knows that certain operations or transactions are aimed at TF is obliged to immediately notify the Minister of Interior and the Chairman of the State Agency for National Security.
In case of suspicion of financing of terrorism, the Company is obliged to identify the customers and verify their identification under the suspicious operation or transaction pursuant to Chapter Two, sections V and VI of the MAMLA, to collect information about the essential elements and the value of the operation or transaction, the relevant documents and other identification data and to notify immediately the FID before performing the operation or transaction, delaying its execution within the allowable period according to the regulations governing the respective type of activity.
The obligation to notify also applies to the attempt to carry out an operation or transaction aimed at FT as well as to the means suspected of being linked to or used for terrorist acts or by terrorist organizations and terrorists.
13.4. The company maintains a log in which it records:
- any notification by an employee of suspected money laundering or of the presence of proceeds of criminal activity or of terrorist financing, regardless of the manner in which the notification was made, together with a conclusion on the need to report the suspicion pursuant to Art. 72 of the MAMLA. The log can be maintained on paper or electronic media subject to compliance with the requirements of RIMAMLA.
- the company, the persons who manage and represent it and its employees cannot notify their customer or third parties about the disclosure of information.
- employees of the Company who submit internal reports of potential or actual violations of the MAMLA, the MAFTA and the acts on their implementation benefit from the protection provided for in Article 86 of the MAMLA.

XIV. SYSTEM OF INTERNAL CONTROL OVER THE FULFILMENT OF OBLIGATIONS ESTABLISHED IN THE MAMLA, MAFTA AND IN THE ACTS FOR THERI IMPLEMENTATION

14.1. The functions of internal control over the fulfillment of the obligations established in the MAMLA, MAFTA and the instruments for their implementation are performed by the Company's Manager, according to Art. 107, paragraph 2 of the MAMLA.
14.2. The persons under item 14.1. are subject to fit and proper verification before being

appointed to the respective position and to an ongoing evaluation for handling their assigned activities.
14.3. The company, through the sole proprietor, verifies his/her professional competence by requesting information on previous professional experience related to AML/CTF or a document of completed training in the same field.
14.4. The reliability of the person/s is certified by presenting a conviction record certificate or other official document, from which it is clear that the person has not been convicted of crimes related to ML and TF and against the financial system, or an analogous document for the persons who are not Bulgarian citizens.
14.5. The current assessment of persons under item 14.1. is certified by means of a document evidencing at least 10 hours of annual training in relation to countering ML and TF, which may include internal or external trainings/webinars and other forms.

XV. RULES FOR THE TRAINING OF THE OTHER EMPLOYEES WHOSE ACTIVITIES ARE RELATED TO THE FULFILLMENT OF DUTIES FOR COUNTERING MONEY LAUNDERING AND THE FINANCING OF TERRORISM

15.1. The company has adopted a training plan for the employees whose duties are related to the implementation of the MAMLA, the MAFTA, the acts on their implementation and these Rules, according to which the employees participate in introductory, continuing and current training.
15.2. The training plan under item 15.1 is prepared, updated and approved by the Company Manager.
15.3. The plan determines the frequency and training that the Company will organize for its employees, with a view to their preparation in matters related to the prevention of ML and TF.
15.4. The company organizes the following trainings for its employees:
- introductory trainings - every new employee becomes familiar with the Company's internal rules under the MAMLA and MAFTA.

- ongoing training – trainings aimed at informing employees about current changes in the legislation related to ML and TF, explaining and acting out practical scenarios, etc.
- current practical trainings - they are aimed entirely at discussing and replaying case studies that the Company's employees have had.
15.5. The employees the Company 14.1. are subject to fit and proper verification before being appointed to the respective position and to an ongoing evaluation for handling their assigned duties.
15.6. The company verifies their professional competence by requesting information on previous professional experience related to AML/CTF or a document of completed training in the same field.
15.7. The reliability of prospective employees whose activities are related to countering ML and TF is certified by presenting a conviction record certificate or other official document, from which it is clear that the person has not been convicted of crimes related to ML and TF

and against the financial system, or an analogous document for the persons who are not Bulgarian citizens.

15.8. The current assessment of current employees is carried out by the Manager in connection with his functions under item 14.1 by means of certifying at least 10 hours of annual training in relation to countering ML and TF, which may include internal or external trainings/webinars and other forms.

XVI. ALLOCATION OF RESPONSIBILITIES AMONG THE REPRESENTATIVES AND EMPLOYEES OF THE COMPANY FOR THE FULFILMENT OF THE OBLIGATIONS ESTABLISHED IN THE MAMLA, THE MAFTA AND IN THE ACTS FOR THEIR IMPLEMENTATION, AS WELL AS CONTACT DETAILS OF THE COMPANY AND OF THE RESPONSIBLE REPRESENTATIVES AND EMPLOYEES THEREOF AND PERSONS IN A COMPARABLE POSITION ENGAGED IN ITS ACTIVITIES ON OTHER GROUNDS, FOR THE PURPOSES OF THE MAMLA, THE MAFTA AND OF THE ACTS FOR THEIR IMPLEMENTATION

16.1 The company has determined the distribution of responsibilities and the fulfillment of the duties of the representatives and employees in connection with the MAMLA, MAFTA and the acts on their implementation.

- The sole owner of the capital - designates the Manager as a person who performs the functions of control over the fulfillment of the obligations established in the MAMLA, MAFTA and the acts for their implementation and, verifies that he meets the fit and proper requirements of the law and these Rules, accepts and amends these Rules and Risk Assessment.
- The Manager - discusses and approves the signals related to ML and TF, which the Company sends to the FID; verifies the fit and proper requirements of employees whose activities are related to countering ML and TF;
- Customer Service Department

Whenever the customer service department accepts documents of a new customer, if in doubt what due diligence should be done on the customer and what documents should be required from him, they consult the head of the department or the Manager. In all matters related to the MAMLA, the MAFTA and the acts for their implementation, the department acts according to the instructions of the Manager.

- The manager performs the functions under Art. 107, paragraph 2 of the MAMLA, has the obligations according to Art. 106 of the MAMLA and all departments cooperate with him.

XVII. PROCEDURE FOR ANONYMOUS AND INDEPENDENT SUBMISSION OF WHISTLEBLOWING REPORTS BY EMPLOYEES ABOUT VIOLATIONS OF THE MAMLA, MAFTA AND THE ACTS FOR THEIR IMPLEMENTATION

17.1. The company creates and maintains a log for submission of anonymous whistleblowing reports by employees engaged in its activity for violations of the MAMLA, MAFTA and the acts for their implementation.

17.2. Every employee has the right to submit an anonymous report for violations of the MAMLA, MAFTA and the acts for their implementation to the Manager. The signal is registered in the Company's log with a reference number and date of receipt. In a reasonable time, but not later than 2 (two) working days, the report is reviewed by the Manager. At his discretion, the case is investigated and further actions are taken, for example for notification under Art. 72 of the MAMLA, if the legal requirements for this are present.
17.3. The Company guarantees the anonymity and protection of the whistleblowing employee, even if his/her identity is accidentally disclosed.

XVIII. REPORTING RESULTS FROM THE COMPANY'S OWN RISK ASSESSMENT AND THE SUPRANATIONAL AND NATIONAL RISK ASSESSMENT REGARDING MONEY LAUNDERING AND THE TERRORIST FINANCING

18. The company has taken into account the conclusions and recommendations made in the updated Supranational Risk Assessment of Money Laundering and Terrorist Financing and National Risk Assessment of 2023 and complied with them when preparing its own risk assessment under Art. 98 of the MAMLA, as well as in the update of the current Internal Rules. The main money laundering risk events that have been identified with the virtual asset sector assessment are also taken into account, including:
1. Laundering proceeds generated by investment fraud or exploiting the inherent characteristics of virtual assets to mislead victims into investing in fiat currencies or virtual assets with get-rich-quick promises.
2. Laundering of proceeds from criminal activity by companies posing as VASPs without a license/registration to carry out such type of activity.
3. Persons engaged in illegal activities register online with foreign VASPs operating as centralized exchanges and use services such as exchange between fiat currency and VA, between one or more forms of VA and transfer of VA to deposit or convert fiat currency or VAs acquired through criminal activity.
4. Money laundering by exchanging fiat currency for virtual asset types, such as Bitcoin, Ethereum and Stablecoins, which have high liquidity and usability (in terms of exchangeability) without significant risk of loss of value of the proceeds of criminal activity.
5. Organized crime using of persons of low social and economic status to act as “financial mules” to launder proceeds of criminal activity through exchanges between virtual assets and fiat currencies and between one or more types of virtual assets for the benefit of the criminal network.
6. Money laundering through ordered/received funds on payment accounts of local natural persons (including in favor of third parties), through transfers from/to VASPs, related to trading in virtual assets of high value or with high frequency.

18.1. The Company believes that the Company's ML/TF risk assessment is high due to the inherent risk of the field of activity and taking into account the findings and specifics of the update of the NRA, SNRA and the Sectoral Assessment for Virtual Currencies. The sector offers the possibility of anonymity and the lack of detailed data on their use, the wide

geographical diversification and the disadvantages of non-face-to-face customer identification. The lack of security of virtual currencies and the underdeveloped regulatory framework allow their abuse for criminal purposes. In order to manage the high risk, the Company has introduced a system of mechanisms and controls for its management by applying due diligence, enhanced due diligence, requiring additional documents and information, and others, described in these rules. In case of suspicion regarding ML and TF, additional documents are required, and if the suspicion is still present the conclusion of a contract and the establishment of business relationships may be refused, and a notification may be sent to the competent authorities. The currently implemented mechanisms and controls for managing the risk of ML and TF are deemed to be sufficient for the management of the inherent risks of the field of activity.

18.2. When preparing its risk assessment, the Company took into account that it still has no registered customers and concluded transactions, therefore it considers that it is currently not under threat from ML and TF but considers that in relation to its overall activity, the inherent risk is high for the above stated reasons. The company monitors the development of the applicable legislation in order to minimize the risk of possible incompetence or ignorance of the legal regulations, as well as to manage the risks and threats inherent in the activity. In its activities, the Company will apply the methods and rules laid down in its Internal Rules and will assess and manage the risk of its customers according to their specifics.

§ The current Internal Rules of "BEAM GROUP" Ltd were adopted by decision of the sole owner of the capital on 20.11.2022 and amended on 31.10.2023.

§ These rules are provided for information and implementation to staff.

Martin Vidolov

Director

"BEAM GROUP" Ltd